

KARTA SCENARIUSZA — WERSJA SKRÓCONA

NOVENERGIA OZE — karta scenariusza

Wersja skrócona · wyciąg operacyjny do sześciu ćwiczeń · Szkolenie „NIS2 / UoKSC w praktyce” · LT MASTERY

Do czego służy ta karta: To jest wyciąg operacyjny ze scenariusza — same dane potrzebne przy sześciu ćwiczeniach, na pięciu stronach zamiast jedenastu. Pełna wersja („Scenariusz NOVENERGIA OZE — 29.12.2025”) zawiera dodatkowo faktografię z raportu CERT Polska, pełny rejestr aktywów, komplet ról i pełną oś czasu incydentu. Trzymaj tę kartę przy sobie; do pełnej wersji sięgaj tylko wtedy, gdy potrzebujesz szczegółu technicznego.

Zastrzeżenie: NOVENERGIA OZE sp. z o.o. jest spółką fikcyjną, utworzoną wyłącznie na potrzeby szkolenia. Mechanizmy ataku odwzorowują publiczny raport CERT Polska „Raport z incydentu w sektorze energii 29.12”; dane spółki, daty wewnętrzne i reakcje organizacji dobrano na potrzeby ćwiczeń.

1. Kim jest NOVENERGIA

Firma i siedziba	NOVENERGIA OZE sp. z o.o., Płock (woj. mazowieckie), działa od 2014 r. Spółka dominująca w grupie.
Co robi	Wytwarzanie energii elektrycznej ze źródeł odnawialnych, sprzedaż energii oraz — od 2022 r. — zdalne monitorowanie parametrów pracy instalacji dla dwóch niezależnych właścicieli farm fotowoltaicznych.
Majątek produkcyjny	5 farm fotowoltaicznych i 1 farma wiatrowa; 180 MW mocy zainstalowanej; 6 Głównych Punktów Odbioru (GPO).
Kody PKD w odpisie z KRS	35.11.Z · 35.14.Z · 33.14.Z · 62.09.Z — odpis sporządzony przed 2025 r., kody w układzie PKD 2007.
Odbiorcy	Rynek hurtowy oraz umowy bilateralne z trzema odbiorcami przemysłowymi.

Uwaga do kodów PKD: Odpis pochodzi sprzed 2025 r. W PKD 2025 te same rodzaje działalności mają inne kody: wytwarzanie z OZE to 35.12.B (fotowoltaika) i 35.12.A (wiatr), handel energią to 35.15.Z, a 62.09.Z w ogóle nie istnieje — zastąpiły go 62.90.Z i 62.20.B. Kod 33.14.Z pozostał bez zmian. Przelicz kody, zanim ustalisz sektor — szczegóły w dokumencie „Mapa PKD 2025 → Załączniki nr 1 i 2 UoKSC”.

2. Grupa kapitałowa i dane wielkościowe

Podmiot	Udział	Zatrudnienie (RJR)	Obrót za 2025 r.
NOVENERGIA OZE sp. z o.o. (dominująca)	—	168	41 mln EUR
NOVENERGIA Serwis sp. z o.o.	100 %	74	11 mln EUR
NOVENERGIA Trading sp. z o.o.	100 %	23	11 mln EUR
RAZEM GRUPA		265	63 mln EUR

Suma bilansowa grupy na 31.12.2025: 58 mln EUR. Rok obrotowy pokrywa się z kalendarzowym. Sprawozdanie finansowe za 2025 r. sporządzono 15 maja 2026 r., a zatwierdzono 12 czerwca 2026 r. — dniem badania przesłanek wielkościowych jest dzień SPORZĄDZENIA sprawozdania (art. 5 ust. 5 UoKSC). Zatrudnienie podano w rocznych jednostkach roboczych (RJR) w rozumieniu załącznika I do rozporządzenia 651/2014. Wartości w euro przeliczono według kursu NBP.

Fakt istotny dla samoidentyfikacji: Wszystkie trzy spółki grupy pracują we WSPÓLNEJ domenie Active Directory utrzymywanej w centrali w Płocku, korzystają z tej samej platformy SCADA i z tego samego łącza oraz urządzeń brzegowych. NOVENERGIA Serwis wykonuje utrzymanie farm należących do spółki dominującej, a Trading sprzedaje wytworzoną przez nią energię — spółki świadczą usługi wspólnie. Ten fakt przesądza, że nie ma zastosowania wyłączenie z art. 5 ust. 6 UoKSC, które pozwala nie liczyć progów łącznie, gdy system informacyjny podmiotu jest niezależny od systemów przedsiębiorstw powiązanych.

3. Infrastruktura — co jest i jak zabezpieczone

Aktywo	Rola	Stan zabezpieczeń
Urządzenie brzegowe FortiGate — 6 szt., po jednym na GPO	Koncentrator VPN i zaporą; zdalny dostęp serwisowy	Interfejs SSL-VPN dostępny z Internetu; konta lokalne bez MFA; TE SAME poświadczenia na wszystkich sześciu obiektach
Sterowniki RTU — 6 szt.	Telemechanika, komunikacja z OSD protokołem DNP3.0	Konto producenta z hasłem domyślnym nigdy niezmienionym; weryfikacja podpisu firmware wyłączona
Sterowniki zabezpieczeń — 12 szt.	Zabezpieczenia polowe	Usługa FTP włączona domyślnie; konto wbudowane aktywne
Komputery HMI — 6 szt., Windows 10	Wizualizacja stanu pracy obiektu	Hasło lokalnego administratora ustawione przez integratora, identyczne na wszystkich obiektach; brak EDR
Serwery portów szeregowych — 18 szt.	Konwersja RS485 na komunikację z OSD	Interfejs webowy włączony, domyślny login i hasło
Serwer SCADA — centrala	Telemetria ze wszystkich obiektów ORAZ usługa dla klientów zewnętrznych	W tej samej domenie Active Directory co sieć biurowa; brak segmentacji IT–OT
Kontrolery domeny AD — 2 szt.	Uwierzytelnianie w sieci biurowej i na SCADA	Brak MFA na kontach administracyjnych; 7 kont z uprawnieniami administratora domeny
Serwer NAS — centrala	Kopie zapasowe systemów biurowych i SCADA	W tej samej domenie; brak kopii offline i kopii niemodyfikowalnej
Pocztą i pakiet biurowy w chmurze	Pocztą, dokumenty, komunikator	MFA włączone dla 60 % kont; brak przeglądu uprawnień administracyjnych

4. Dostawcy z dostępem do systemów

Dostawca	Usługa	Dostęp i stan umowy
ELEKTROSERWIS TECHNIKA sp. z o.o.	Integrator automatyki; wdrożenie i serwis GPO	Stały, BEZTERMINOWY dostęp VPN do wszystkich sześciu obiektów; konta wspólne dla zespołu serwisowego; umowa z 2019 r. bez klauzul bezpieczeństwa
NET-KOM sp. z o.o.	łącza i utrzymanie urządzeń brzegowych	Zdalna administracja urządzeniami FortiGate; brak wymogu zgłaszania incydentów
BIURO IT PARTNER s.c.	Obsługa informatyczna sieci biurowej	Konta administratora domeny; umowa zawiera klauzulę poufności, nie zawiera wymagań bezpieczeństwa
Dostawca chmury publicznej	Poczta, dokumenty, komunikator	Umowa standardowa na regulaminie dostawcy; brak indywidualnych klauzul; brak planu wyjścia
Producent sterowników RTU	Wsparcie techniczne i firmware	Kontakt wyłącznie przez zgłoszenia serwisowe; brak subskrypcji powiadomień o podatnościach

5. Kto za co odpowiada

Prezes zarządu	Całość działalności. Nie uczestniczył dotąd w żadnym szkoleniu z cyberbezpieczeństwa.
Członek zarządu ds. technicznych	Eksploracja farm i inwestycje. Formalny właściciel obszaru OT.
Kierownik działu IT (dział 2 osoby)	Sieć biurowa, poczta, stacje robocze, kopie zapasowe. Pełni nieformalnie funkcję opiekuna bezpieczeństwa — bez powołania i bez zakresu obowiązków.
Kierownik działu utrzymania (4 osoby)	Eksploracja GPO, współpraca z integratorem. Dysponuje dostępem serwisowym; nie raportuje do IT.
Dyżurni operatorzy (praca zmianowa)	Nadzór ruchowy i kontakt z dyspozycją OSD — całodobowo, ale bez kompetencji i uprawnień w zakresie bezpieczeństwa IT.
Główna księgowa	Finanse i rozliczenia. Prowadzi rejestr umów i faktur — jedyne kompletne źródło listy dostawców.
Specjalista ds. kadr	Rekrutacja i dokumentacja pracownicza. Nie prowadzi weryfikacji niekaralności.
Radca prawny (obsługa zewnętrzna)	Umowy i sprawy korporacyjne. Nie był angażowany w tematy cyberbezpieczeństwa.

6. Stan zgodności na 1 grudnia 2025 r.

Dwadzieścia osiem dni przed atakiem. To jest punkt wyjścia Ćwiczenia 4.

Obszar	Stan	Szczegóły
Ustalenie statusu podmiotu kluczowego lub ważnego	BRAK	Temat nigdy nie był przedmiotem analizy ani posiedzenia zarządu
Wniosek o wpis do wykazu	BRAK	Nie złożono; nikt nie ma konta w systemie teleinformatycznym

Obszar	Stan	Szczegóły
Struktury odpowiedzialne za cyberbezpieczeństwo (art. 14)	CZĘŚCIOWO	Kierownik IT pełni funkcję nieformalnie, bez powołania i bez zakresu obowiązków; brak umowy z MSSP
Polityka bezpieczeństwa informacji	NIEAKTUALNA	Dokument z 2019 r. przygotowany na potrzeby przetargu, nigdy nieaktualizowany i niedystrybuowany
Analiza ryzyka i rejestr ryzyk	BRAK	Nigdy nie przeprowadzono
Uwierzytelnianie wieloskładnikowe (MFA)	CZĘŚCIOWO	60 % kont w chmurze; brak na dostępie VPN i na kontach administracyjnych
Zarządzanie podatnościami	BRAK	Brak skanowania; aktualizacje OT wyłącznie przy okazji wizyt serwisowych
Segmentacja sieci IT i OT	BRAK	SCADA w tej samej domenie co sieć biurowa; brak zapory segmentacyjnej
Monitorowanie systemów	CZĘŚCIOWO	Tryb 8x5 realizowany przez dwuosobowy dział IT; logi lokalne, bez centralizacji
Procedura zarządzania incydentami	CZĘŚCIOWO	Istnieje jako załącznik do polityki z 2019 r., nigdy nieprzećwiczona; nie wskazano właściwego CSIRT
Kopie zapasowe i testy odtworzeniowe	CZĘŚCIOWO	Kopie codzienne na NAS w tej samej domenie; ostatni test odtworzenia — marzec 2023 r.
Plan ciągłości działania	CZĘŚCIOWO	Opracowany w 2021 r. dla ubezpieczyciela; brak RTO i RPO; nigdy nietestowany
Ocena ryzyka dostawców	BRAK	Brak rejestru dostawców ICT; umowy bez klauzul bezpieczeństwa
Szkolenia kierownictwa (art. 8e)	BRAK	Nie prowadzono
Weryfikacja niekaralności personelu (art. 8f)	BRAK	Nie prowadzona ani wobec pracowników, ani wobec personelu integratora

7. Oś czasu incydentu

Oznaczenie: Techniki i mechanizmy odwzorowują raport CERT Polska. Dаты, godziny i reakcje organizacji dobrano na potrzeby ćwiczeń — zwłaszcza opóźnienie zgłoszenia, którego raport CERT Polska nie opisuje.

Data i godzina	Etap	Co się wydarzyło
ok. 20.11.2025	Rozpoznanie	Skanowanie internetowych adresów spółki z zagranicznego adresu IP. Zapisane w logach urządzenia brzegowego — nikt ich nie przeglądał.
08.12.2025, 21:14	Dostęp wstępny	Logowanie do SSL-VPN na GPO nr 3, na konto serwisowe integratora, bez MFA. Poświadczenia identyczne na wszystkich sześciu obiektach.
08.12.2025, 21:40	Utrwalenie dostępu	Pulpit zdalny do komputera HMI na koncie lokalnego administratora; zmiany konfiguracji przez PowerShell — udziały administracyjne i reguła zapory „Microsoft Update” na porcie TCP 445.

Data i godzina	Etap	Co się wydarzyło
25.12.2025, 03:20	Rozpoznanie OT	Skanowanie sieci obiektowych i próby logowania na sterownikach RTU oraz serwerach portów szeregowych. Zapisane w logach; brak monitorowania w dni świąteczne.
27.12.2025	Eskalacja uprawnień	Zrzut pamięci procesu uwierzytelniania na stacji administratora IT, przejęcie konta administratora domeny, kopia bazy Active Directory.
29.12.2025, 07:40	Destrukcja — OT	Na wszystkich sześciu obiektach: uszkodzenie firmware'u sterowników RTU, usunięcie plików systemowych na sterownikach zabezpieczeń, reset serwerów portów szeregowych do ustawień fabrycznych ze zmianą adresu IP na nieosiągalny.
29.12.2025, 07:52	Destrukcja — IT	Uruchomienie oprogramowania niszczącego dane na komputerach HMI i serwerze SCADA; próba uruchomienia go na stacjach w centrali przez politykę GPO — brak EDR, nic tego nie zatrzymało.
29.12.2025, 07:58	Zacieranie śladów	Przywrócenie wszystkich sześciu urządzeń brzegowych do ustawień fabrycznych. Utrata logów lokalnych.
29.12.2025, 08:05	Pierwszy sygnał	Telefon dyspozytora OSD: brak telemetrii z czterech farm. Dyżurny operator traktuje to jako awarię łączą.
29.12.2025, 08:20	Potwierdzenie	Dyżurny inżynier potwierdza brak zdalnego sterowania na WSZYSTKICH obiektach i brak dostępu do urządzeń brzegowych. Powiadamia kierownika utrzymania.
29.12.2025, 09:30	Diagnostyka	Kontakt z integratorem. Hipoteza: awaria zasilania i uszkodzenie sprzętu. Wyjazd ekipy serwisowej.
29.12.2025, 14:10	Rozpoznanie charakteru	Serwisant stwierdza firmware w wersji nigdy nieinstalowanej w spółce i zmienione hasła serwerów portów. Informacja trafia do kierownika IT.
29.12.2025, 16:45	Eskalacja wewnętrzna	Kierownik IT informuje członka zarządu ds. technicznych. Decyzja: „przeanalizujemy sprawę po Nowym Roku”.
30.12.2025, 11:00	Decyzja	Prezes zarządu dowiadyuje się o zdarzeniu od dyspozytora OSD, nie z wewnątrz organizacji. Polecenie natychmiastowego zgłoszenia.
30.12.2025, 18:00	Zgłoszenie	Zgłoszenie do CSIRT NASK — około 34 godziny po uzyskaniu wiedzy o zdarzeniu. Brak logów z urządzeń brzegowych uniemożliwia ustalenie pełnego przebiegu.

Moment, od którego liczy się termin: Wzorcowy start zegara to 29.12.2025 o godz. 08:20 — potwierdzenie utraty zdalnego sterowania na sześciu obiektach jednocześnie. Jednoczesność wyklucza awarię. To jest przedmiot rozstrzygnięcia w Ćwiczeniu 5.

8. Które dane do którego ćwiczenia

Ćw.	Temat	Rozdziały tej karty
1	Samoidentyfikacja podmiotu	Rozdz. 1 (profil i kody PKD) oraz rozdz. 2 (grupa, dane wielkościowe, wspólne systemy)
2	Macierz RACI dla 10 obszarów art. 8	Rozdz. 5 (role) oraz rozdz. 6 (stan zgodności)
3	Rejestr ryzyk	Rozdz. 3 (infrastruktura) i rozdz. 4 (dostawcy)

Ćw.	Temat	Rozdziały tej karty
4	Analiza luk	Rozdz. 6 (stan zgodności na 1.12.2025)
5	Pierwsze 24 godziny	Rozdz. 7 (oś czasu) oraz rozdz. 1 i 2 do danych podmiotu w formularzu zgłoszenia
6	Plan na 90 dni	Wynik Ćwiczenia 4 plus rozdz. 3, 4 i 5 do przypisania właścicieli