BEZPIECZEŃSTWO DANYCH I URZĄDZEŃ POMIAROWYCH

Dawid Gruszka

Bezpieczeństwo danych i urządzeń pomiarowych

Dlaczego bezpieczeństwo danych i urządzeń pomiarowych jest tak istotne ?

Cyberbezpieczeństwo

CERT podaje, że w 2021 roku prawie 14% wszystkich cyberataków w naszym kraju dotyczyło sektora energetycznego. Na świecie 34% firm z branży naftowej i gazowniczej w ciągu ostatnich dwóch lat napotkało problem przejęcia maszyn przez hakerów. Ochrona internetu rzeczy to obecnie jedno z największych wyzwań dla całej branży.

Jak podaje World Economic Forum („Global Security Outlook Report 2023"), w ubiegłym roku jednym z głównych celów cyberataków były elementy infrastruktury krytycznej, takie jak szpitale, lotniska czy elektrownie.

Cyfryzacja i cyberbezpieczeństwo kluczowe dla transformacji energetyki. W ostatnim czasie znacząco rośnie liczba cyberzagrożeń dla sektora

2023-03-13 | 06:30

Fala cyberataków uderza w europejski sektor energetyki wiatrowej

GOSPODARKA | Piątek, 29 kwietnia 2022 (05:10)

Polski sektor energetyczny na celowniku hakerów. Co nam grozi?

3 października 2022, 13:58

Hakerzy coraz częściej atakują energetykę

18.11.2021

Rozporządzenie MKiŚ z dnia 22 marca 2022 r.

Dz. U. 2018 poz. 1560

U S T A W A

z dnia 5 lipca 2018 r.

o krajowym systemie cyberbezpieczeństwa[1)]

Warszawa, dnia 8 kwietnia 2022 r.

Poz. 788

ROZPORZĄDZENIE
MINISTRA KLIMATU I ŚRODOWISKA[1)]

z dnia 22 marca 2022 r.

w sprawie systemu pomiarowego[2), 3)]

Rozdział 1

Przepisy ogólne

§ 1. Rozporządzenie określa:

1) wymagania funkcjonalne, jakie spełnia system pomiarowy;

2) wymagania w zakresie bezpieczeństwa systemu pomiarowego, w tym ochrony tego systemu przed nieuprawnioną ingerencją w ten system oraz nieuprawnionym dostępem do informacji rynku energii;

Rozporządzenie MKiŚ z dnia 22 marca 2022 r.

Rozdział 3

Wymagania w zakresie bezpieczeństwa systemu pomiarowego, w tym ochrony tego systemu przed nieuprawnioną ingerencją w ten system oraz nieuprawnionym dostępem do informacji rynku energii

§ 4. 1. System pomiarowy działa w sposób ciągły oraz zapewniający jego ochronę przed nieuprawnioną ingerencją. W tym celu stosuje się środki techniczne i organizacyjne polegające w szczególności na:

1) ustaleniu warunków i sposobu przydzielania uprawnień do dostępu do informacji rynku energii przetwarzanych w systemie pomiarowym;

2) opracowaniu instrukcji bezpieczeństwa systemu pomiarowego, w tym zarządzania ryzykiem oraz procedury bezpiecznej eksploatacji tego systemu umożliwiającej w szczególności jak najszybsze wykrywanie incydentów zagrażających bezpieczeństwu tego systemu;

3) okresowym sprawdzaniu stanu bezpieczeństwa systemu pomiarowego i odpowiednim podnoszeniu poziomu tego bezpieczeństwa;

4) stosowaniu zabezpieczeń na możliwie wielu różnych poziomach organizacji ochrony systemu pomiarowego w celu ograniczenia występowania przypadków, w których przełamanie pojedynczego zabezpieczenia będzie skutkować naruszeniem poufności, integralności lub dostępności danych pomiarowych;

5) opracowaniu procedury postępowania w przypadku awarii elementów systemu pomiarowego;

6) zapewnieniu odporności na awarie systemu pomiarowego, w szczególności przez zapewnienie ciągłości działania jego systemów telekomunikacyjnych i teleinformatycznych przez co najmniej 8 godzin po wystąpieniu awarii;

7) stosowaniu zabezpieczeń przed działaniem złośliwego oprogramowania;

8) zapewnieniu autoryzacji autentyczności i sprawdzeniu integralności aktualizacji oprogramowania systemu pomiarowego;

9) zapewnieniu poufności, integralności oraz dostępności informacji rynku energii;

10) zabezpieczeniu przed nieuprawnionym dostępem do informacji rynku energii oraz przypadkowymi zmianami i celową modyfikacją tych informacji.

2. Licznik zdalnego odczytu spełnia wymagania techniczno-funkcjonalne określone w pkt 10 załącznika nr 1 do rozporządzenia dla danej kategorii.

Obszary ochrony Systemu Pomiarowego

Ludzie & procesy

Procedury & regulacje

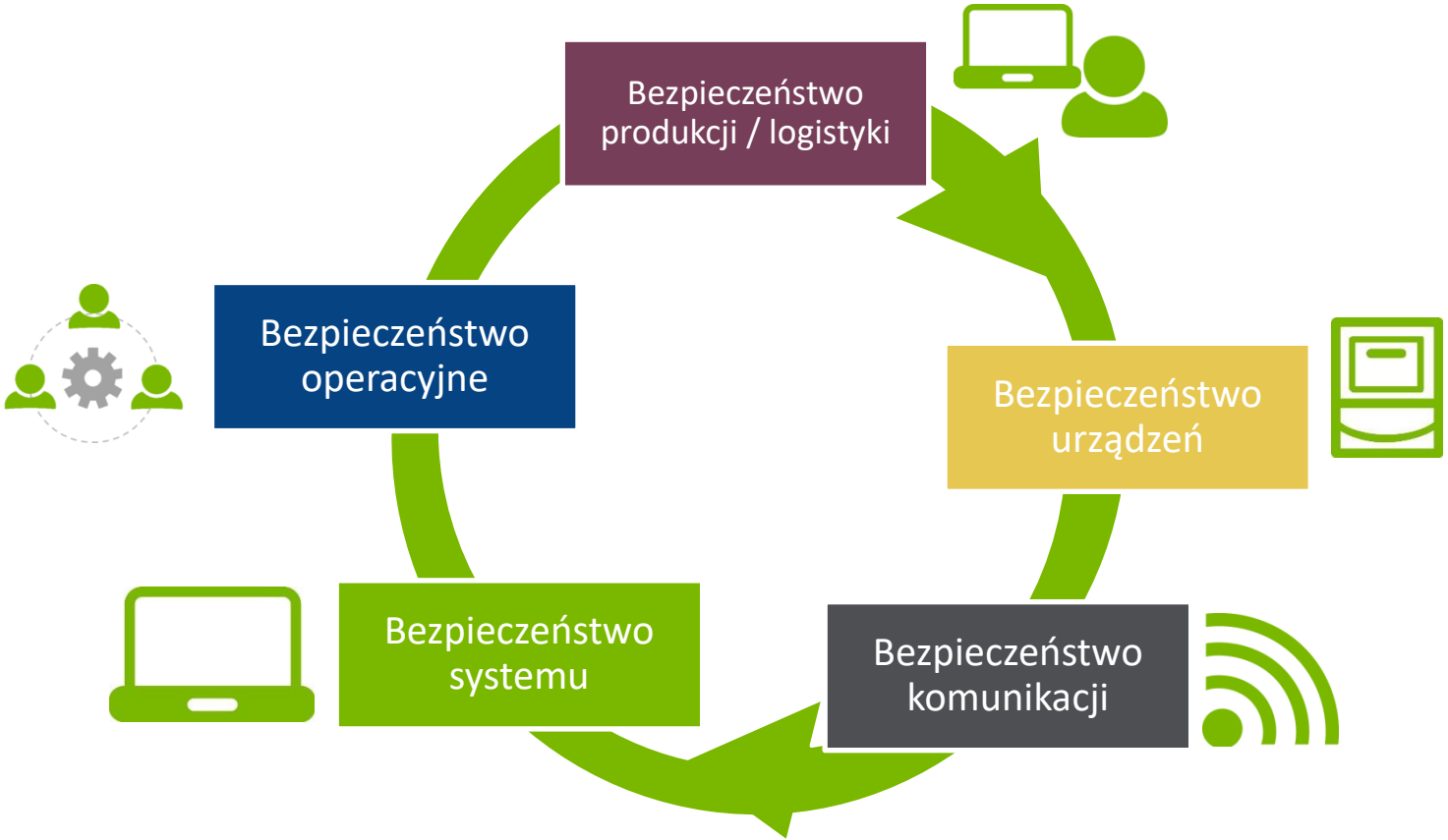
Infrastruktura IT

Fizyczne bezpieczeństwo

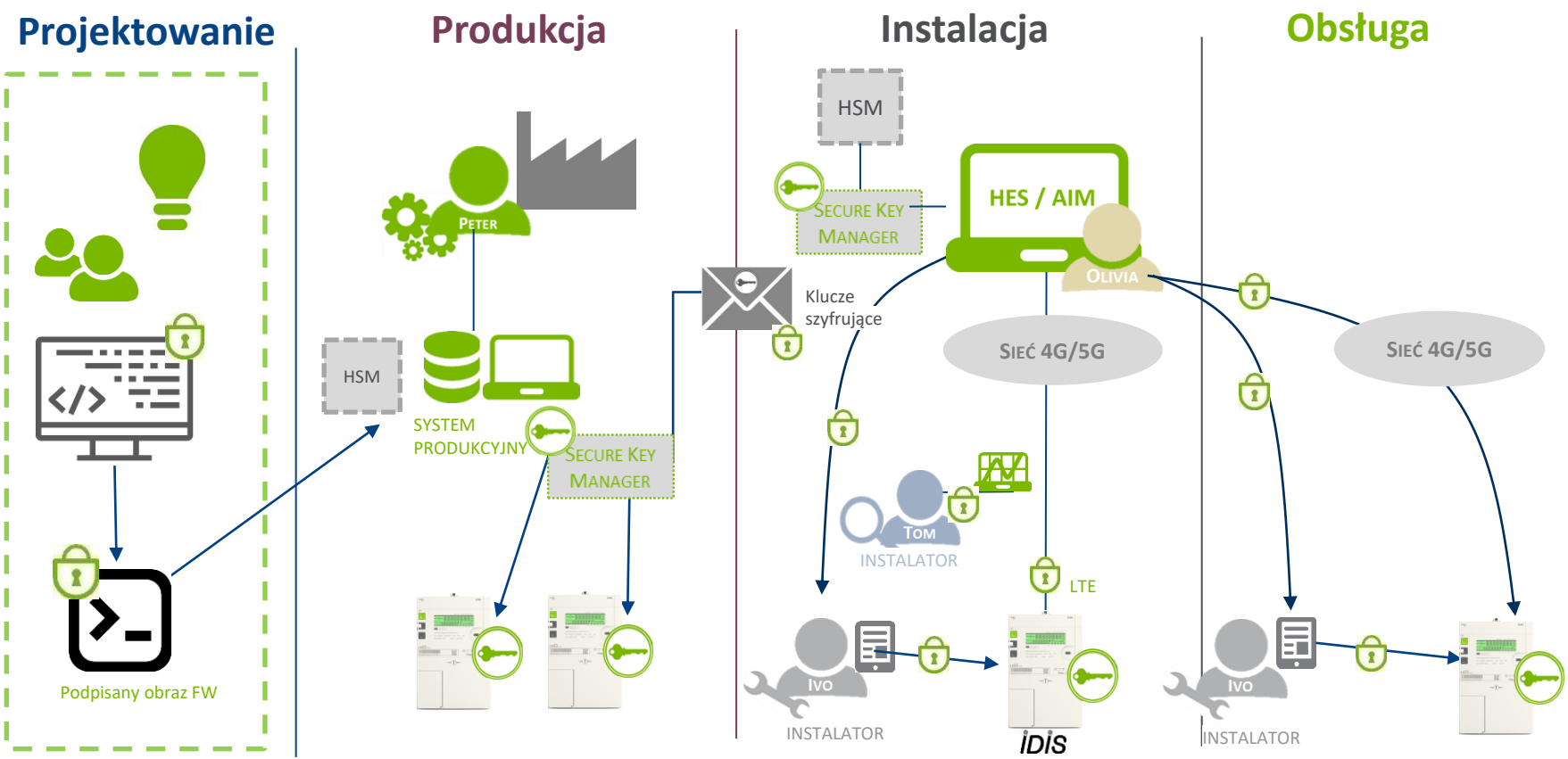
Aplikacje i urządzenia

Poufność, integralność, dostępność

Bezpieczeństwo danych i urządzeń pomiarowych



Bezpieczeństwo na każdym etapie procesu



Podstawowe filary bezpieczeństwa informacji

Landis+Gyr

Dostęp
Ochrona dostępu do systemu, sieci lub urządzenia

Uwierzytelnienie, Poświadczenia, Separacja

Uprawnienia
Definiowanie, co użytkownicy mogą zrobić z danymi

Autoryzacja, Role użytkowników, uprawnienia

Ochrona danych
Zabezpieczenie danych przed nieautoryzowanym odczytem, kopiowanie, modyfikacja

Szyfrowanie, Tokenizacja

Monitorowanie
Raportowanie działań użytkowników, zdarzeń i ruchów danych

Zdarzenia, Logowanie, Audyt

Aktualizacje
Aktualizacje lub modyfikacje podnoszące poziom bezpieczeństwa

Aktualizacja oprogramowania

Zabezpiecz

Wykryj i Zareaguj

Wykryj i Zareaguj

Bezpieczeństwo produkcji i dostaw LZO

Każdy producent liczników jest odpowiedzialny za produkcję i przechowywanie materiałów bezpieczeństwa związanych z licznikiem, tak aby poufność, integralność i autentyczność materiału bezpieczeństwa nie zostały naruszone podczas produkcji i przetwarzania końcowego licznika w miejscu produkcji

Producent urządzeń musi zapewnić procedury gwarantujące, że tylko odpowiednio upoważniony personel może uzyskać dostęp do bezpiecznych danych i obsługiwać je.

Producent urządzeń powinien utrzymać ścieżkę audytu w zakresie generowania, przechowywania oraz parowania kluczowych materiałów bezpieczeństwa wyprodukowanych przed wysyłką do klienta.

Bezpieczeństwo produkcji i dostaw LZO

Dostęp

W jaki sposób i gdzie materiał bezpieczeństwa jest przechowywany na etapie produkcji ?

W jaki sposób materiał bezpieczeństwa jest dystrybuowany i kto ma do niego dostęp ?

Czy materiał bezpieczeństwa jest dostarczany bezpośrednio od producenta urządzeń czy od pośrednika ?

Uprawnienia

Czy systemy produkcyjne posiadają właściwe zabezpieczenia zapewniające ochronę przed pozyskaniem materiału bezpieczeństwa urządzeń przez osoby nieuprawnione ?

Kto posiada uprawnienia pozwalające na wgląd lub pozyskanie materiału bezpieczeństwa?

Ochrona danych

Czy systemy produkcyjne przechowują materiał bezpieczeństwa urządzeń w postaci zaszyfrowanej ?

Czy wszystkie etapy dystrybucji kluczy (proces eksportu, przekazania oraz importu) zapewniają właściwą ochronę materiału bezpieczeństwa ?

Monitorowanie

Czy systemy produkcyjne posiadają mechnizmy monitorowania i logowania dostępu do przechowywanych tam danych ?

Czy proces dystrybucji materiałów bezpieczeństwa jest w pełni transparentny, a zdarzenia dostępu do tych danych rejestrowane ?

Aktualizacje

Czy procesy produkcyjne urządzeń oraz dystrybucji materiałów bezpieczeństwa są cyklicznie weryfikowane oraz dostosowywane do aktualnych wymagań bezpieczeństwa ?

Bezpieczeństwo produkcji i dostaw LZO

System bezpieczeństwa jest tak silny, jak jego najsłabsze ogniwo

Zarządzanie bezpieczeństwem informacji na etapie projektowania (RnD) oraz produkcji urządzeń (ISO 27001)

Zarządzanie materiałem bezpieczeństwa (generacja, przechowywanie, wgrywanie) w kontrolowanym i w pełni chronionym środowisku zlokalizowane na tereniu EU, EEA lub EFTA.

Zarządzanie jakością, bezpieczeństwem oraz środowiskiem produkcji zgodne z obowiązującymi standardami:

- ✓ ISO 9001 (Zarządzanie jakością)
- ✓ ISO 14001 (Zarządzanie środowiskowe)
- ✓ ISO 45001 (Bezpieczeństwo i higiena pracy)
- ✓ ISO 22301 (Ciągłość produkcji)

Bezpieczeństwo inwestycji

- **Trwałość i jakość projektowanych komponentów**
- **Stosowanie bibliotek certyfikowanych i zatwierdzonych przez NIST**
- **Wiarygodność finansowa oraz zdolności produkcyjne**
- **Gwarancja ciągłości dostaw i prowadzenia biznesu**
- **Europejskie doświadczenia projektowe**
- **Doświadczony i lokalny zespół wsparcia technicznego**
- **Kodeks etyczny prowadzenia biznesu**
- **Zrównoważony rozwój i społeczna odpowiedzialność (CSR) -** publikacja i audyt raportów zrównoważenia (ang. Sustainability repors) opisujących stosowanie przez przedsiębiorców praktyk obejmujących kwestie środowiskowe, ekonomiczne, społeczne oraz ekologiczne

Podsumowanie

Rozwiązania bezpieczeństwa muszą chronić Spółki Energetyczne, jednocześnie przewidując zmieniające się zagrożenia, aby sprostać wymaganiom **potrzeb jutra**.

Standardy branżowe, powinny bazować na **standardach otwartych** i być wykorzystywane w celu uzyskania spójności oraz **interoperacyjności rozwiązania**.

Opracowując najlepsze w swojej klasie rozwiązania bezpieczeństwa, bazujące na standardach rekomendowanych przez FIPS, **Landis+Gyr zapewnia gwarancję, że bezpieczeństwo danych i infrastruktura krytyczna Spółek Energetycznych jest bezpieczna**, a usługi świadczone na rzecz klientów oraz reputacja Spółek Enrgetycznych są chronione.

Dziękuję za uwagę

Dawid Gruszka
Regionalny Kierownik ds. Sprzedaży

dawid.gruszka@landisgyr.com
Phone +48 606780690

Landis+Gyr Sp. z o.o.
www.landisgyr.com