

MATERIAŁ DLA UCZESTNIKA

Scenariusz szkoleniowy: NOVENERGIA OZE sp. z o.o.

Studium przypadku na podstawie ataku na polską energetykę z 29 grudnia 2025 r. · Materiał wspólny dla wszystkich sześciu ćwiczeń · Szkolenie „NIS2 / UoKSC w praktyce”

Jak korzystać z tego dokumentu: To jest jedno wspólne studium przypadku dla całego dnia szkoleniowego. Wszystkie sześć ćwiczeń opiera się na danych zawartych w Części II i III. Proszę mieć ten dokument otwarty przez cały czas trwania szkolenia i wracać do niego przy każdym ćwiczeniu — mapa „które dane do którego ćwiczenia” znajduje się na końcu, w Części IV.

Dokument składa się z czterech części:

- Część I — tło faktyczne: rzeczywisty incydent z 29 grudnia 2025 r. opisany w raporcie CERT Polska. Wszystko, co znajduje się w tej części, wydarzyło się naprawdę.
- Część II — NOVENERGIA OZE sp. z o.o.: fikcyjna spółka, na której wykonujemy ćwiczenia. Jej profil, architektura i podatności odwzorowują realia opisane w Części I.
- Część III — przebieg incydentu w NOVENERGII: oś czasu ćwiczeniowa, zbudowana na technikach z Części I.
- Część IV — mapa ćwiczeń: które dane z tego dokumentu są potrzebne w którym ćwiczeniu.

Zastrzeżenie: NOVENERGIA OZE sp. z o.o. jest spółką fikcyjną, utworzoną wyłącznie na potrzeby szkolenia. Wszelkie podobieństwo do istniejących podmiotów jest przypadkowe. Fakty z Części I pochodzą z publicznie dostępnego raportu CERT Polska „Raport z incydentu w sektorze energii 29.12” i zostały zacytowane w celu edukacyjnym. Elementy dodane na potrzeby ćwiczeń są w Części III wyraźnie oznaczone.

Część I. Tło faktyczne — incydent z 29 grudnia 2025 r.

Źródło: CERT Polska, „Raport z incydentu w sektorze energii 29.12”. CERT Polska to zespół działający w strukturach Naukowej i Akademickiej Sieci Komputerowej — Państwowego Instytutu Badawczego, jeden z trzech zespołów krajowych w ramach Krajowego Systemu Cyberbezpieczeństwa.

1. Co się wydarzyło

29 grudnia 2025 roku, w godzinach porannych i popołudniowych, doszło do skoordynowanych ataków w polskiej cyberprzestrzeni. Był to okres, w którym Polska zmagala się z niskimi temperaturami i zamieciami śnieżnymi, tuż przed Nowym Rokiem.

Ataki były wymierzone w trzy grupy celów:

- co najmniej 30 farm wiatrowych i fotowoltaicznych w Polsce,
- dużą elektrociepłownię dostarczającą ciepło dla blisko pół miliona odbiorców,
- prywatne przedsiębiorstwo z sektora produkcyjnego.

Wszystkie ataki miały cel wyłącznie destrukcyjny. Nie było żądania okupu ani kradzieży dla zysku. CERT Polska porównuje je — przez analogię do świata fizycznego — do celowych podpałów. Na podstawie analizy technicznej ustalono, że wszystkie ataki przeprowadził ten sam atakujący.

Zdarzenia miały wpływ zarówno na systemy informatyczne, jak i na fizyczne urządzenia przemysłowe — co jest rzadko spotykane w dotychczas opisywanych atakach. CERT Polska ocenia je jako znaczną eskalację w porównaniu ze zdarzeniami obserwowanymi wcześniej.

Skutek — i czego NIE było: Atak spowodował zerwanie komunikacji między obiektami a operatorami sieci dystrybucyjnej (OSD) i uniemożliwił zdalne sterowanie. Nie miał wpływu na bieżącą produkcję energii elektrycznej ani na stabilność krajowego systemu elektroenergetycznego. Należy jednak podkreślić: poziom dostępu uzyskanych przez atakującego stwarzał ryzyko spowodowania przestoju w produkcji.

2. Architektura farmy OZE i Główny Punkt Odbioru

Energia ze źródeł wiatrowych i fotowoltaicznych jest zbierana i kierowana do stacji elektroenergetycznej zwanej Głównym Punktem Odbioru (GPO). Wewnątrz stacji transformator podnosi napięcie do poziomu 110 kV, co umożliwia przekazanie mocy do sieci dystrybucyjnej. Cały proces jest objęty nadzorem i sterowaniem przez operatora sieci dystrybucyjnej.

GPO to obiekty zarządzane zdalnie, bez obsady na miejscu, w których powszechna jest możliwość zdalnego dostępu. Z perspektywy opisywanego ataku istotne są następujące elementy:

Element GPO	Funkcja
Sterownik RTU	Telemechanika i nadzór nad pracą stacji elektroenergetycznej
Lokalne HMI	Wizualizacja stanu pracy obiektu na podstawie danych z RTU
Sterowniki zabezpieczeń	Ochrona przed uszkodzeniami elektrycznymi
Serwery portów szeregowych	Podłączenie urządzeń RS232/RS485 i konwersja na protokoły szeregowo używane w komunikacji z OSD
Łącze podstawowe i zapasowe	Router komórkowy; połączenie z systemem SCADA operatora sieci dystrybucyjnej protokołem DNP3.0 lub IEC 101
Koncentrator VPN i firewall	Jedno urządzenie zapewniające zdalny dostęp serwisowy, segmentację sieci i ewentualne połączenie z SCADA

Zabezpieczenie systemowe, które zadziałało: Operatorzy sieci dystrybucyjnej wymagają, aby komunikacja między systemem SCADA operatora a GPO odbywała się wyłącznie łączem szeregowym, z wykorzystaniem protokołów DNP3.0 lub IEC 101. Takie rozwiązanie minimalizuje ryzyko wykorzystania ataku na GPO jako bezpośredniego wektora ataku na sieć teleinformatyczną operatora — i w tym incydencie zadziałało.

3. Wektor wejścia — ten sam we wszystkich obiektach

W każdym zaatakowanym obiekcie było obecne urządzenie brzegowe Fortigate pełniące funkcję koncentratora VPN oraz zapory sieciowej. W każdym przypadku:

- interfejs VPN był dostępny z sieci Internet,
- umożliwiał logowanie na konta zdefiniowane lokalnie w konfiguracji urządzenia,
- bez uwierzytelniania wieloskładnikowego.

W toku analizy ustalono, że w przeszłości niektóre z tych urządzeń, w różnych okresach, przez dłuższy czas były podatne — w tym na zdalne wykonanie kodu.

Dlaczego jeden obiekt otworzył trzydzieści: Z przeprowadzonego przez CERT Polska wywiadu wynika, że powszechną praktyką w branży jest wykorzystywanie tych samych kont i haseł w wielu obiektach. W takiej sytuacji przejęcie nawet jednego konta mogło pozwolić atakującemu na znalezienie innych urządzeń, w których było ono użyte.

Sieci badanych obiektów często posiadały wydzielone podsieci VLAN, ale atakujący w momencie ataku posiadał uprawnienia administratora urządzenia. Pozwoliło to pozyskać poświadczenia konta VPN z dostępem do

wszystkich podsieci — a nawet gdyby takiego konta nie było, uprawnienia administratora umożliwiały zmianę konfiguracji urządzeń.

Wszystkie badane urządzenia w dniu ataku zostały przywrócone do ustawień fabrycznych. Miało to prawdopodobnie cel destrukcyjny — utrudnić przywrócenie sprawności obiektu — ale służyło też zatarciu śladów. Z powodu tych działań nie udało się odzyskać pełnych logów z żadnego z zaatakowanych urządzeń.

4. Działania destrukcyjne — urządzenie po urządzeniu

W dniu 29 grudnia w każdym z obiektów rozpoczęto działania destrukcyjne na urządzeniach, do których atakujący uzyskał dostęp. Ataki w obrębie danej stacji były prawdopodobnie częściowo zautomatyzowane: urządzenia były uszkadzane w kolejności rosnącej po adresacji IP, a gdy atak nie powiódł się na jednym z adresów, nie był kontynuowany na kolejnych.

Urządzenie	Jak przejęte	Efekt destrukcyjny
Sterownik RTU Hitachi RTU560 (firmware 12.6.6.0 – 13.5.2.0)	Logowanie do interfejsu webowego na wbudowane konto „Default” z domyślnymi poświadczeniami. Konto to ma uprawnienia do zmiany firmware.	Wgranie uszkodzonego firmware: w miejscu startu programu wstawiono 240 bajtów 0xFF. Procesor wykonał nieprawidłową instrukcję → nieskończona pętla restartu urządzenia.
Sterownik RTU Mikronika (architektura Linux)	Logowanie przez konsolę SSH na konto z uprawnieniami root, z domyślnymi poświadczeniami.	Usunięcie wszystkich plików z systemu → awaria urządzenia. Na tych obiektach 25 grudnia 2025 r. odnotowano skanowanie sieci i próby logowania.
Sterowniki zabezpieczeń Hitachi Relion 650 v1.1	Domyślnie włączona usługa FTP dająca dostęp do plików systemowych; wbudowane konto z domyślnymi poświadczeniami.	Usunięcie plików niezbędnych do działania → błąd, wyłączenie urządzenia i brak możliwości ponownego uruchomienia.
Komputer HMI (Mikronika Syndis na Windows 10)	Domyślne hasło konta lokalnego administratora ustawione podczas wdrożenia; dostęp przez pulpit zdalny — bez prób zgadywania hasła.	8.12.2025 zmiany konfiguracji przez PowerShell (udziały administracyjne, reguła zapory „Microsoft Update” na porcie TCP 445), rekonesans pakietem Impacket. 29.12 rano utworzenie i uruchomienie pliku C:\Source.exe — wipera DynoWiper.
Serwery portów Moxa NPort 6xxx	Włączony interfejs webowy z domyślnym loginem i hasłem.	Przywrócenie do ustawień fabrycznych, zmiana hasła logowania i ustawienie adresu IP na nieosiągalny (np. 127.0.0.1) — w celu opóźnienia przywrócenia sprawności. Celem były wszystkie urządzenia Moxa na obiekcie.

Trzy zabezpieczenia, które by wystarczyły: (1) Funkcja secure update w sterownikach RTU, sprawdzająca podpis wgrzanego firmware, była dostępna od wersji 13.2.1 — ale wymagała włączenia i na żadnym urządzeniu nie została włączona. (2) Gdyby sterowniki zabezpieczeń wdrożono zgodnie z zaleceniami producenta, domyślne konto FTP zostałoby automatycznie zablokowane. (3) Tam, gdzie na komputerach HMI ustawiono inne hasło niż domyślne, widać nieskuteczne próby jego przełamania — te komputery nie zostały uszkodzone.

5. Atak na elektrociepłownię — długotrwała infiltracja

Celem sabotażu było nieodwracalne uszkodzenie danych w sieci wewnętrznej podmiotu przez uruchomienie oprogramowania typu wiper. Destrukcyjny atak poprzedzony był długotrwałą infiltracją infrastruktury oraz kradzieżą wrażliwych informacji dotyczących działania podmiotu.

Faza pierwsza: marzec – lipiec 2025

- Pierwsze działania atakującego odnotowano w okresie marzec – maj 2025. Dostęp do maszyny przesiadkowej przez pulpit zdalny, z adresu przypisanego do interfejsu urządzenia brzegowego Fortigate. Z tej maszyny atakujący łączył się do kolejnych, w tym do kontrolera domeny.
- Rekonesans: narzędzie nircmd do wykonywania rzutów ekranu, PsExec do zdalnego uruchamiania poleceń, zapisywanie do pliku outlog.txt listy procesów, połączeń sieciowych, tablic routingu, pamięci ARP i zawartości katalogów użytkowników.
- Szczególne zainteresowanie systemami automatyki przemysłowej — większość systemów przeglądanych przez SMB miała w nazwie słowo „scada”. Działania prowadzono w zdecydowanej większości w godzinach pracy biurowej.
- Eskalacja uprawnień: rzut pamięci procesu LSASS, użycie narzędzia Rubeus do ataku na protokół Kerberos i stworzenia biletu typu Diamond Ticket, a w drugiej połowie lipca rzut całej bazy Active Directory (plik ntds.dit).

Faza druga: koniec 2025 r.

- Dostęp przez usługę SSL-VPN portal urządzenia Fortigate, przy użyciu wielu kont zdefiniowanych statycznie w konfiguracji i bez uwierzytelniania dwuskładnikowego. Połączenia przez węzły sieci TOR oraz z polskich i zagranicznych adresów IP, często będących przejętą infrastrukturą.
- Wykorzystanie zakładek (bookmarks) zdefiniowanych w konfiguracji urządzenia — niektóre z nich miały statycznie ustawione poświadczenia użytkownika docelowego, co umożliwiało połączenie do maszyny przesiadkowej bez podawania dodatkowych danych logowania.
- Tunelowanie ataków przez Reverse SOCKS Proxy (narzędzie rsocx pod nazwami r.exe i rsocx.exe) do serwera kontrolowanego przez atakującego.
- Rekonesans narzędziami systemowymi (nslookup, ping) oraz skanerami Advanced Port Scanner i Advanced IP Scanner. Wykorzystanie przeglądarki w trybie prywatnym do pobierania plików z dysku chmurowego i serwisu pastebin.
- Kradzież rejestrów SAM i SYSTEM poleceniem reg, kopii Shadow partycji C poleceniem vssadmin w celu wykradzenia bazy Active Directory, a następnie próba przesłania skompresowanych danych przez PowerShell do serwera atakującego.
- Kradzież plików konfiguracyjnych kilku urządzeń Fortigate oraz modyfikacja konfiguracji urządzenia brzegowego: dodanie reguły zezwalającej na połączenia dowolnym protokołem z dowolnego adresu IP do określonego urządzenia, z wyłączonym logowaniem ruchu. Nazwa reguły imitowała nazwę instytucji już występującą w konfiguracji.

29 grudnia w godzinach porannych atakujący uzyskał dostęp do portalu SSL-VPN, połączył się przez pulpit zdalny do maszyny przesiadkowej, a z niej do kontrolera domeny, gdzie utworzył archiwum zawierające plik wipera. Wiper został umieszczony na zasobie sieciowym dostępnym dla innych komputerów, a następnie uruchomiony przy użyciu dodatkowej polityki GPO.

Co uratowało elektrociepłownię: Plik wykonywalny nie został wykryty przez oprogramowanie antywirusowe. Jego wykonanie zostało jednak zablokowane w trakcie działania przez oprogramowanie klasy EDR — poprzez mechanizm kanarków, czyli plików, które w momencie rozpoczęcia modyfikacji ich zawartości podnoszą alarm. Zatrzymało to nadpisywanie danych na ponad 100 maszynach. Odnotowano również próbę rekonfiguracji macierzy RAID jednego z serwerów.

6. Atak na przedsiębiorstwo produkcyjne — persystencja na urządzeniu brzegowym

Tego samego dnia atakujący podjął próbę zakłócenia funkcjonowania przedsiębiorstwa z sektora produkcyjnego. Działania były skoordynowane z atakami na sektor energetyczny, ale cel miał charakter oportunistyczny.

- Dostęp początkowy: urządzenie brzegowe Fortinet, które było w przeszłości podatne, a jego konfiguracja została wykradziona i opublikowana m.in. w poście na forum wykorzystywanym przez środowiska przestępcze.

- Persystencja: atakujący wykorzystał wbudowany w urządzenie mechanizm skryptów. Utworzył trzy skrypty wykonywane co tydzień — do odczytu hasła uprzywilejowanego użytkownika, do modyfikacji ustawień bezpieczeństwa oraz do przesyłania wyników na kontrolowany przez siebie kanał w komunikatorze Slack (Fortigate ma wbudowaną funkcję powiadomień Slack).
- Wszystkie trzy skrypty były widoczne w panelu konfiguracyjnym urządzenia, w zakładce zaplanowanych zadań.
- Dalszy przebieg: tunel SSL-VPN, poruszanie się po sieci pakietem Impacket, dostęp do kontrolera domeny z uprawnieniami administratora i dystrybucja wipera tą samą metodą co w elektrociepłowni — przez politykę GPO. Sam wiper był tu napisany w języku PowerShell (LazyWiper).

7. Działania przeciwko usługom chmurowym

Atakujący wykorzystywał dane uwierzytelniające pozyskane ze środowiska lokalnego do prób uzyskania dostępu do usług chmurowych. Po znalezieniu poświadczeń, dla których istniało odpowiadające im konto w usłudze Microsoft 365, pobierał wybrane dane z usług Exchange, Teams i SharePoint.

Atakujący był zainteresowany przede wszystkim plikami i wiadomościami e-mail dotyczącymi modernizacji sieci OT, systemów SCADA oraz prac technicznych prowadzonych w podmiotach. Próbował również poszerzyć uprawnienia, korzystając z błędnie skonfigurowanych uprawnień w środowisku chmurowym.

8. Złośliwe oprogramowanie i atrybucja

Użyto dwóch kategorii oprogramowania niszczącego dane, których nie udało się dopasować do żadnej istniejącej rodziny: DynoWiper (skompilowany plik wykonywalny, występujący w dwóch wersjach) oraz LazyWiper (napisany w języku PowerShell). Celem obu była nieodwracalna destrukcja danych, bez próby wymuszania okupu.

CERT Polska ustalił, że infrastruktura użyta do uzyskania początkowego dostępu, kradzieży danych i zestawienia tuneli VPN pokrywa się z klastrem aktywności znanym publicznie jako „Static Tundra” (Cisco), „Berserk Bear” (CrowdStrike), „Ghost Blizzard” (Microsoft) oraz „Dragonfly” (Symantec). Publiczne opisy działań tego aktora wskazują na duże zainteresowanie sektorem energetyki oraz zdolności w atakowaniu urządzeń przemysłowych.

Jest to pierwsza publicznie opisana aktywność o charakterze destrukcyjnym przypisywana do tego klastra.

Atakujący korzystał m.in. z przejętych serwerów VPS oraz przejętych routerów jako infrastruktury anonimizującej.

Wniosek metodyczny: Żaden z mechanizmów użytych w tym ataku nie wymagał wiedzy niedostępnej publicznie ani podatności typu zero-day. Domyślne poświadczenia, brak uwierzytelniania wieloskładnikowego, niewłączone funkcje bezpieczeństwa dostępne w urządzeniach, współdzielone hasła między obiektami i brak analizy logów. Każdy z tych punktów jest wprost adresowany przez art. 8 ustawy o krajowym systemie cyberbezpieczeństwa — i każdy da się zamknąć bez znaczącej inwestycji.

Część II. NOVENERGIA OZE sp. z o.o. — organizacja ćwiczebna

Spółka fikcyjna. Profil, struktura właścicielska, architektura techniczna i stan zgodności zostały zbudowane tak, aby odwzorowywać realia opisane w Części I. Na tych danych wykonujemy wszystkie sześć ćwiczeń.

1. Dane rejestrowe i profil działalności

Firma	NOVENERGIA OZE spółka z ograniczoną odpowiedzialnością
Siedziba	Płock, województwo mazowieckie
Rok rozpoczęcia działalności	2014
Forma prawna	Spółka z ograniczoną odpowiedzialnością, spółka dominująca w grupie
Przedmiot działalności	Wytwarzanie energii elektrycznej ze źródeł odnawialnych; sprzedaż energii; usługi utrzymania i serwisu farm dla podmiotów trzecich

Kody PKD ujawnione w KRS	35.11.Z — wytwarzanie energii elektrycznej 35.14.Z — handel energią elektryczną 33.14.Z — naprawa i konserwacja urządzeń elektrycznych 62.09.Z — pozostała działalność usługowa w zakresie technologii informatycznych i komputerowych
Majątek produkcyjny	5 farm fotowoltaicznych i 1 farma wiatrowa; łączna moc zainstalowana 180 MW; 6 Głównych Punktów Odbioru
Odbiorcy	Sprzedaż na rynku hurtowym; umowy bilateralne z trzema odbiorcami przemysłowymi

Uwaga: czwarty kod PKD (62.09.Z) został ujawniony w 2022 r., gdy spółka zaczęła świadczyć usługi zdalnego monitorowania parametrów pracy farm dla dwóch niezależnych właścicieli instalacji fotowoltaicznych. Usługa działa do dziś i obejmuje dostęp do systemów sterowania tych podmiotów.

2. Struktura grupy i dane wielkościowe

Podmiot	Udział	Zatrudnienie (EPC)	Obrót za 2025 r.
NOVENERGIA OZE sp. z o.o. (spółka 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 rokiem kalendarzowym; sprawozdanie za 2025 r. zostało zatwierdzone przez zgromadzenie wspólników 12 czerwca 2026 r. Wartości w euro przeliczone według kursu ogłoszonego przez Narodowy Bank Polski.

3. Usługi i procesy krytyczne

Proces	Wspierające systemy	Skutek przerwania
Wytwarzanie i oddawanie energii do sieci	Sterowniki RTU w GPO, systemy zabezpieczeń, łączą do OSD	Utrata zdolności oddawania mocy; ryzyko kar bilansujących
Zdalny nadzór i sterowanie farmami	SCADA, HMI, telemetria, serwery portów szeregowych	Brak zdalnego sterowania; konieczność obsługi ręcznej na obiektach
Rozliczenia i sprzedaż energii	System bilingowy, poczta w chmurze, arkusze handlowe	Opóźnienia rozliczeń; ryzyko kar umownych
Usługa monitorowania dla podmiotów trzecich (PKD 62.09.Z)	Ta sama platforma SCADA, dostęp VPN do instalacji klientów	Utrata usługi u dwóch klientów zewnętrznych; ryzyko przeniesienia incydentu
Serwis i utrzymanie techniczne	System zgłoszeń, dostęp zdalny integratora	Wydłużenie czasu napraw; brak wsparcia producenta

4. Architektura IT i OT — rejestr aktywów

Aktywo	Lokalizacja	Opis	Stan zabezpieczeń
Urządzenie brzegowe Fortigate (6 szt., po jednym na obiekt)	Każdy GPO	Koncentrator VPN i zaporą; zdalny dostęp serwisowy dla integratora i dla działu utrzymania	Interfejs SSL-VPN dostępny z Internetu; konta lokalne bez MFA; te same poświadczenia na wszystkich sześciu obiektach
Sterownik RTU (6 szt.)	Każdy GPO	Telemechanika, komunikacja z OSD protokołem DNP3.0	Konto producenta z domyślnym hasłem nigdy niezmienione; funkcja weryfikacji podpisu firmware niewłączona
Sterowniki zabezpieczeń (12 szt.)	Każdy GPO	Zabezpieczenia polowe	Usługa FTP włączona domyślnie; konto wbudowane aktywne
Komputery HMI (6 szt., Windows 10)	Każdy GPO	Wizualizacja stanu pracy obiektu	Hasło lokalnego administratora ustawione przez integratora przy wdrożeniu, identyczne na wszystkich obiektach; brak EDR
Serwery portów szeregowych (18 szt.)	Każdy GPO	Konwersja RS485 na komunikację z OSD	Interfejs webowy włączony, domyślny login i hasło
Serwer SCADA	Centrala, Płock	Zbieranie telemetry ze wszystkich obiektów i usług dla klientów zewnętrznych	W tej samej domenie Active Directory co sieć biurowa; brak segmentacji IT–OT
Kontroler domeny Active Directory (2 szt.)	Centrala	Uwierzytelnianie w sieci biurowej i na serwerze 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 brak kopii niemodyfikowalnej
Usługa poczty i pakiet biurowy w chmurze	Chmura publiczna	Poczta, dokumenty, komunikator	MFA włączone dla 60 % kont; brak przeglądu uprawnień administracyjnych
System bilingowy	Centrala	Rozliczenia sprzedaży energii	Dostęp przez konta domenowe; brak rejestru uprawnień

5. Dostawcy i podmioty zewnętrzne

Dostawca	Rodzaj usługi	Dostęp i stan umowy
ELEKTROSERWIS TECHNIKA sp. z o.o.	Integrator systemów 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

Dostawca	Rodzaj usługi	Dostęp i stan umowy
NET-KOM sp. z o.o.	Dostawca łączy i utrzymanie urządzeń brzegowych	Zdalna administracja urządzeniami Fortigate; brak wymogu zgłaszania incydentów
Dostawca chmury publicznej	Poczta, dokumenty, komunikator	Umowa standardowa, regulamin dostawcy; brak indywidualnych klauzul; brak ustalonego planu wyjścia
BIURO IT PARTNER s.c.	Obsługa informatyczna sieci biurowej	Konta administratora domeny; umowa zawiera klauzulę poufności, nie zawiera wymagań bezpieczeństwa
Producent sterowników RTU	Wsparcie techniczne i firmware	Kontakt wyłącznie przez zgłoszenia serwisowe; brak subskrypcji powiadomień o podatnościach

6. Ludzie i role

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

7. Stan zgodności na 1 grudnia 2025 r.

Obszar	Stan	Szczegóły
Ustalenie statusu podmiotu kluczowego lub ważnego	BRAK	Temat nigdy nie był przedmiotem analizy ani posiedzenia zarządu
Wniosek o wpis do wykazu w systemie S46	BRAK	Nie złożono; nikt nie ma konta w systemie
Osoba odpowiedzialna za cyberbezpieczeństwo	CZĘŚCIOWO	Kierownik IT pełni tę funkcję nieformalnie, bez powołania i bez zakresu obowiązków
Polityka bezpieczeństwa informacji	NIEAKTUALNA	Dokument z 2019 r., przygotowany na potrzeby przetargu, nigdy nieaktualizowany i niedystrybuowany

Obszar	Stan	Szczegóły
Analiza ryzyka i rejestr ryzyk	BRAK	Nigdy nie przeprowadzono
Uwierzytelnianie wieloskładnikowe	CZĘŚCIOWO	Włączone dla 60 % kont w usłudze chmurowej; brak na dostępie VPN i na kontach administracyjnych
Zarządzanie podatnościami	BRAK	Brak skanowania; aktualizacje urządzeń OT wyłącznie przy okazji wizyt serwisowych
Segmentacja sieci IT i OT	BRAK	Serwer SCADA w tej samej domenie co sieć biurowa; brak zapory segmentacyjnej
Monitorowanie systemów	CZĘŚCIOWO	Monitoring 8x5 realizowany przez dwuosobowy dział IT; logi zbierane lokalnie na urządzeniach, bez centralizacji
Procedura zarządzania incydentami	CZĘŚCIOWO	Dokument istnieje jako załącznik do polityki z 2019 r., nigdy nieprzećwiczony; nie wskazano właściwego CSIRT
Kopie zapasowe i testy odtworzeniowe	CZĘŚCIOWO	Kopie wykonywane codziennie na serwer NAS w tej samej domenie; ostatni test odtworzenia: marzec 2023 r.
Plan ciągłości działania	CZĘŚCIOWO	Plan opracowany w 2021 r. na potrzeby ubezpieczyciela; brak parametrów RTO i RPO; nigdy nietestowany
Ocena ryzyka dostawców	BRAK	Brak rejestru dostawców ICT; umowy bez klauzul bezpieczeństwa
Szkolenia kierownictwa	BRAK	Nie prowadzono
Weryfikacja niekaralności personelu	BRAK	Nie prowadzona ani wobec pracowników, ani wobec personelu integratora

Część III. Przebieg incydentu w NOVENERGII

Oznaczenie: Oś czasu poniżej jest elementem ćwiczeniowym. Techniki i mechanizmy odwzorowują raport CERT Polska z Części I; daty, godziny i reakcje organizacji zostały dobrane na potrzeby ćwiczeń — zwłaszcza opóźnienie zgłoszenia, którego raport CERT Polska nie opisuje.

Data i godzina	Etap	Co się wydarzyło
ok. 20.11.2025	Przygotowanie	Skanowanie internetowych adresów spółki z zagranicznego adresu IP. Zdarzenie zarejestrowane w logach urządzenia brzegowego, nikt ich nie przeglądał.
08.12.2025, 21:14	Dostęp wstępny	Logowanie do interfejsu SSL-VPN urządzenia brzegowego na GPO nr 3, na konto serwisowe integratora, bez MFA. Poświadczenia identyczne na wszystkich sześciu obiektach.

Data i godzina	Etap	Co się wydarzyło
08.12.2025, 21:40	Utrwalenie dostępu	Dostęp przez pulpit zdalny do komputera HMI na koncie lokalnego administratora. Zmiany konfiguracji przez PowerShell: włączenie udziałów administracyjnych i utworzenie reguły zapory o nazwie „Microsoft Update” na porcie TCP 445.
09–24.12.2025	Rekonesans	Poruszanie się między obiektami. Zrzuty ekranu komputerów operatorskich. Wylistowanie zasobów serwera NAS. Dostęp do skrzynki pocztowej kierownika utrzymania i pobranie dokumentacji powykonawczej GPO oraz harmonogramu prac serwisowych.
25.12.2025, 03:20	Rozpoznanie OT	Skanowanie sieci obiektowych i próby logowania na sterownikach RTU oraz serwerach portów szeregowych. Zdarzenia zapisane w logach urządzeń; brak monitorowania w dni świąteczne.
27.12.2025	Eskalacja	Zrzut pamięci procesu uwierzytelniania na stacji roboczej administratora IT i pozyskanie poświadczeń konta z uprawnieniami administratora domeny. Kopia bazy Active Directory.
29.12.2025, 07:40	Destrukcja — OT	Na wszystkich sześciu obiektach: wgranie uszkodzonego firmware na sterowniki RTU, usunięcie plików systemowych na sterownikach zabezpieczeń, przywrócenie 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 oraz na serwerze SCADA. Podjęcie próby uruchomienia go na stacjach roboczych w centrali przez politykę GPO — brak oprogramowania klasy EDR, więc 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 od dyspozytora operatora sieci dystrybucyjnej: brak telemetrii z czterech farm. Dyżurny operator przyjmuje zgłoszenie i traktuje je jako awarię łącza.
29.12.2025, 08:20	Weryfikacja	Dyżurny inżynier potwierdza brak zdalnego sterowania na wszystkich obiektach i brak dostępu do urządzeń brzegowych. Powiadamia kierownika utrzymania.
29.12.2025, 09:30	Diagnostyka	Kierownik utrzymania kontaktuje się z integratorem. Wstępna hipoteza: awaria zasilania i uszkodzenie sprzętu. Wyjazd ekipy serwisowej na obiekty.
29.12.2025, 14:10	Rozpoznanie charakteru zdarzenia	Serwisant stwierdza, że sterowniki mają wgrane oprogramowanie w wersji, która nigdy nie była instalowana w spółce, a serwery portów mają zmienione hasła. Informacja trafia do kierownika IT.
29.12.2025, 16:45	Eskalacja wewnętrzna	Kierownik IT informuje członka zarządu ds. technicznych. Zapada decyzja o „przeanalizowaniu sprawy po świątach”.
30.12.2025, 11:00	Decyzja	Prezes zarządu dowiaduje 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.

Skutki i koszty

- 9 dni ograniczonego nadzoru nad farmami; konieczność obsługi ręcznej na obiektach i całodobowych dyżurów wyjazdowych.

- Utrata telemetrii wykorzystywanej do rozliczeń — konieczność rozliczenia szacunkowego i sporu z odbiorcami.
- Przerwa w świadczeniu usługi monitorowania dla dwóch klientów zewnętrznych; jeden z nich wypowiedział umowę.
- Koszt odtworzenia infrastruktury: wymiana lub przeprogramowanie 6 sterowników RTU, 12 sterowników zabezpieczeń i 18 serwerów portów; rekonfiguracja 6 urządzeń brzegowych.
- Brak możliwości pełnego ustalenia przebiegu ataku z powodu utraty logów — sprawozdanie końcowe do CSIRT niekompletne.
- Zapytanie od operatora sieci dystrybucyjnej o status podmiotu w wykazie podmiotów kluczowych i ważnych oraz o posiadane certyfikaty.

Część IV. Mapa ćwiczeń

Poniższa tabela wskazuje, które rozdziały tego dokumentu są potrzebne w którym ćwiczeniu. Proszę mieć dokument otwarty przez cały dzień.

Ćwiczenie	Zadanie	Dane wejściowe	Moduł
Nr 1	Samoidentyfikacja — ustalenie statusu podmiotu	Część II, rozdz. 1 i 2	Moduł 1
Nr 2	Macierz odpowiedzialności RACI dla 10 obszarów art. 8	Część II, rozdz. 6 i 7	Moduł 2
Nr 3	Rejestr ryzyk	Część II, rozdz. 3, 4 i 5; Część I, rozdz. 3 i 4	Moduł 3
Nr 4	Analiza luk wobec wymagań UoKSC	Część II, rozdz. 7	Moduł 3
Nr 5	Pierwsze 24 godziny od uzyskania wiedzy o incydencie	Część III w całości	Moduł 4
Nr 6	Plan naprawczy na 90 dni	Wynik ćwiczeń 3 i 4	Moduł 5

Druga część każdego ćwiczenia: W każdym ćwiczeniu po wykonaniu zadania na danych NOVENERGII przechodzimy do tej samej pracy na Państwa własnej organizacji. Pierwsza część uczy metody, druga daje wynik, który zabierają Państwo ze sobą. Proszę więc mieć pod ręką odpis z KRS swojej spółki oraz — jeżeli to możliwe — dane o zatrudnieniu i obrocie za ostatni zatwierdzony rok obrotowy.