Przegląd Techniczny Cyberbezpieczeństwa

Maj 2025

V1.3

1,63 MW Kampus Venco Holandia
Zainstalowany przez Alius Energy

1. Przegląd cyberbezpieczeństwa SolarEdge

1.1.1. Twoje bezpieczeństwo jest podstawą naszej działalności

SolarEdge to kompleksowe rozwiązanie dla energii słonecznej, oferujące falowniki, optymalizatory mocy i rozwiązania do monitorowania systemów w chmurze dla klientów indywidualnych i komercyjnych na całym świecie, obsługujące miliony użytkowników końcowych. Od pierwszego produktu SolarEdge aż po obecną ofertę, cyberbezpieczeństwo było kluczowym elementem rozwoju produktów SolarEdge i przyszłych planów, ewoluując wraz z najnowszą technologiąi stale zmieniającymi się zagrożeniami cybernetycznymi. Dążymy do ciągłej ochrony naszych klientów poprzez wdrażanie zaawansowanych środków cyberbezpieczeństwa na każdym etapie projektowania architektury naszych produktów i systemów, aż po kodowanie i testowanie.

1.1.2. Ochrona przed rosnącymi zagrożeniami cybernetycznymi

W dzisiejszym połączonym świecie, podobnie jak w przypadku innej krytycznej infrastruktury, energia może być celem zagrożeń cybernetycznych pochodzących z wielu źródeł. Takie zagrożenia obejmują zarówno finansowo motywowane schematy realizowane przez cyberprzestępców, jak i politycznie motywowane ataki organizowane przez państwa.Tylko w 2024 roku ofiary cyberataków na całym świecie (ze wszystkich sektorów) zapłaciły 814 milionów dolarów w wyniku ataków ransomware - i to tylko te zgłoszone przypadki.*

1.1.3. Niezabezpieczone systemy fotowoltaiczne stwarzają ryzyko biznesowe

Energia słoneczna to szybko rozwijający się element globalnego miksu energetycznego, stanowiący znaczącą część całkowitej produkcji energii w wielu krajach, takich jak Holandia, Niemcy i USA. Jest już krytycznym źródłem energii, które pomaga obniżyć koszty energii elektrycznej i zapewnić ciągłość działania wielu firm. Oferując zrównoważone rozwiązania energetyczne, systemy fotowoltaiczne wprowadzają również nowe drogi dla zagrożeń cybernetycznych. W sercu każdego systemu znajduje się falownik, urządzenie Internetu Rzeczy (IoT), które zwykle jest podłączone do Internetu w celu umożliwienia monitorowania i kontroli systemu.

Energia słoneczna jest wykorzystywana do zasilania coraz większej liczby lokalnych odbiorników energii, takich jak akumulatory, ładowarki pojazdów elektrycznych i systemy HVAC, i będzie to coraz częstsze w miarę przechodzenia do ery systemów zarządzania energią. Niezabezpieczony system fotowoltaiczny nie tylko zagraża ciągłości działania, ale może również służyć jako nieświadoma brama dla hakerów do uzyskania dostępu do odbiorników energii, a także szerszych platform cyfrowych organizacji, powodując dalsze szkody materialne, finansowe i reputacyjne.

1.1.4. Typowe zagrożenia cybernetyczne dla systemów fotowoltaicznych z ograniczoną ochroną lub jej brakiem:

Wyciek danych i kary

Jeśli nie są odpowiednio chronione, hakerzy mogą wykorzystać podatne systemy fotowoltaiczne do kradzieży prywatnych danych znajdujących się w wewnętrznych sieciach organizacji, co prowadzi do naruszenia danych i zmusza ofiarę do płacenia wysokich grzywien.

Zdalne sterowanie i odmowa usługi (DoS)

Gdy firma pada ofiarą ataków DoS lub naruszeń zdalnego sterowania, staje w obliczu znaczących zakłóceń. Oprogramowanie ransomware może przetrzymywać krytyczne dane jako zakładnika, podczas gdy ataki i naruszenia zdalnego sterowania i DoS mogą całkowicie zatrzymać podstawowe usługi.

Narażenie na niezgodność z przepisami

W miarę wprowadzania nowych regulacji dotyczących cyberbezpieczeństwa, właściciele instalacji fotowoltaicznych muszą podjąć proaktywne działania, aby zapewnić zgodność swoich systemów i uniknąć ryzyka wycofania produktów lub kar finansowych w przypadku naruszenia ich sieci.

* https:/ /www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion- 2025

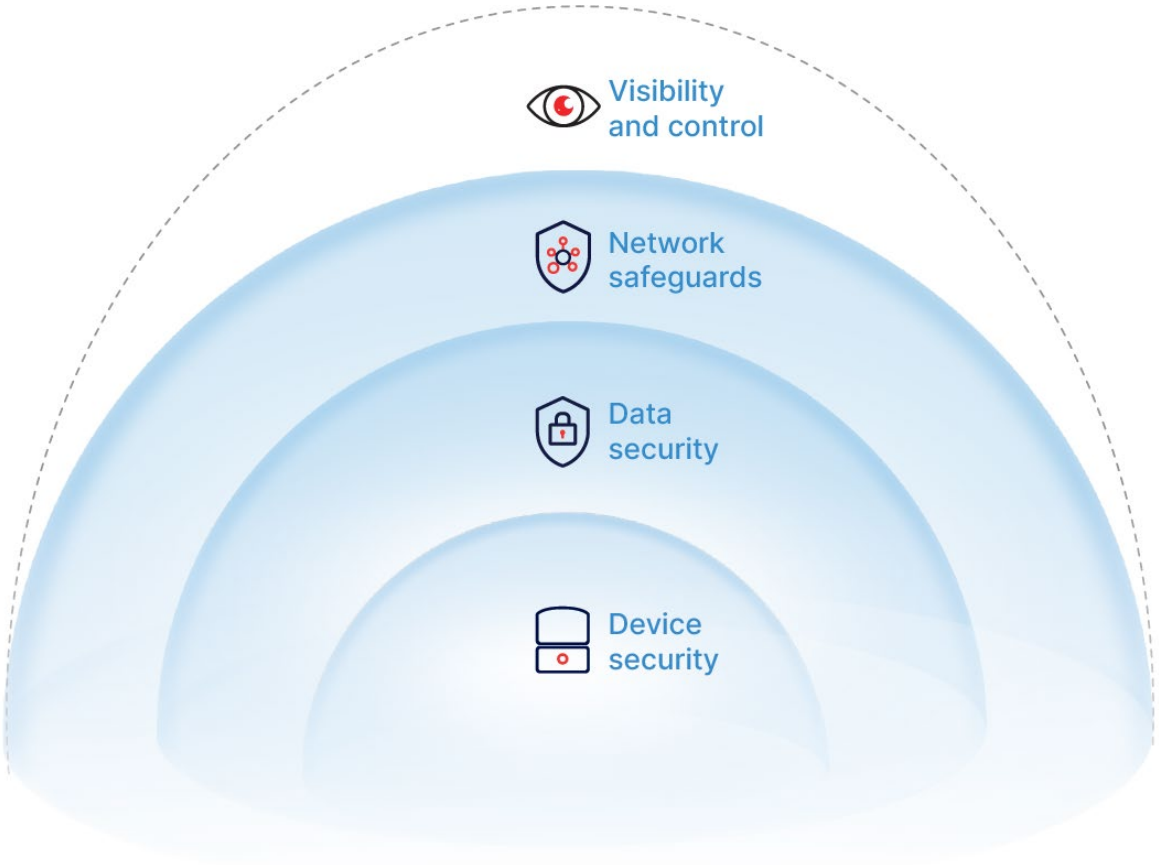
2. Podobnie jak bezpieczeństwo fotowoltaiki, cyberbezpieczeństwo fotowoltaiki jest niepodważalne

Podobnie jak w sportach zespołowych, cyberbezpieczeństwo wymaga współpracy i interdyscyplinarnego wysiłku, aby odnieść sukces. Bezpieczeństwo każdego produktu jest tylko tak dobre, jak bezpieczeństwo firmy, która go produkuje i zarządza jego działaniem. Wspierana rozległą wiedzą z zakresu cyberbezpieczeństwa, SolarEdge jest jednym z wiodących graczy w dziedzinie cyberbezpieczeństwa fotowoltaiki.

Innowacje mogą rozwijać się szybciej niż regulacje. Dlatego firmy muszą współpracować z agencjami regulacyjnymi, aby pomóc w zapewnieniu standaryzacji i harmonizacji rozwiązań cyberbezpieczeństwa z najnowszymi technologiami. Aktywnie uczestnicząc w różnych komitetach technicznych związanych z cyberbezpieczeństwem, SolarEdge nie tylko dba o to, aby nasze projektowanie produktów było zgodne z nadchodzącymi standardami cyberbezpieczeństwa, ale także pomaga w kształtowaniu tych standardów.

Podejście SolarEdge do bezpieczeństwa produktów

Opracowaliśmy holistyczne podejście oparte na czterech filarach, które ma na celu uwzględnienie wszystkich aspektów bezpieczeństwa produktu i jest szczegółowo opisane w następujących sekcjach tego dokumentu:



W miarę ewolucji przepisów w tej ważnej dziedzinie, SolarEdge utrzymuje aktywne zaangażowanie w odpowiednie standardy i regulacje na całym świecie, jak opisano w Rozdziale 3: Certyfikaty standardów i zgodność z przepisami.

3. Spis treści

1. Zakres dokumentu

Celem tego dokumentu jest zapewnienie klientom SolarEdge i właścicielom systemów kompleksowego przeglądu projektu i wdrożenia cyberbezpieczeństwa SolarEdge.
Środki cyberbezpieczeństwa SolarEdge są zgodne z zasadami przedstawionymi w:

- Dyrektywie Unii Europejskiej w sprawie urządzeń radiowych (RED) Artykuł 3.3
- Rozporządzeniu Unii Europejskiej NIS2
- Ustawie o cyberodporności Unii Europejskiej
- ETSI-303-645: Cyberbezpieczeństwo dla konsumenckich urządzeń Internetu Rzeczy
- Wytycznych i wymogach raportowania ENISA dotyczących cyberbezpieczeństwa
- UL-2941: Standard cyberbezpieczeństwa dla rozproszonych zasobów energetycznych i zasobów opartych na falownikach
- NIST IR 8498: Wytyczne dotyczące cyberbezpieczeństwa dla inteligentnych falowników
- IEEE 1547.3: Przewodnik po cyberbezpieczeństwie rozproszonych zasobów energetycznych połączonych z systemami elektroenergetycznymi
- Program etykietowania cyberbezpieczeństwa FCC dla inteligentnych urządzeń w USA
- Podstawy cyberbezpieczeństwa NARUC/NASEO dla systemów dystrybucji energii elektrycznej i DER
- ISO-27001 (2022): Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności — Systemy zarządzania bezpieczeństwem informacji – Wymagania
- OWASP (dla bezpieczeństwa aplikacji)
- Najlepsze praktyki bezpiecznego rozwoju oprogramowania, takie jak IEC 62443-4-1

Pełna lista certyfikatów, zgodności i powiązanych deklaracji znajduje się w Rozdziale 3: Certyfikaty standardów i zgodność z przepisami.

1.1. Produkty objęte zakresem

Następujące produkty SolarEdge są objęte zakresem tego dokumentu:

- Falowniki domowe
- Falowniki komercyjne
- Falownik SolarEdge TerraMax™
- Aplikacje internetowe i mobilne SolarEdge
- API SolarEdge i usługi sieciowe
- Kontroler SolarEdge ONE dla C&I
- Kontroler SolarEdge ONE dla zastosowań domowych

W całym tym dokumencie funkcje i możliwości bezpieczeństwa opisane są przypisane do "Urządzenia Bramy":

- W instalacjach, gdzie zainstalowany jest pojedynczy falownik, Urządzenie Bramy jest wbudowane w elektronikę samego falownika i jego płytę komunikacyjną
- W miejscach, gdzie kilka falowników jest połączonych lub skonfigurowanych w układzie lider-podążający; falownik lider zazwyczaj działa jako jedyne Urządzenie Bramy. Jako takie, zarządza ono aspektami cyberbezpieczeństwa całej komunikacji zewnętrznej z systemu do backendu, przez internet. W szczególnych przypadkach obsługiwane są inne topologie instalacji, aby dostosować się do specyficznych potrzeb
- W instalacjach C&I zarządzanych przez platformę SolarEdge ONE dla C&I, kontroler SolarEdge ONE może działać jako urządzenie bramy

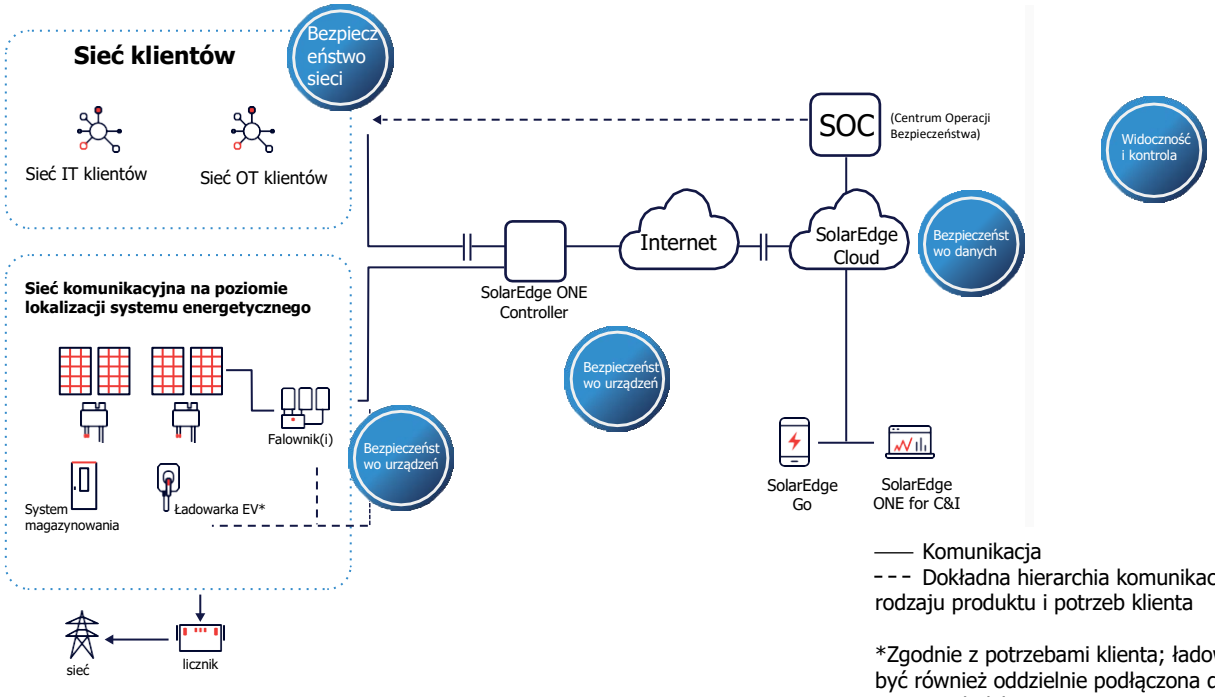
Optymalizatory mocy SolarEdge, akumulatory i inteligentne urządzenia, takie jak przełączniki, liczniki i podgrzewacze wody, są wyłączone z zakresu tego dokumentu, ponieważ nie są bezpośrednio dostępne z internetu i polegają na Urządzeniu Bramy w kwestii cyberbezpieczeństwa. W zależności od potrzeb klienta, ładowarki EV mogą być oddzielnie podłączone do internetu. Zalecamy robienie tego w ramach dedykowanej sieci VLAN.

Starsze systemy: Produkty wyprodukowane przed 2020 rokiem mogą mieć mniejsze możliwości niż te opisane w tym dokumencie.

2. Bezpieczeństwo produktów SolarEdge

Poniżej przedstawiono ilustrację typowego systemu SolarEdge C&I, podkreślającą cztery filary, które łączą się, aby chronić nasze produkty przed zagrożeniami cybernetycznymi (bezpieczeństwo urządzeń, bezpieczeństwo danych, zabezpieczenia sieciowe, widoczność i kontrola). Kolejne sekcje tego rozdziału szczegółowo omawiają różne funkcje, które składają się na to holistyczne podejście do cyberbezpieczeństwa SolarEdge. Oprócz tego poniższego przykładu, możliwe jest również lokalne połączenie w celu uruchomienia i konfiguracji.

Dodatkowe ilustracje typowego systemu SolarEdge z falownikiem TerraMax™ oraz typowej instalacji domowej SolarEdge można znaleźć w załączniku do tego dokumentu.



Rysunek 1: Schemat typowego układu systemu C&I w stanie ustalonym

2.1. Bezpieczeństwo urządzeń

Bezpieczeństwo urządzeń SolarEdge opiera się na okresowych ćwiczeniach analizy zagrożeń i oceny ryzyka, ciągłym wewnętrznym ręcznym i automatycznym skanowaniu kodu oraz przeglądach projektów, a także na corocznym cyklu testów penetracyjnych, przeprowadzanych zarówno wewnętrznie, jak i przez zewnętrznych audytorów.

2.1.1. Kontrola dostępu

Aktywacja produktu falownika

- Każdy falownik SolarEdge posiada własne unikalne hasło dostępu Wi-Fi, które jest generowane przy użyciu silnych algorytmów randomizacji i jest traktowane jako chroniona informacja od etapu linii montażowej. Zapewnia to bezpieczeństwo projektowe dla instalacji i eliminuje ryzyko związane z używaniem domyślnych haseł, przy jednoczesnym zachowaniu szybkiego i niezawodnego procesu instalacji
- Klienci mogą zobaczyć unikalne hasło dostępu Wi-Fi produktu na fizycznej etykiecie wydrukowanej na każdym urządzeniu
- Silne unikalne hasło generowane maszynowo jest uzupełnione wymogiem fizycznego dostępu podczas początkowego uruchomienia produktu
- Aktywacja produktu SolarEdge podczas uruchamiania może być przeprowadzona tylko przez właścicieli konta instalatora SolarEdge, którzy ukończyli proces wdrażania instalatora SolarEdge
- Użytkownicy muszą być zalogowani na swoje konto przez aplikację mobilną, aby aktywować produkt SolarEdge podczas uruchamiania
- Tylko gdy użytkownik spełni następujące trzy czynniki weryfikacji, może aktywować produkt:
  - Zalogowany jako instalator
  - Znane unikalne hasło
  - Ma fizyczny dostęp do urządzenia
- Gdy użytkownik lub instalator łączy się z bezpiecznym punktem dostępu Wi-Fi falownika, jego rola i uprawnienia są weryfikowane poprzez walidację tokena z ograniczonym czasem dostarczonego przez łączący się podmiot.
- W przypadku falowników w miejscach bez dostępu do internetu, instalatorzy muszą zalogować się przed opuszczeniem obszarów z łącznością. Pozostaną zalogowani przez ograniczony czas. Po przywróceniu łączności instalator powiąże się z numerem seryjnym urządzenia i miejscem, aby sfinalizować proces.
- Podczas udanej aktywacji przeprowadzana jest początkowa wymiana kluczy między wdrożonym systemem a centralnym systemem monitorowania SolarEdge. Ta wymiana zapewnia silny początkowy poziom uwierzytelnienia, bez potrzeby generowania lub zapamiętywania haseł przez użytkownika.
- W przypadku kontrolera ONE używany jest dedykowany punkt dostępu Wi-Fi do konfiguracji i uruchomienia, a proces uruchamiania i aktywacji jest oddzielny i bezpieczny.

Zdalne kontrole dostępu

- Użytkownicy i instalatorzy muszą korzystać z dedykowanych, ograniczonych interfejsów SolarEdge, aby uzyskać dostęp do urządzenia i zarządzać nim. Egzekwowany jest ścisły zestaw ról i uprawnień (RBAC), pozwalający na różne uprawnienia dla właścicieli systemów, instalatorów, personelu wsparcia itp.
- W przypadkach, gdy strony trzecie, takie jak lokalne zakłady energetyczne, wymagają dostępu do danych generowanych przez urządzenie, można włączyć tryb "Tylko podgląd", zapewniający ograniczony dostęp "Tylko do odczytu" do statusu i konfiguracji falownika. Aby uzyskać ten dostęp, użytkownicy muszą mieć fizyczny dostęp do urządzenia i znać jego unikalne hasło Wi-Fi
- Wszelki zdalny dostęp odbywa się tylko za pośrednictwem SolarEdge i zatwierdzonych aplikacji partnerów technologicznych, tj. przez chmurę SolarEdge i po prawidłowym uwierzytelnieniu przez odpowiednią platformę SolarEdge oraz w oparciu o unikalne poświadczenia
- Aby się zalogować, instalatorzy muszą co najmniej użyć swoich unikalnych poświadczeń. Dodatkowe metody identyfikacji wykorzystują urządzenie instalatora i obejmują opcje biometryczne (takie jak rozpoznawanie twarzy lub skanowanie odcisków palców), a także kody PIN i uwierzytelnianie oparte na wzorach
- Hasła użytkowników są zgodne z najlepszymi praktykami dotyczącymi złożoności haseł, które są okresowo aktualizowane. Wymagania dotyczące złożoności haseł uwzględniają wytyczne NIST 800-63-B.
- Dostęp do aplikacji lub komunikacja przeglądarkowa użytkownika odbywa się przez połączenie TLS 1.2+ (HTTPS) (przechodzenie na TLS 1.3+)
- SolarEdge proaktywnie monitoruje wyciek haseł instalatorów, poświadczeń do portalu monitorowania właścicieli systemów i inne potencjalne wskaźniki naruszenia systemu
- Każda próba dostępu do urządzenia jest rejestrowana i monitorowana

Wkrótce w 2025 roku:

- MFA dla kont instalatorów
- SSO i federacyjne SSO dla instalatorów i dużych kont
- Uwierzytelnianie kompatybilne z SAML2

Kontrola dostępu do sieci lokalnej

Falowniki SolarEdge są zaprojektowane tak, aby wspierać szybką, funkcjonalną i bezpieczną lokalną instalację dla instalatorów SolarEdge, w tym konfigurację parametrów sieciowych dla połączenia Wi-Fi. Podczas instalacji, zanim Urządzenie Bramy zostanie skonfigurowane, instalatorzy korzystają z dedykowanego zabezpieczonego kanału Wi-Fi między aplikacją instalacyjną SolarEdge a zainstalowanym systemem SolarEdge (jako punkt dostępu). Ten zabezpieczony kanał Wi-Fi opiera się na następujących zasadach:

- Urządzenie działa jako lokalny punkt dostępu Wi-Fi dla aplikacji instalatora SolarEdge
- Kanał hosta Wi-Fi jest domyślnie zamknięty
- Łączność Wi-Fi jest aktywowana tylko wtedy, gdy jest potrzebna do wykonania wyznaczonych zadań, i jest wyłączana zaraz po tym, aby zminimalizować wykrywanie sygnału przez osoby w pobliżu
- Aby ponownie włączyć sygnał Wi-Fi, użytkownicy i instalatorzy muszą nacisnąć fizyczny przycisk znajdujący się na urządzeniu (patrz Rysunek 2)

Aby nawiązać połączenie Wi-Fi, przesuń czerwony przełącznik ON/OFF/P falownika do pozycji "P" i zwolnij w ciągu 2 sekund.

Przesuń i zwolnij

Rysunek 2: Schemat przycisku sygnału Wi-Fi

- W każdym innym czasie punkt dostępu Wi-Fi urządzeń nie działa i przypadkowe skanowanie Wi-Fi nie ujawni punktu dostępu Bramy
- Zabezpieczony dostęp:
  - Każda Brama ma unikalne hasło Wi-Fi o długości 8 bajtów
  - Protokół szyfrowania Wi-Fi to WPA2
  - Komunikacja Wi-Fi LAN jest implementowana z najlepszymi praktykami związanymi z bezpieczeństwem dla silnego uwierzytelniania (802.1x) i algorytmów szyfrowania (WPA2-PSK z 128-bitowymi kluczami AES)
- Kontroler SolarEdge ONE wykorzystuje oddzielny bezpieczny mechanizm dostępu lokalnego

Kontrola dostępu fizycznego dla falowników

Podejście SolarEdge do bezpieczeństwa zakłada, że właściciel systemu traktuje falownik tak samo jak skrzynkę bezpieczników, zapewniając podstawową ochronę fizyczną przed nieupoważnioną osobą, która może próbować uzyskać fizyczny dostęp do sprzętu lub przeniknąć do sieci LAN. Chociaż lokalny dostęp jest uważany za mało prawdopodobny wektor ataku, urządzenie nadal implementuje pewne zabezpieczenia, takie jak zamykanie wszystkich portów debugowania, bezpieczny rozruch, mechanizmy bezpiecznego przechowywania i inne zabezpieczenia na poziomie urządzenia. Ponadto architektura łączności lokalnej produktu zakłada integrację różnych urządzeń energetycznych (SolarEdge i innych firm) i wspiera bezpieczną łączność.

Architektura opiera się na następujących zasadach bezpieczeństwa:

- Preferowana jest łączność przewodowa nad bezprzewodową, tam gdzie to możliwe
- Bezpieczeństwo dostępu fizycznego:
  - Wszystkie nieużywane interfejsy (usługi/porty) Urządzenia Bramy i falowników są wyłączone. Tylko określone, chronione porty są otwarte do komunikacji, umożliwiając dostęp do z góry określonych, bezpiecznych usług
  - Porty debugowania są zamknięte
  - Fizyczne mechanizmy antysabotażowe, w tym aluminiowe obudowy ze specjalnymi śrubami sześciokątnymi
- Gdy wymagana jest łączność na odległość fizyczną:
  - Zamiast Ethernetu można użyć Wi-Fi
  - Używana jest komunikacja radiowa krótkiego zasięgu
  - Komunikacja radiowa krótkiego zasięgu opiera się na protokole Thread© zgodnie z surowymi wymogami bezpieczeństwa. Wymusza to bliskość do Bramy w celu zainicjowania dostępu i nawiązania bezpiecznego połączenia
  - SolarEdge wykorzystuje to bezpieczne połączenie do przesyłania okresowych danych telemetrycznych z Bramy i innego sprzętu SolarEdge na miejscu. To połączenie jest również używane do celów konfiguracji i aktualizacji oprogramowania

- Komunikacja bezprzewodowa krótkiego zasięgu jest szyfrowana i zaprojektowana tak, aby zapewnić, że przerwanie komunikacji między urządzeniami w ramach jednej instalacji nie zakłóci działania sprzętu poza tą instalacją
- Nieautoryzowane urządzenia nie mogą uzyskać dostępu do ustanowionej sieci i dzielić komunikacji z podłączonymi urządzeniami

- Urządzenia nie obsługują funkcji automatycznego wykrywania i łączenia, takich jak te zapewniane przez UPnP, zapobiegając tym samym nawiązywaniu nieautoryzowanych i nieznanych połączeń. Muszą być ręcznie sparowane
- Walidacja danych wejściowych – dane wysyłane z dowolnych podłączonych urządzeń do innych urządzeń są skanowane i weryfikowane, w tym przez Urządzenie Bramy
- Ograniczony dostęp do urządzeń lokalnych – monitorowanie, konfiguracja i aktualizacje wersji są wykonywane przez Urządzenie Bramy (jeśli jest skonfigurowane do tego celu). Nie jest włączony bezpośredni dostęp/logowanie do urządzeń lokalnych

2.1.2. Integralność systemu

Głównym ryzykiem w urządzeniach wbudowanych jest możliwość manipulacji oprogramowaniem sprzętowym przez atakującego i zmiany zachowania urządzenia. Różne mechanizmy bezpieczeństwa są wbudowane w Bramę SolarEdge i inne urządzenia w celu weryfikacji integralności oprogramowania urządzenia.

Bezpieczna aktualizacja oprogramowania

Mechanizm zdalnej aktualizacji oprogramowania jest ważnym mechanizmem wsparcia i krytycznym wymogiem w każdej architekturze cyberbezpieczeństwa. Nowa aktualizacja oprogramowania (wersja) może zawierać nowe funkcjonalności, poprawki błędów oprogramowania i/lub rozwiązania problemów ze stabilnością oprogramowania, i/lub rozwiązania nowych zagrożeń cybernetycznych lub luk w zabezpieczeniach.

Wersje są kontrolowane, regularnie monitorowane i poddawane ocenie ryzyka zgodnie z najlepszymi praktykami. Nowe wersje są dostarczane do urządzeń za pomocą bezpiecznego mechanizmu zdalnej aktualizacji oprogramowania SolarEdge:

- Zdalna aktualizacja oprogramowania może być wykonana tylko po tym, jak urządzenie zainicjuje kanał komunikacyjny z backendem SolarEdge
- Integralność całego oprogramowania sprzętowego stosowanego na urządzeniu jest kryptograficznie uwierzytelniana
- Wersje oprogramowania sprzętowego nie mogą być obniżane
- Oprogramowanie sprzętowe i pliki wykonywalne są walidowane po otrzymaniu i odrzucane w przypadku złośliwego kodu
- Proces aktualizacji oprogramowania sprzętowego i wersji stosuje zabezpieczenia przed otrzymaniem lub instalacją uszkodzonych aktualizacji
- Minimalny okres wsparcia bezpieczeństwa i aktualizacji oprogramowania dla wszystkich urządzeń SolarEdge jest zgodny z wymogami regulacyjnymi
- SolarEdge wspiera bezpieczne i stopniowe wdrażanie aktualizacji w całej flocie

Mechanizmy białej listy

Aby zapobiec manipulacji kodem przed dostępem lub wykonaniem plików, urządzenie weryfikuje podpis plików wykonywalnych w czasie wykonania. W przypadku niepowodzenia walidacji, urządzenie zgłasza to do centrum monitorowania cyberbezpieczeństwa i podejmuje niezbędne działania, aby powrócić do bezpiecznego stanu.

Bezpieczny rozruch (nadchodzący w 2026 roku)

SolarEdge pracuje nad włączeniem mechanizmu bezpiecznego rozruchu w produktach Nexis, sprzętowej funkcji bezpieczeństwa zaprojektowanej w celu zapewnienia, że tylko zaufane i zweryfikowane komponenty oprogramowania są ładowane podczas procesu rozruchu.

Ten środek bezpieczeństwa jest planowany do włączenia w falownikach SolarEdge Nexis wydawanych od 2026 roku poprzez walidację integralności oprogramowania sprzętowego, systemu operacyjnego i krytycznych sterowników. Bezpieczny rozruch będzie zaprojektowany w celu ochrony przed nieautoryzowanymi modyfikacjami, złośliwym oprogramowaniem i rootkitami, zapewniając dodatkową warstwę obrony przed zagrożeniami bezpieczeństwa niskiego poziomu.

Aby zapobiec działaniu złośliwego oprogramowania bezplikowego w pamięci systemu (RAM), Brama jest zaprojektowana tak, aby okresowo resetować się, gdy falownik nie generuje energii, usuwając pamięć i pliki tymczasowe, a następnie powracając do zabezpieczonego podpisanego oprogramowania sprzętowego i plików wykonywalnych.

2.1.3. Bezpieczeństwo w czasie wykonywania

Dedykowany agent

SolarEdge integruje zaawansowane agenty antymalware IoT na swoich falownikach, zapewniając następujące ulepszenia bezpieczeństwa:

- Ochrona IoT przed atakami typu zero-day (które celują w nieznane luki w kodzie) i możliwości zapobiegania w czasie rzeczywistym
- Dedykowana ochrona plików oparta na jądrze (Odczyt/Zapis/Wykonanie) oprócz istniejących mechanizmów systemu operacyjnego
- Rozwiązanie agenta jest zaprojektowane do ciągłego monitorowania zdarzeń bezpieczeństwa i blokowania lub alertowania zespołu bezpieczeństwa SolarEdge (powiadomienia o alertach są przesyłane w czasie prawie rzeczywistym do naszego centrum operacji bezpieczeństwa)

Integralność przepływu sterowania

Zaawansowany agent bezpieczeństwa IoT SolarEdge zawiera warstwę bezpieczeństwa zwaną Integralnością Przepływu Sterowania (CFI). Wykonanie Bramy w czasie rzeczywistym jest zaprojektowane tak, aby chronić przed wrogimi próbami złośliwej manipulacji w linii produkcyjnej i w terenie. Dodatkowo, agent i urządzenie są zaprojektowane do ochrony integralności kodu poprzez:

- Warstwę weryfikacji do sprawdzania i zezwalania na legalne aktualizacje kodu
- Dynamiczny mechanizm, który weryfikuje i zezwala tylko na ładowanie legalnych stron kodu do pamięci

Ochrona pamięci

Agent jest zaprojektowany do ciągłego monitorowania i ochrony przed uszkodzeniami pamięci w celu zapobiegania wykorzystywaniu luk w zarządzaniu pamięcią. Monitoruje również każdą stronę ładowaną do pamięci, aby wykryć i zapobiec różnym etapom wykorzystywania.

Monitorowanie zdarzeń bezpieczeństwa

Zdarzenia wysyłane z agenta monitorującego urządzenie są przekazywane do panelu monitorowania i środowiska SIEM/SOC, a flota jest monitorowana pod kątem anomalii i nieoczekiwanych zachowań. Te strumienie danych mogą być udostępniane klientom i agencjom rządowym na żądanie.

Zarządzanie lukami w zabezpieczeniach urządzeń

Całe oprogramowanie i oprogramowanie sprzętowe urządzeń SolarEdge jest objęte programem zarządzania lukami w zabezpieczeniach, który składa się z automatycznego i ręcznego śledzenia luk w zabezpieczeniach open source i firm trzecich, zarządzania wewnętrznie znalezionymi lukami, programów bug bounty i odpowiedzialnego ujawniania oraz regularnych aktualizacji oprogramowania i oprogramowania sprzętowego.

2.1.4. Integralność i poufność danych

Głównym ryzykiem w urządzeniach wbudowanych jest możliwość kradzieży lub manipulacji wrażliwymi lub operacyjnie krytycznymi danymi i konfiguracjami przez atakującego. Różne mechanizmy bezpieczeństwa są wbudowane w falowniki SolarEdge w celu weryfikacji integralności danych urządzenia.

Bezpieczne przechowywanie z ARM TrustZone dla falowników SolarEdge Nexis (wkrótce)

Wrażliwe dane bezpieczeństwa, klucze kryptograficzne i krytyczne konfiguracje w falownikach Nexis będą bezpiecznie przechowywane przy użyciu naszego rozwiązania bezpiecznego przechowywania. Wykorzystując technologię ARM TrustZone i

specyficzne dla SoC funkcje sprzętowe, nasze bezpieczne przechowywanie jest izolowane od głównego systemu operacyjnego i aplikacji, mając na celu zapewnienie dodatkowej warstwy ochrony przed nieautoryzowanym dostępem i manipulacją.

To podejście do bezpieczeństwa oparte na sprzęcie ma na celu zapewnienie, że najcenniejsze zasoby pozostają poufne i bezpieczne, nawet w obliczu zaawansowanych ataków i bezpośrednich zdalnych naruszeń urządzenia. Kopia zapasowa danych konfiguracyjnych Bram jest przechowywana na serwerach SolarEdge i może być ponownie załadowana do Bramy, przywracając ją do bezpiecznego i działającego trybu.

Tryb offline

Całe systemy SolarEdge na miejscu są zaprojektowane do wykonywania swoich obowiązków nawet bez łączności internetowej. Jeśli połączenie internetowe zostanie utracone, tylko funkcje online będą upośledzone, takie jak możliwość zdalnego monitorowania wydajności systemu fotowoltaicznego, a także przeprowadzania zdalnego wsparcia. Jednak podstawowe funkcje są zaprojektowane do dalszego działania. Obejmują one między innymi działanie magazynu energii, produkcję fotowoltaiczną, zgodność z siecią i przepisami i wiele innych.

Uwierzytelniona i szyfrowana komunikacja

Cała istotna komunikacja jest szyfrowana i uwierzytelniana przy użyciu aktualnych i zalecanych mechanizmów kryptograficznych. Obejmuje to wszelką znaczącą komunikację IP, wszelką komunikację radiową, w tym Wi-Fi, oraz wszelką komunikację do lub z usług backendowych.

Zatwierdzone narzędzia kryptograficzne

Falowniki SolarEdge używają tylko zatwierdzonych i zalecanych metod komunikacji, w tym ścisłego wyboru zestawów szyfrów i wersji TLS, aby zapewnić poufność na lata, oraz gwarancję forward secrecy dla wszystkich istotnych komunikacji.

2.1.5. Logowanie i monitorowanie

SolarEdge stale monitoruje aktywność floty falowników w obliczu stale zmieniającego się krajobrazu i zagrożeń cybernetycznych. Poniższa sekcja opisuje procesy logowania falowników.

Logi na poziomie urządzenia

Wykonywane są następujące działania:

- Logowanie jest domyślnie włączone przy uruchomieniu
- Dla każdego zdarzenia Logi rejestrują, w stosownych przypadkach, użytkownika, rolę, identyfikator zdarzenia i znacznik czasu zdarzenia
- Logi bezpieczeństwa rejestrują następujące zdarzenia cyberbezpieczeństwa:
    - Wykryte manipulacje kodem
    - Wykryty złośliwy kod
    - Wykryta awaria logowania zdarzeń
    - Udane zdarzenia logowania
    - Nieudane zdarzenia logowania
- Dodatkowe logi są zbierane w celu identyfikacji potencjalnych wskaźników naruszenia o charakterze cyber-fizycznym. Takie wskaźniki obejmują przegrzanie, wydajność wewnętrznego wentylatora, a także inne parametry eksportu energii elektrycznej
- Logi bezpieczeństwa są dostępne tylko dla uprzywilejowanych użytkowników
- Logi są przechowywane przez 6-24 miesięcy, w zależności od typu logu
- W przypadku utraty łączności, urządzenia będą przechowywać logi w pamięci wewnętrznej przez okres wystarczający do retrospektywnej analizy.

Aby uzyskać informacje na temat reżimu logowania urządzenia bramy kontrolera SolarEdge ONE, prosimy o kontakt z przedstawicielem SolarEdge.

Logi na poziomie systemu

SolarEdge wykorzystuje najlepszy w swojej klasie system bazy danych oparty na czasie, który indeksuje wszystkie logi infrastruktury i sieci Platformy Monitorowania do indeksów opartych na czasie, integrując panel oparty na czasie, który pozwala SolarEdge przeszukiwać przeszłe i obecne logi, a także badać przeszłe i obecne incydenty. Logowanie serwerowe jest kluczową częścią architektury bezpieczeństwa SolarEdge. W rezultacie:

- Pliki logów serwera są częścią infrastruktury monitorowania bezpieczeństwa, umożliwiając SolarEdge badanie incydentów bezpieczeństwa, przeprowadzanie analizy przyczyn źródłowych itp.
- Uprawnienia dostępu do plików logów serwera są ograniczone tylko do autoryzowanych użytkowników, chroniąc je przed nieautoryzowaną modyfikacją lub usunięciem.

1MW, Asbury, NJ, USA,
zainstalowany przez Solar Landscape

2.2. Bezpieczeństwo danych

SolarEdge traktuje wszystkie dane z najwyższą ostrożnością i przestrzega najnowszych wymagań dotyczących cyberbezpieczeństwa i przepisów o ochronie prywatności.

2.2.1. Bezpieczeństwo aplikacji (AppSec)

Platforma backendowa

Platforma Monitorowania SolarEdge i usługi backendowe są rozwijane przy użyciu nowoczesnych bezpiecznych procesów rozwoju, w tym skanowania kodu źródłowego, bezpiecznego rozwoju, testów penetracyjnych, monitorowania konfiguracji, bezpiecznego przeglądu kodu, bezpiecznego projektowania i innych.

Aplikacje mobilne i internetowe dla klientów

Aplikacje mobilne i internetowe SolarEdge, w tym SolarEdge Go, SolarEdge Designer, SetApp, Mapper i mySolarEdge, klient internetowy monitorowania, Grid Services, SolarEdge ONE i API, są sprawdzane pod kątem luk w zabezpieczeniach i używają minimalnych uprawnień wymaganych na urządzeniu mobilnym. Logowanie do aplikacji odbywa się w stosunku do usług backendowych i planowane jest włączenie SSO, Federated SSO i MFA od III kwartału 2025 roku. Dane są bezpiecznie przechowywane w spoczynku i szyfrowane podczas przesyłania. Do rozwoju używane są frameworki aplikacji mobilnych, co utrudnia inżynierię wsteczną i zwiększa bezpieczeństwo elementów składowych aplikacji.

Regularne testy bezpieczeństwa

Klienci aplikacji i backendy SolarEdge przechodzą regularne wewnętrzne i zewnętrzne testy penetracyjne. Bezpieczeństwo aplikacji w SolarEdge jest realizowane zgodnie z ramami OWASP z dostosowaniami do unikalnego środowiska fotowoltaicznego.

2.2.2. Prywatność i integralność danych

Dane urządzenia

- Na urządzeniach SolarEdge, takich jak falowniki lub bramy, nie są przechowywane żadne dane osobowe. Dlatego nie jest stosowany żaden mechanizm szyfrowania do przechowywania osobistych danych użytkownika na urządzeniu
- Zmienne, które są mierzone w czasie rzeczywistym i zbierane, to stan sieci, zużycie urządzenia i pełna widoczność przepływu energii systemu: dane dotyczące zużycia, produkcji i importu/eksportu
- Przechowywane hasła są solone i haszowane
- Na urządzeniu nie są przechowywane nazwy użytkowników i hasła w postaci zwykłego tekstu
- Poufność danych przesyłanych między urządzeniem a chmurą jest chroniona przy użyciu najlepszych praktyk kryptograficznych (jak opisano w sekcji Bezpieczna komunikacja)
- Przywrócenie urządzenia do stanu fabrycznego usuwa wszelkie zebrane dane z urządzenia
- Bezpieczne przechowywanie - wrażliwe dane bezpieczeństwa, klucze kryptograficzne i krytyczne konfiguracje są bezpiecznie przechowywane przy użyciu rozwiązania bezpiecznego przechowywania naszego produktu. Wykorzystując technologię ARM TrustZone (dla falowników) i specyficzne dla SoC funkcje sprzętowe, nasze bezpieczne przechowywanie jest izolowane od głównego systemu operacyjnego i aplikacji, zapewniając dodatkową warstwę ochrony przed nieautoryzowanym dostępem i manipulacją. To podejście do bezpieczeństwa oparte na sprzęcie ma na celu zapewnienie, że najcenniejsze zasoby pozostają poufne i bezpieczne, nawet w obliczu zaawansowanych ataków i bezpośrednich zdalnych naruszeń urządzenia
- Sprzęt SolarEdge nie zawiera możliwości wykrywania (z wyjątkiem temperatury) i nie jest w stanie nagrywać dźwięku i wideo z założenia

Dane w chmurze i aplikacjach internetowych SolarEdge

Przechowywane dane

- SolarEdge wykorzystuje własną prywatną chmurę zlokalizowaną w Europie
- SolarEdge przestrzega przejrzystej polityki zbierania i przetwarzania danych, jak określono w jej Polityce prywatności
- Polityka prywatności danych SolarEdge jest w pełni zgodna z przepisami RODO
- SolarEdge stosuje różne kontrole bezpieczeństwa w celu ochrony danych użytkowników i kont w swoim prywatnym środowisku chmurowym
- Dane przechowywane w chmurze SolarEdge obejmują:
- Szczegóły identyfikacyjne dotyczące instalacji, zgłoszone przez instalatora za zgodą właściciela instalacji
- Dane dotyczące wydajności systemu, produkcji energii i zużycia
- Użytkownicy mogą zażądać usunięcia swoich danych osobowych (mailowo na adres privacy@solaredge.com)

Ochrona przed kradzieżą finansową i oszustwami

- Proces instalacji systemu SolarEdge nie obejmuje danych kart kredytowych ani żadnych innych form danych płatniczych
- Produkty SolarEdge są zaprojektowane w celu ochrony integralności danych i bezpiecznego działania urządzeń, również w odniesieniu do wpływu na finansowe aspekty wydajności systemu. Takie aspekty obejmują integralność funkcji pomiarowych klasy przychodowej, ochronę przed ograniczeniami eksportu nałożonymi przez lokalne zakłady dystrybucji energii oraz funkcje specyficzne dla jurysdykcji, takie jak generowanie i raportowanie REC (renewable energy credit)

Aplikacje internetowe i mobilne

Dostęp aplikacji do danych ma następujące mechanizmy bezpieczeństwa zaprojektowane w następujący sposób:

- Każdy użytkownik wymaga nazwy użytkownika i hasła do uwierzytelnienia aplikacji
- Od III kwartału 2025 roku instalatorzy będą mogli korzystać z uwierzytelniania wieloskładnikowego (MFA)
- Dostęp do aplikacji jest ograniczony zgodnie z określoną polityką SolarEdge
- W platformie SolarEdge stosowana jest kontrola dostępu oparta na rolach (RBAC), z zastosowaniem koncepcji projektowej "najmniejszych uprawnień"
- Aplikacje przechodzą testy penetracyjne w celu wykrycia typowych luk, takich jak OWASP Top 10 i inne, co najmniej raz w roku
- Program Bug Bounty - SolarEdge oferuje wynagrodzenie ekspertom ds. cyberbezpieczeństwa, którzy zgłaszają luki w zabezpieczeniach. Oferowane wynagrodzenie jest według uznania firmy i opiera się naryzyku, wpływie, łatwości wykorzystania, jakości raportu i dodatkowych względach (przeczytaj naszą Politykę skoordynowanego ujawniania luk)

GDPR (Ogólne rozporządzenie o ochronie danych)

SolarEdge świadczy usługi globalne i utrzymuje znaczącą obecność w Europie, w pełni przestrzegając wymogów RODO, w tym:

- Zgodne z prawem, uczciwe i przejrzyste przetwarzanie
- Ograniczenie celu, danych i przechowywania praw podmiotów danych
- Zgoda
- Naruszenia danych osobowych
- Prywatność w fazie projektowania - kontrole techniczne
- Ocena skutków dla ochrony danych
- Inspektor ochrony danych
- Świadomość i szkolenia

2.2.3. Zaawansowane obiekty hostingowe

Lokalizacja danych

SolarEdge przechowuje dane generowane przez swoje produkty w trzech dedykowanych obiektach hostingowych w Niemczech. Obiekty te są zgodne z następującymi standardami:

- ISO 9001:2015 Standard Systemów Zarządzania Jakością - wiodący standard zarządzania jakością, który zapewnia jasno ustrukturyzowane i systematyczne podejście do utrzymania i poprawy doświadczenia klienta.
- ISO/IEC 27001:2005, 27001:2013 i 27001:2022 Standard Systemu Zarządzania Bezpieczeństwem Informacji - szeroko akceptowana certyfikacja dostępna do wspierania bezpieczeństwa informacji, cyberbezpieczeństwa i ochrony prywatności. ISO 27001 zapewnia, że:
    - Ryzyka i zagrożenia dla biznesu są oceniane i zarządzane
    - Procesy bezpieczeństwa fizycznego, takie jak ograniczony/nazwany dostęp, są konsekwentnie egzekwowane
    - Audyty są regularnie przeprowadzane w każdym obiekcie, w tym testy bezpieczeństwa oraz planowanie i monitorowanie CCTV

Wszystkie odpowiednie wewnętrzne systemy SolarEdge są również zgodne z ISO 9001:2015. W miarę rozszerzania portfolio produktów SolarEdge, ta sekcja może być aktualizowana w przyszłości, aby uwzględnić dodatkowe lokalizacje przetwarzania w chmurze.

Bezpieczeństwo fizyczne

Środki bezpieczeństwa fizycznego dedykowanych obiektów hostingowych obejmują:

- Obecność ochroniarzy, systemów alarmowych i CCTV
- Środki ochrony ciągłości systemu obejmują urządzenie UPS i generatory zapasowe
- W całym obiekcie wdrożona jest metoda elektronicznej kontroli dostępu oparta na kartach magnetycznych
- W centrum danych działa system wykrywania wody, wraz z wodnym systemem gaszenia pożarów

2.2.4. Monitorowanie luk w zabezpieczeniach

Ciągłe programy monitorowania ułatwiają bieżącą świadomość zagrożeń, luk w zabezpieczeniach i bezpieczeństwa informacji w celu wspierania decyzji dotyczących zarządzania ryzykiem organizacji. SolarEdge wdrożyła i stale dostosowuje swoją strategię monitorowania serwerów, wykorzystując różnorodne rozwiązania technologiczne i najlepsze praktyki:

- Ustanowienie zdefiniowanych przez organizację metryk do monitorowania
- Na podstawie powyższego, wdrożenie ciągłego monitorowania wydajności przy użyciu narzędzi technologicznych
- Bieżące oceny kontroli bezpieczeństwa zgodnie ze strategią monitorowania organizacji

USA, zainstalowany przez Isolara Solar Power

2.3. Zabezpieczenia sieciowe

Systemy SolarEdge są podłączone do internetu, aby umożliwić szczegółowe dane monitorowania, ciągłe zdalne wsparcie, zdalne aktualizacje urządzeń i monitorowanie cyberbezpieczeństwa. Łączność internetowa systemów SolarEdge jest zaprojektowana i wdrożona z uwzględnieniem restrykcyjnych wymagań cyberbezpieczeństwa i jest stale testowana i aktualizowana zgodnie z modelami zagrożeń dla rozproszonych zasobów energetycznych.

2.3.1. Bezpieczne sieci

Bezpieczna i szyfrowana komunikacja

Cała komunikacja internetowa i bezprzewodowa jest szyfrowana i uwierzytelniana przy użyciu najlepszych w swojej klasie szyfrów i nowoczesnych standardów oraz zestawów kryptograficznych, wykorzystując "Uzgodnione mechanizmy kryptograficzne" SOG-IS i inne wytyczne jako podstawę do stosowania mechanizmów kryptograficznych i zestawów szyfrów.

Opcja komunikacji poza pasmem (komórkowa)

Falowniki obsługują łączność internetową przez opcjonalny modem komórkowy, tworząc w ten sposób przerwę powietrzną od sieci klienta i zapewniając najwyższy możliwy poziom ochrony sieci IT klienta przy jednoczesnym zachowaniu łączności. W takim ustawieniu wiele urządzeń SolarEdge może komunikować się między sobą przez oddzielną sieć radiową, dedykowaną sieć przewodową bez IP lub przez oddzielną sieć IP zarządzaną przez klienta, zgodnie z potrzebami instalacji i klienta.

Komunikacja asymetryczna

Bezpieczeństwo połączenia internetowego Bramy opiera się na tym, że wszystkie połączenia internetowe są inicjowane przez Bramę SolarEdge i urządzenia. Gdyby urządzenia wdrożone w terenie miały otwarte kanały odbiorcze, takie jak strona logowania użytkownika, mogłyby one być wykorzystane przez cyberprzestępców, którzy sondują urządzenie w poszukiwaniu otwartych portów i luk w usługach. Aby zminimalizować to ryzyko, urządzenia SolarEdge są zaprojektowane z bezpiecznym mechanizmem komunikacji, w którym Bramy otrzymują wiadomości z serwerów tylko wtedy, gdy Brama inicjuje kontakt z serwerami, odpytując o nowe polecenia i przesyłając nowe dane.

Urządzenia nie są wystawione na internet i nie mogą być dostępne ani wykryte przez skanery internetowe. Zaprojektowane rozwiązanie maskuje Bramy przed potencjalnymi hakerami i ma na celu uczynienie ich niewidocznymi dla ataków skanujących.

2.3.2. Mała powierzchnia ataku

Brak otwartych portów

Projekt i implementacja wszystkich urządzeń SolarEdge obejmują minimalizację powierzchni ataku na wszystkich poziomach. Zapewnia to, że tylko potrzebne porty IP są otwarte na poziomie oprogramowania. Ponadto, na poziomie urządzenia, nieużywane interfejsy i porty debugowania są zamknięte i chronione, jeśli nie są potrzebne.

Skanowanie Wi-Fi

Aby przeprowadzić początkowe uruchomienie, falowniki muszą wygenerować sieć Wi-Fi, aby działać jako punkt dostępu (AP). Jest to ograniczone tylko do sytuacji, w których urządzenie nie zostało jeszcze uruchomione lub nie ma aktywnego połączenia internetowego, które umożliwia działanie przez internet. Włączenie AP wymaga również ponownego uruchomienia lub fizycznego naciśnięcia przycisku, jeśli ma to zastosowanie. Te środki pomagają zapobiec widoczności urządzenia dla sąsiadów, przechodniów lub osób aktywnie skanujących dostępne sieci Wi-Fi.

2.3.3. Walidacja danych wejściowych

Połączenie z chmurą

Komunikacja z prywatną chmurą SolarEdge

Komunikacja między Urządzeniem Bramy a chmurą SolarEdge jest zaprojektowana z następującymi wielowarstwowymi zabezpieczeniami:

- Zapora sieciowa
- Zapora aplikacji internetowych (WAF) i globalny balancer obciążenia (GLB)
- Wewnętrzny IPS do serwera aplikacji
- Segmentacja sieci ACL (Lista kontroli dostępu)
- ACL (Lista kontroli dostępu) wewnętrznej platformy
- Wewnętrzna segmentacja sieci i architektura sieci zero-trust

Połączenie lokalne

Cała komunikacja między urządzeniami w lokalnej instalacji obejmuje ścisłą walidację danych wejściowych dla urządzeń SolarEdge i firm trzecich, aby zapewnić, że nieprawidłowo sformatowane dane wejściowe nie zostaną zaakceptowane w komunikacji urządzenie-urządzenie i użytkownik-urządzenie.

2.4. Widoczność i kontrola

Celem tej sekcji jest przedstawienie funkcji bezpieczeństwa produktu opracowanych w celu ułatwienia ciągłego monitorowania i reagowania. Głównym celem opisanych tu funkcji jest zapewnienie administratorom IT klientów i menedżerom ds. cyberbezpieczeństwa narzędzi do przygotowania się i reagowania na zagrożenia cybernetyczne, koncentrując się na widoczności przepływu danych, kanałach komunikacji i wydajności systemu w czasie rzeczywistym, aby umożliwić monitorowanie bezpieczeństwa i wykrywanie anomalii.

2.4.1. Kontrola łączności internetowej

Celem tej sekcji jest opisanie funkcji bezpieczeństwa produktu, które zapewniają szczegółową kontrolę nad trybami łączności internetowej. Pozwala to klientom o wysokich wymaganiach bezpieczeństwa na podłączenie urządzeń w konfiguracjach, które minimalizują ryzyko sieciowe do bardzo niskiego poziomu.

Tryby pracy offline

Jak opisano w sekcji Tryb offline , Brama i cały system SolarEdge na miejscu są zaprojektowane do kontynuowania wykonywania swoich obowiązków nawet bez łączności internetowej. Jeśli istnieje zagrożenie cybernetyczne, klienci mogą skonfigurować swoją zaporę sieciową, aby tymczasowo zablokować łączność internetową. Dane będą tymczasowo przechowywane cyklicznie przez okres do dwóch tygodni na urządzeniach i zostaną wysłane po wznowieniu łączności. łączności.

Wiele opcji łączności

W oparciu o politykę cyberbezpieczeństwa i IT użytkownika końcowego, falowniki SolarEdge mogą bezpiecznie łączyć się z internetem przez lokalny Ethernet, Wi-Fi lub modem komórkowy. Zabezpieczenia sieciowe opisane w sekcji 2.3 są stosowane niezależnie od warstwy fizycznej.

Urządzenia bramy (kontroler SolarEdge ONE) mogą być jednocześnie podłączone do Wi-Fi i Ethernetu, przy czym połączenie Ethernet jest głównym połączeniem. Jeśli połączenie Ethernet zawiedzie, komunikacja automatycznie przełączy się na Wi-Fi. Urządzenie bramy nie korzysta z łączności komórkowej.

"Tryb bezpieczny" – komunikacja jednokierunkowa

SolarEdge zapewnia dodatkowy mechanizm bezpieczeństwa zwany Komunikacją Jednokierunkową lub "Zdalnym Wsparciem" dla falowników. Gdy ta funkcja jest włączona, wszystkie przychodzące polecenia do urządzenia (z chmury SolarEdge) są odrzucane i nie przetwarzane. W takim scenariuszu cały dostęp zewnętrzny jest ograniczony, chyba że osoba jest fizycznie obecna przy systemie i otwiera tymczasowe okno dostępu dla zdalnego wsparcia lub aktualizacji oprogramowania.

2.4.2. Udostępnianie danych dotyczących cyberbezpieczeństwa

Ujawnianie luk w zabezpieczeniach

SolarEdge wspiera i zachęca do skoordynowanego ujawniania luk w zabezpieczeniach (CVD) dotyczących swoich produktów. W ramach polityki cyberbezpieczeństwa SolarEdge utrzymuje procedurę ujawniania i program bug bounty. Każda zgłoszona luka w produktach lub aplikacjach SolarEdge, która otrzymuje CVE, jest dokumentowana i udostępniana publicznie. Najnowsze, aktualne informacje można znaleźć na naszej stronie internetowej Polityki Skoordynowanego Ujawniania Luk stronie internetowej.

Integracja z rozwiązaniem SIEM/SOC

SolarEdge wdrożyła solidny system, w którym alerty i zdarzenia z naszej rozległej sieci milionów zainstalowanych falowników są stale przesyłane do Centrum Operacji Bezpieczeństwa (SOC).

Pozwala to na monitorowanie w czasie rzeczywistym, aby szybko wykryć wszelkie nietypowe aktywności w całej flocie. Te dane mogą być udostępniane rozwiązaniom SIEM/SOC klientów lub dostawcom usług, zarówno w kontekście pojedynczej instalacji, jak i dla konta klienta.

2.4.3. Wskazówki dotyczące bezpiecznej instalacji

Przewodnik konfiguracji zapory sieciowej – FQDN

Menedżerowie muszą skonfigurować polityki zapory sieciowej przy użyciu białych list, które umożliwią komunikację między falownikami na miejscu a funkcjonalnymi FQDN (Fully Qualified Domain Names) SolarEdge.

Białe listy umożliwiają również operacje wsparcia między urządzeniami.

Obowiązkowe FQDN na białej liście

Następujące FQDN muszą być na białej liście, aby umożliwić transmisję danych z falownika:

Funkcja	FQDN	Protokół	Port
Komunikacja IOT	prodfqdn.solaredge.com	TCP	443
Bezpieczne wdrażanie	svcfqdn.solaredge.com	TCP	443
Monitorowanie bezpieczeństwa	svcfqdn.solaredge.com	TCP	443
Synchronizacja czasu	time.google.com * Adresy IP mogą się zmieniać w zależności od lokalizacji geograficznej. Upewnij się, że używasz FQDN, a nie adresu IP.	TCP	123
Zapasowa synchronizacja czasu	www.google.com * Adresy IP mogą się zmieniać w zależności od lokalizacji geograficznej. Upewnij się, że używasz FQDN, a nie adresu IP.	TCP	80
Wyszukiwanie DNS	www.google.com	TCP	53
Zdalny dostęp instalatora	portia- tu.solaredge.com	TCP	5555
Zdalny dostęp wsparcia	serminv.solaredge.com	TCP	2222
Aktualizacje oprogramowania	Biała lista serwerów brzegowych CloudFront docs.aws.amazon.com	TCP	443
Łączność i opóźnienie (ping)	8.8.8.8	ICMP	

Opcjonalne FQDN na białej liście

Następujące FQDN mogą być dodane do białej listy w celu obsługi funkcji opcjonalnych:

Funkcja	FQDN	Protokół	Port
Komunikacja z chmurą	prodfqdn.solaredge.com	TCP	22222 / 22221
Aktualizacje oprogramowania	https://embedded-repo-dev.s3.eu-central-1.amazonaws.com	TCP	443
RSSH	linux-prod.solaredge.com	TCP	2222

Aby uzyskać listę FQDN dla kontrolera SolarEdge ONE, prosimy o kontakt z lokalnym przedstawicielem SolarEdge.

W niektórych przypadkach karamba-proxi.solaredge.com będzie pojawiać się jako FQDN monitorowania bezpieczeństwa, do czasu zakończenia migracji.

3. Certyfikaty standardów i zgodność z przepisami

Raporty certyfikacyjne SolarEdge można uzyskać tutaj.

3.1. Certyfikaty cyberbezpieczeństwa

3.1.1. ISO27001

- SolarEdge posiada certyfikat ISO 27001. ISO/IEC 27001 to międzynarodowy standard dotyczący zarządzania bezpieczeństwem informacji. Określa on wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji (ISMS) - którego celem jest zwiększenie bezpieczeństwa posiadanych zasobów informacyjnych. Organizacje spełniające wymagania standardu mogą zdecydować się na certyfikację przez akredytowaną jednostkę certyfikującą po pomyślnym zakończeniu audytu. Przestrzegając tego standardu, SolarEdge potwierdza przyjęcie praktyk bezpieczeństwa informacji w całej swojej sieci i systemach.

SolarEdge jest zgodna z najnowszą wersją standardu ISO 27001, opublikowaną w 2022 roku (ISO 27001:2022)

- Przestrzeganie tego standardu obejmuje takie działania jak, ale nie ogranicza się do:
    - Pisemne wewnętrzne polityki, wytyczne i udokumentowane praktyki bezpiecznego przetwarzania i ochrony danych
    - Testowanie pracowników SolarEdge pod kątem phishingu e-mailowego
    - Wewnętrzne audyty programu bezpieczeństwa i prywatności
    - Audyty zewnętrzne programu bezpieczeństwa i prywatności
    - Proces oceny ryzyka i zarządzania ryzykiem w celu regularnego przeglądu zagrożeń, na które narażona jest firma
    - Program zapewniający bezpieczeństwo w procesach zarządzania zasobami ludzkimi SolarEdge
    - Procesy i procedury zapewniające, że incydenty bezpieczeństwa są wykrywane w odpowiednim czasie i skutecznie rozwiązywane
    - Terminowe łatanie znanych luk w zabezpieczeniach
    - Ochrona systemów przed złośliwym kodem
    - Blokowanie oprogramowania i sprzętu w celu ograniczenia niepotrzebnych usług

3.1.2. ETSI-303-645

Falowniki SolarEdge posiadają certyfikat ETSI-303-645. Ten standard określa podstawowe wymagania bezpieczeństwa dla konsumenckich urządzeń Internetu Rzeczy (IoT), zapewniając kompleksowe ramy dla zapewnienia, że urządzenia i systemy IoT są bezpieczne już na etapie projektowania. Obejmuje on kluczowe obszary, takie jak ochrona danych, zarządzanie lukami w zabezpieczeniach, aktualizacje oprogramowania i kontrola dostępu użytkowników, mając na celu łagodzenie najczęstszych i najbardziej znaczących zagrożeń w krajobrazie IoT.

Dostosowując się do ETSI EN 303 645, SolarEdge demonstruje swoje zaangażowanie w osadzanie solidnych środków bezpieczeństwa w swoich produktach i infrastrukturze IoT. Standard wymaga wdrożenia praktyk bezpieczeństwa, takich jak:

- Silne polityki haseł i eliminacja uniwersalnych haseł domyślnych
- Regularne aktualizacje bezpieczeństwa falownika w celu rozwiązania znanych luk w zabezpieczeniach
- Proaktywne środki zapobiegające nieautoryzowanemu dostępowi i manipulacji
- Jasne i dostępne informacje dla użytkowników umożliwiające bezpieczne i świadome korzystanie z urządzeń

3.1.3. SSDLC

- Nasze oprogramowanie jest tworzone z bezpieczeństwem jako podstawą, wykorzystując ramy Bezpiecznego Cyklu Życia Rozwoju Oprogramowania (SSDLC) do osadzenia solidnych środków bezpieczeństwa w całym procesie rozwoju, zapewniając ochronę przed lukami w kodzie i minimalizując ryzyko bezpieczeństwa
- SolarEdge wykorzystuje szereg metodologii w swoich procesach rozwoju sprzętu i oprogramowania. Stosujemy bezpieczne procedury rozwoju oprogramowania, w tym okresowe automatyczne i ręczne testy podatności
- Zdecydowana większość kodu w produktach SolarEdge pochodzi od wewnętrznych zespołów rozwojowych. Zespoły te przechodzą szkolenia z zakresu bezpiecznych praktyk kodowania
- SolarEdge nie zleca na zewnątrz rozwoju kodu w swoich produktach

- W przypadkach, gdy używane są zewnętrzne biblioteki lub partnerstwa związane z oprogramowaniem, stosowane są kompensacyjne kontrole bezpieczeństwa, takie jak audyty, aby zapewnić jakość kodu w kontekście bezpiecznego rozwoju
- Oprogramowanie open source jest skanowane pod kątem znanych luk w zabezpieczeniach jako część procesów rozwoju i wdrażania oprogramowania
- Kody źródłowe produkcji są przechowywane w lokalnych systemach kontroli źródeł chronionych przez fizyczną i hasłową/prywatną autentykację kluczem
- Nasz poziom SSDLC jest zgodny z wymaganiami przedstawionymi w IEC 62443-4-1

3.2. Zgodność z przepisami

3.2.1. UK Product Security and Telecommunications Infrastructure (UK-PSTI)

Produkty SolarEdge są zgodne z wymaganiami UK-PSTI. Certyfikat można znaleźć tutaj.

3.2.2. Dyrektywa w sprawie urządzeń radiowych (RED), artykuł 3.3

Falowniki SolarEdge są zgodne ze wszystkimi odpowiednimi wymaganiami cyberbezpieczeństwa Dyrektywy w sprawie urządzeń radiowych (Artykuł 3.3).

3.2.3. NIS2 – zgodność na poziomie "Podmiotu Podstawowego"

- SolarEdge jest zgodna ze wszystkimi odpowiednimi wymaganiami cyberbezpieczeństwa dyrektywy NIS 2 na wszystkich obowiązujących rynkach państw członkowskich Unii Europejskiej.
- SolarEdge jest zgodna z regulacją NIS 2.0 zgodnie z podwyższonymi wymaganiami bezpieczeństwa dla "Podmiotu Podstawowego"

3.3. Nadchodzące regulacje

- Ustawa o cyberodporności

Produkty SolarEdge są rozwijane zgodnie z opublikowanymi wymaganiami Ustawy o cyberodporności, która ma stać się obowiązkowa w latach 2026-2027 Dowiedz się więcej.

- Wytyczne NIST dotyczące inteligentnych falowników

Produkty SolarEdge w pełni spełniają wytyczne opisane w wytycznych Narodowego Instytutu Standardów i Technologii (NIST) IR 8498 "Cyberbezpieczeństwo dla inteligentnych falowników" z 2024 roku dla mieszkaniowych i lekkich komercyjnych systemów energii słonecznej Dowiedz się więcej.

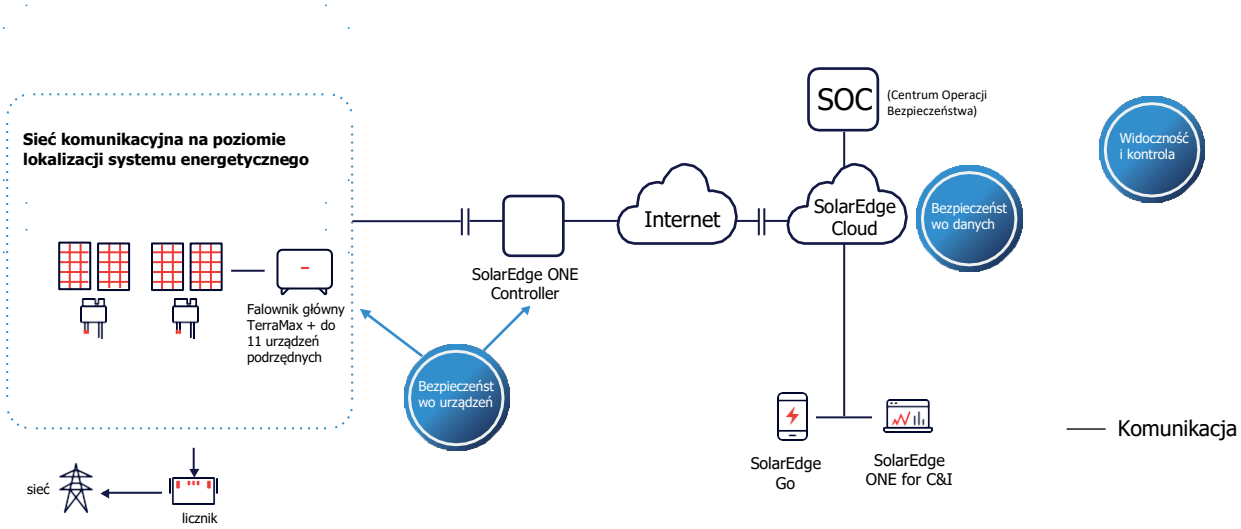
- NARUC/ NASEO

Produkty SolarEdge spełniają podstawowe wymagania cyberbezpieczeństwa opisane przez Narodowe Stowarzyszenie Regulatorów Użyteczności Publicznej (NARUC) Stanów Zjednoczonych dla systemów dystrybucji i DER Dowiedz się więcej.

4. Załącznik - Schematy rozwiązań

- **Typowa instalacja z falownikiem SolarEdge TerraMax™:**

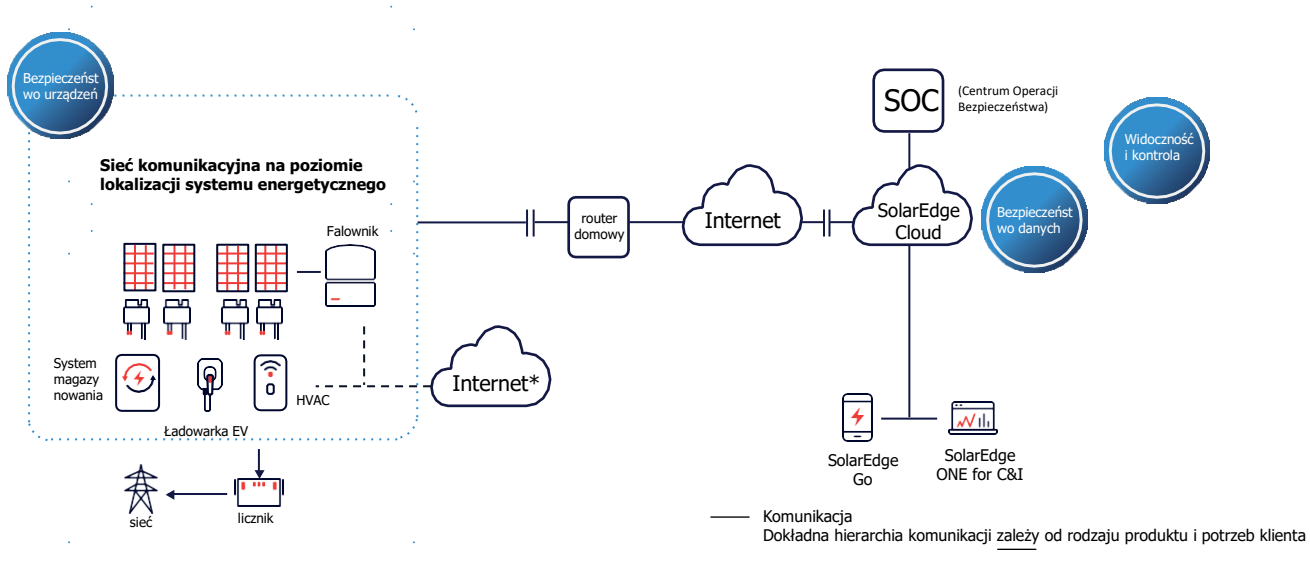
Poniżej przedstawiono ilustrację typowego systemu komercyjnego SolarEdge z falownikiem TerraMax, podkreślającą różne filary, które łączą się, aby chronić nasze produkty przed zagrożeniami cybernetycznymi (bezpieczeństwo urządzeń, bezpieczeństwo danych oraz widoczność i kontrola).



Rysunek 3: Typowa instalacja falownik SolarEdge TerraMax

- Typowa instalacja z systemem domowym SolarEdge:

Poniżej przedstawiono ilustrację typowego systemu domowego SolarEdge, podkreślającą różne filary, które łączą się, aby chronić nasze produkty przed zagrożeniami cybernetycznymi (bezpieczeństwo urządzeń i bezpieczeństwo danych).



Rysunek 4: Typowa instalacja mieszkaniowa SolarEdge

*Zgodnie z potrzebami klientów; połączenia ładowarek EV, baterii domowych i inteligentnych termostatów z internetem mogą być dozwolone.

©SolarEdge Technologies, Ltd. Wszelkie prawa zastrzeżone. Zmiany zastrzeżone bez uprzedzenia