Cyberbezpieczeństwo infrastruktury krytycznej.

Lekcje z incydentów w systemach automatyki.

Analiza ataków z grudnia 2025 r. i nowe standardy zabezpieczeń.

MIKRONIKA

Energia pod Twoją kontrolą

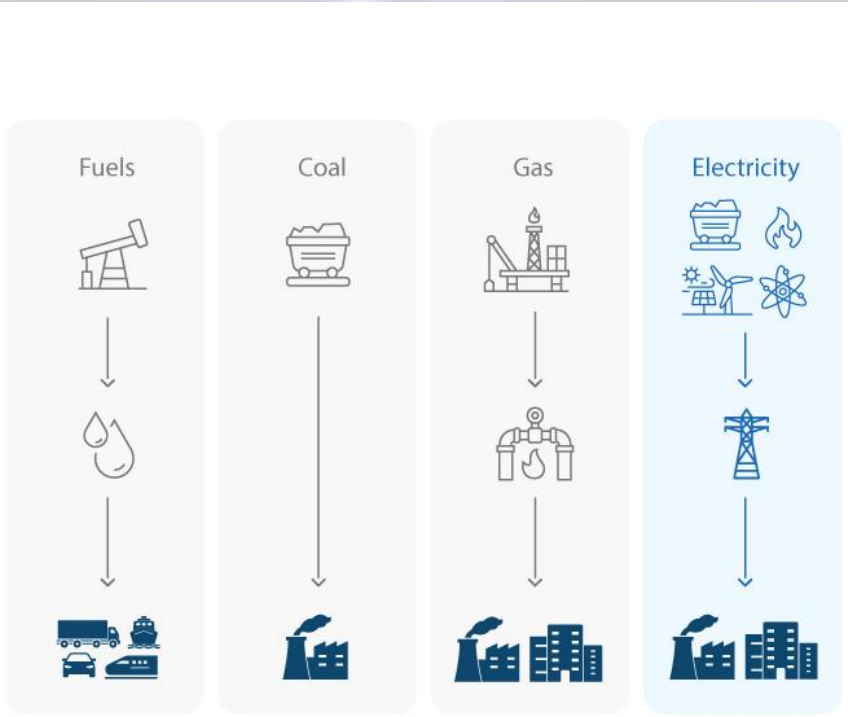
Tomasz Szała

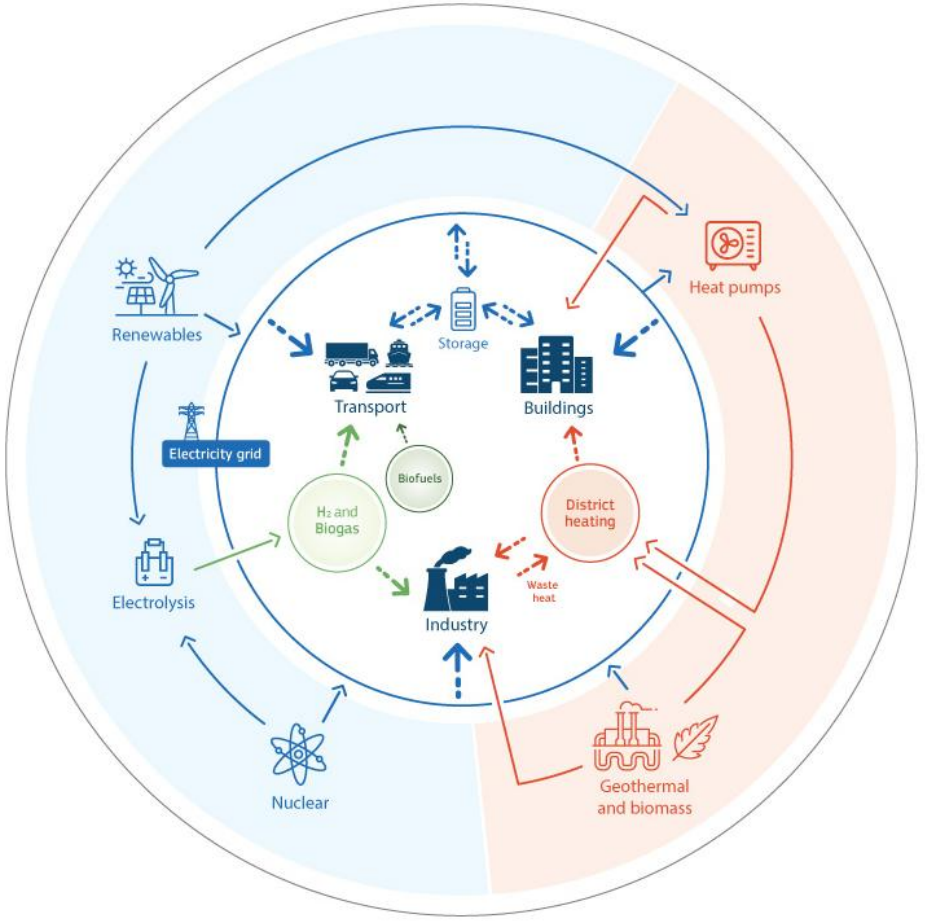
Poznań, 16 czerwca 2026

Po co zajmować się (cyber)bezpieczeństwem?

Transformacja energetyczna i znaczenie OZE w systemie energetycznym

wczoraj

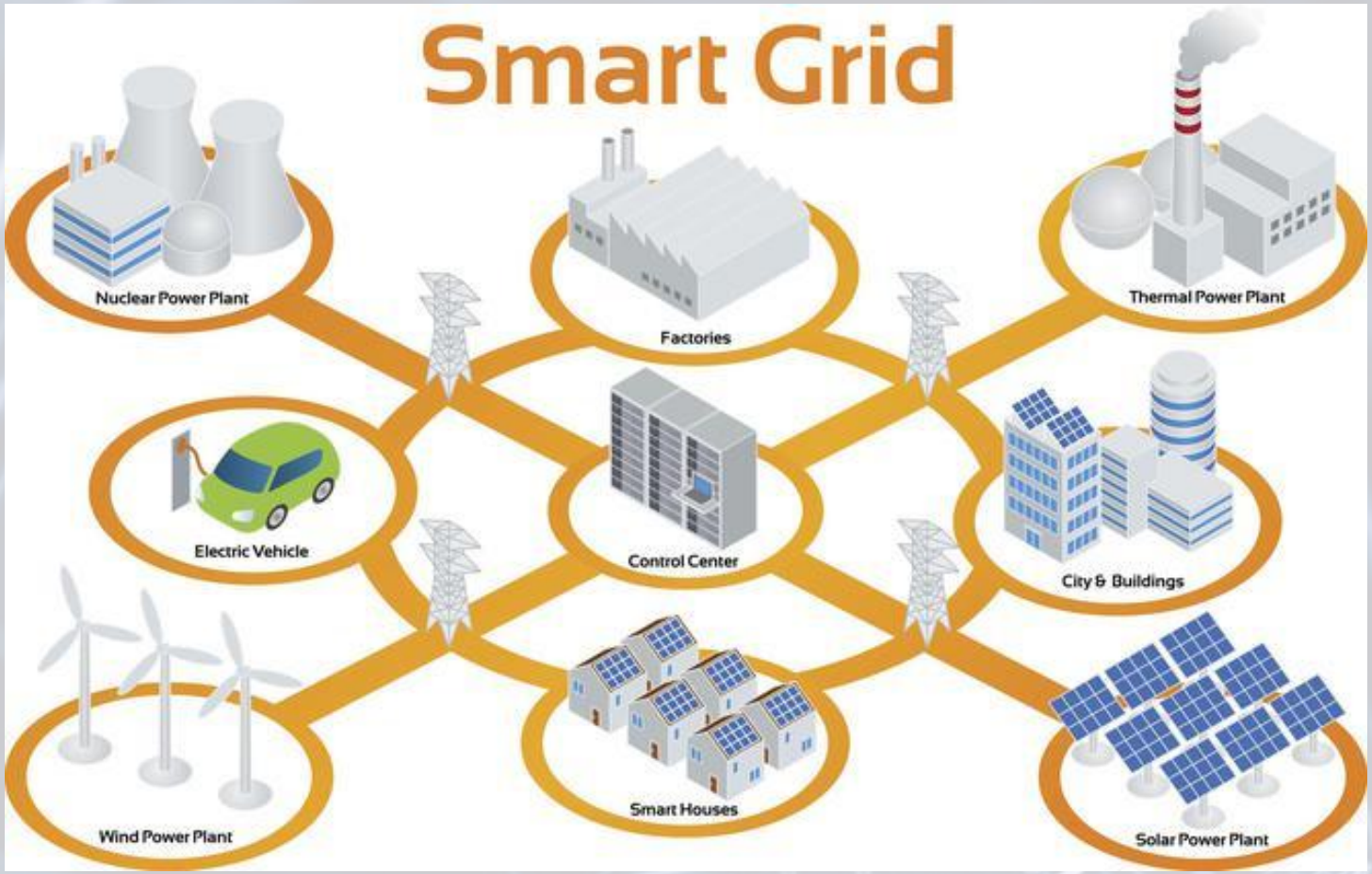




jutro

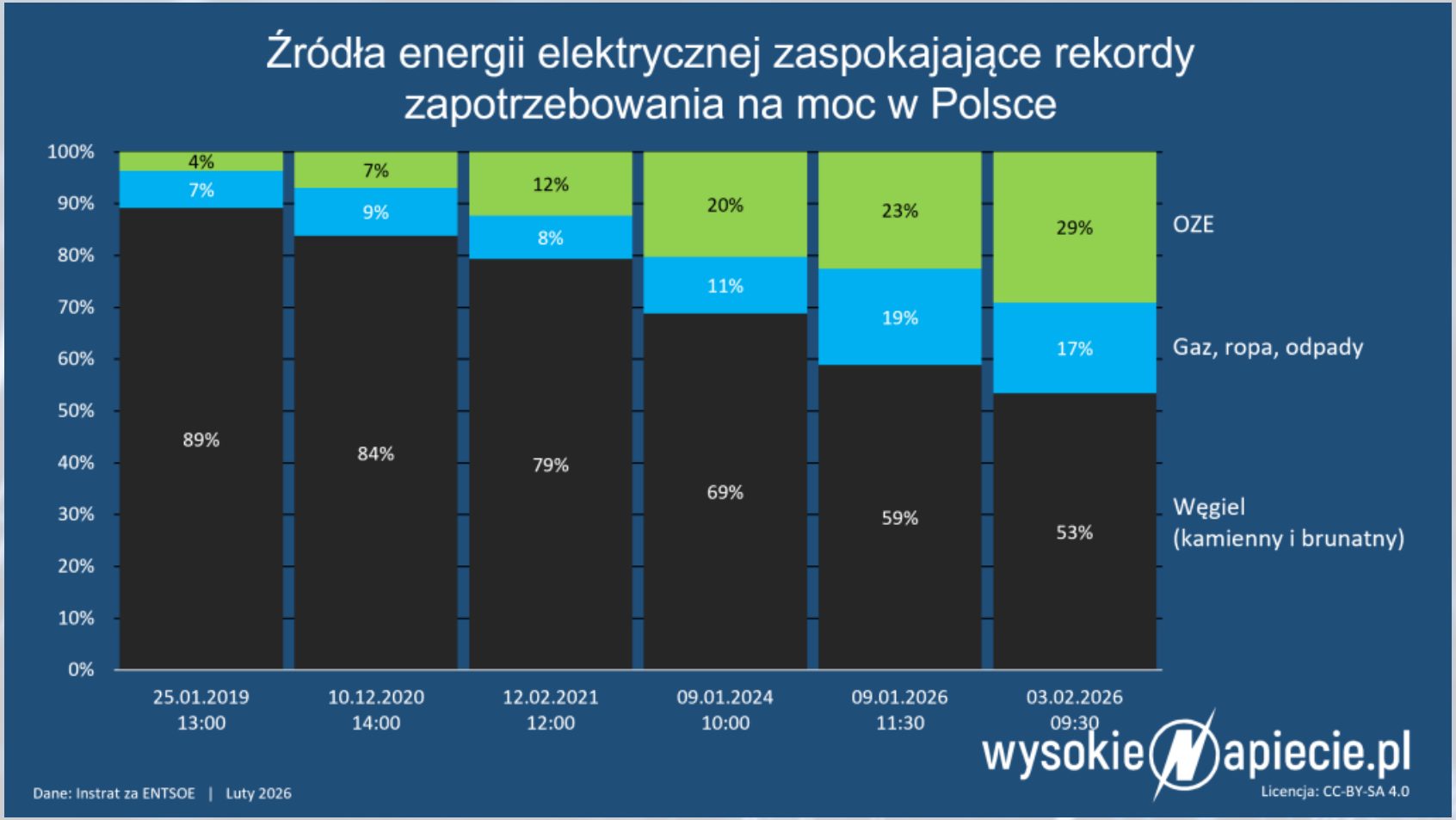
źródło EU strategy on energy system integration, Komisja Europejska

Znaczenie OZE w systemie energetycznym

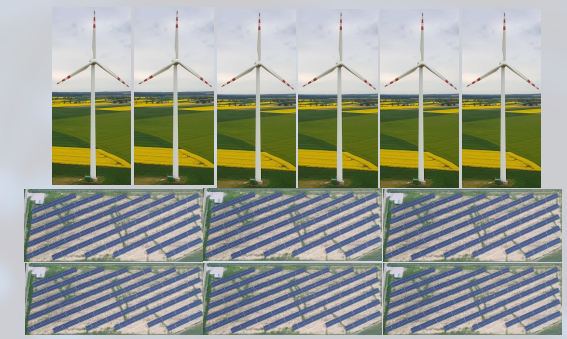


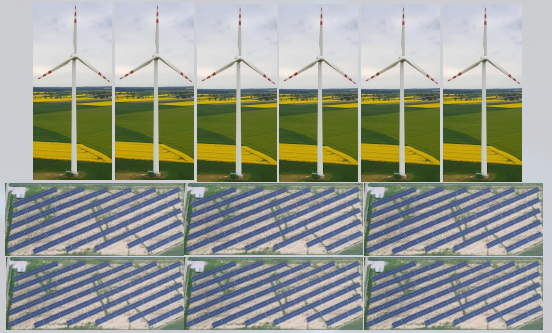
autor: Getty ImagesInteligentna sieć elektroenergetyczna, tzw. Smart Gird

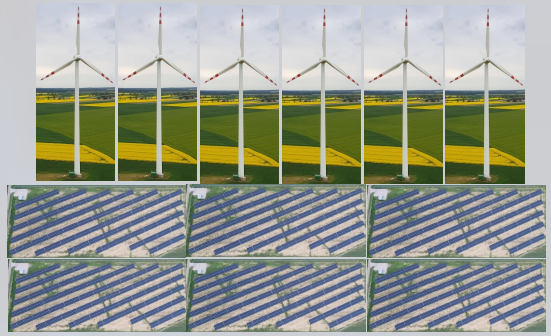
Znaczenie OZE w systemie energetycznym

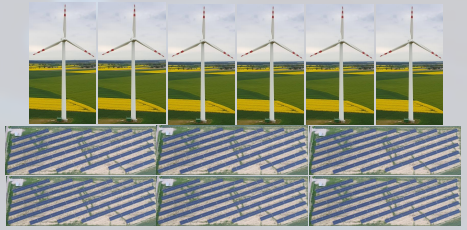


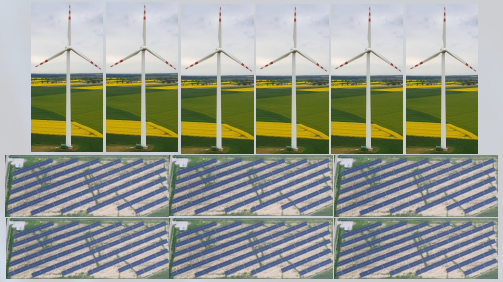
Znaczenie OZE w systemie energetycznym

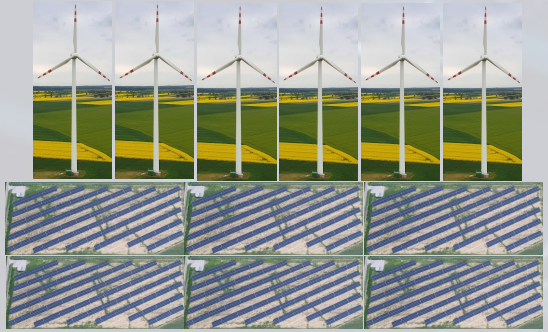


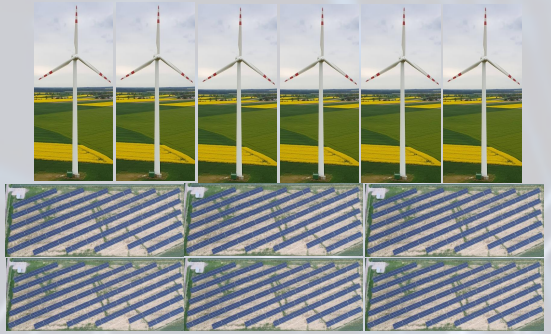


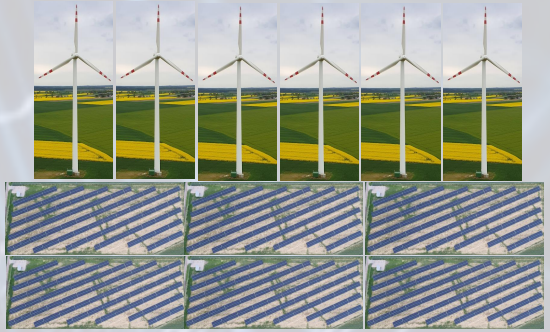












Co się stało w grudniu 2025?

Co się stało w grudniu 2025?

Cyberatak na polską energetykę. Trop wiedzie do Rosji

ESET wskazał, że atak z 29–30 grudnia na polską infrastrukturę energetyczną przeprowadzili hakerzy z rosyjskiej grupy Sandworm. Według firmy, nie odnotowano skutecznych zakłóceń działania sieci.

Źródło zdjęć: © East News

Potężny cyberatak na Polskę. Gawkowski: byliśmy blisko blackoutu

Krzysztof Gawkowski poinformował, że pod koniec grudnia Polska zmierzyła się z "najpoważniejszym atakiem na infrastrukturę energetyczną" ze strony Rosji. Według relacji ministra cyfryzacji, mało brakowało, a doszłoby do blackoutu.

2026-01-13, 20:24

Udostępnij

Minister cyfryzacji poinformował o rosyjskim cyberataku na infrastrukturę energetyczną, do którego doszło pod koniec grudnia Foto: Marysia Zawada/REPORTER

Next • Technologie • Minister ujawnia. Ogromny cyberatak pod koniec roku. "Największy od lat"

Minister ujawnia. Ogromny cyberatak pod koniec roku. "Największy od lat"

Tomasz Kilian
13 stycznia 2026, 12:52

Jak poinformował minister energii Miłosz Motyka, pod koniec 2025 roku nasiliły się ataki cybernetyczne na krajową infrastrukturę elektroenergetyczną. Szef resortu podkreślił jednak, że ataki zostały skutecznie odparte.

Agencja Wyborcza.pl

MIKRONIKA

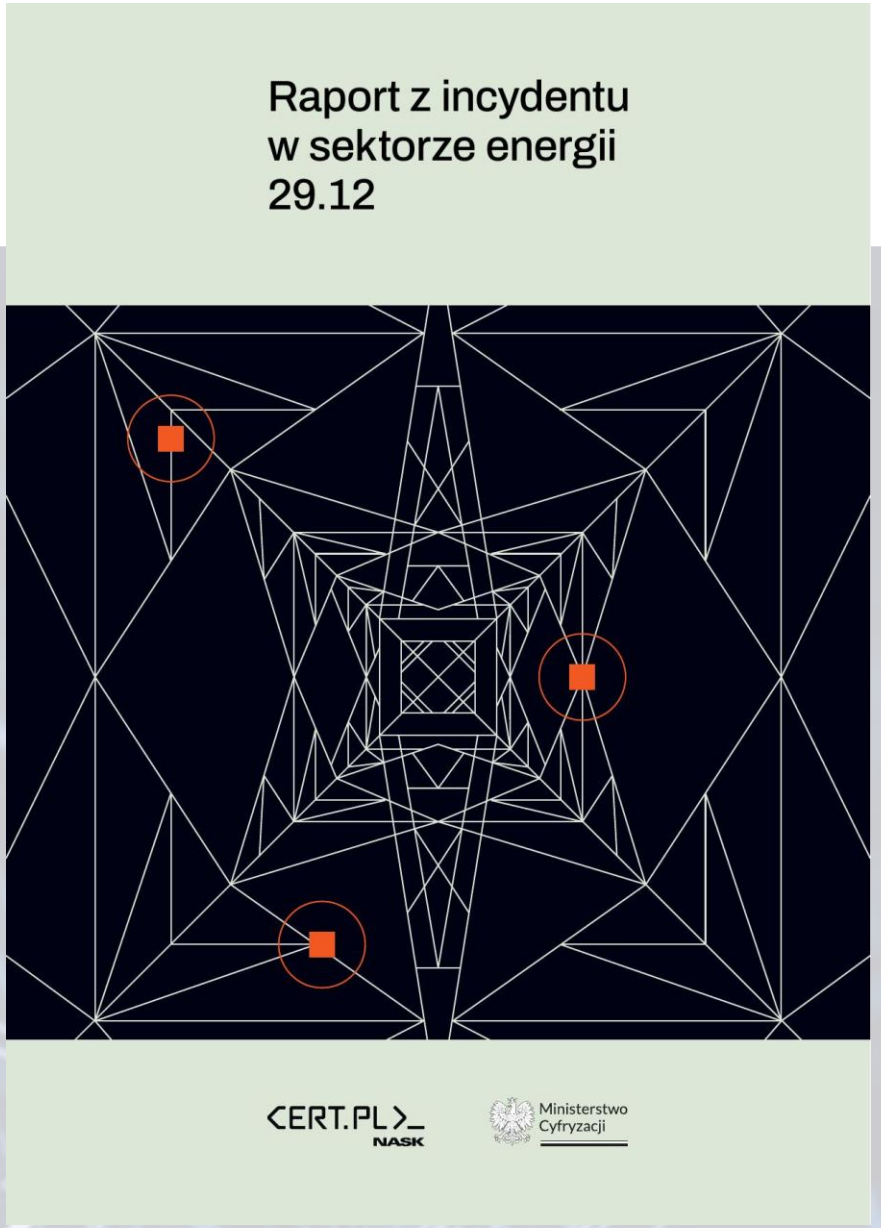
Poznań, 16.06.2026r.

Co się stało w grudniu 2025?

Wg raportu CERT Polska:

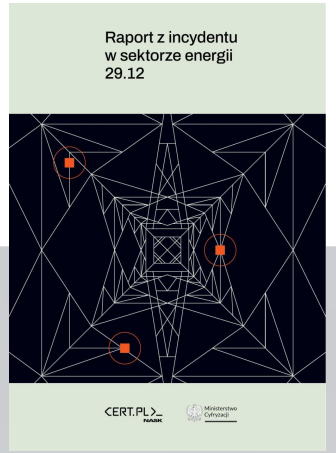
- atak był skoncentrowany na GPO obsługujące kilkadziesiąt (co najmniej 30) farm wiatrowych i PV.
- zaatakowana została duża elektrociepłownia (prawie pół miliona odbiorców)

*Farm było więcej i jeszcze jedna elektrociepłownia**



Co się stało w grudniu 2025?

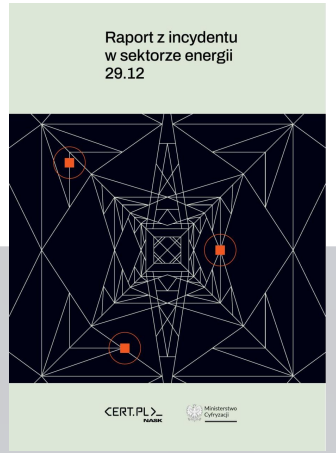
- Scenariusz ataku
  - Fortigate (firewall z VPN)
    - luki bezpieczeństwa i brak aktualizacji,
    - standardowe lub znane konta i hasła,
    - bezpośredni dostęp z sieci Internet,
    - skasowanie konfiguracje i logi (ustawienia fabr.).
  - Płaska sieć – czyli po wejściu „widzę wszystko”.
  - Standardowe konta i hasła do usług na urządzeniach obiektowych (serwery portów, sterowniki komunikacyjne itd.).
  - Wykonanie poleceń kasujących dane z urządzeń tak głęboko jak się da i następnie restart urządzenia. Takie urządzenia już się nie uruchomią.



Co się stało w grudniu 2025?

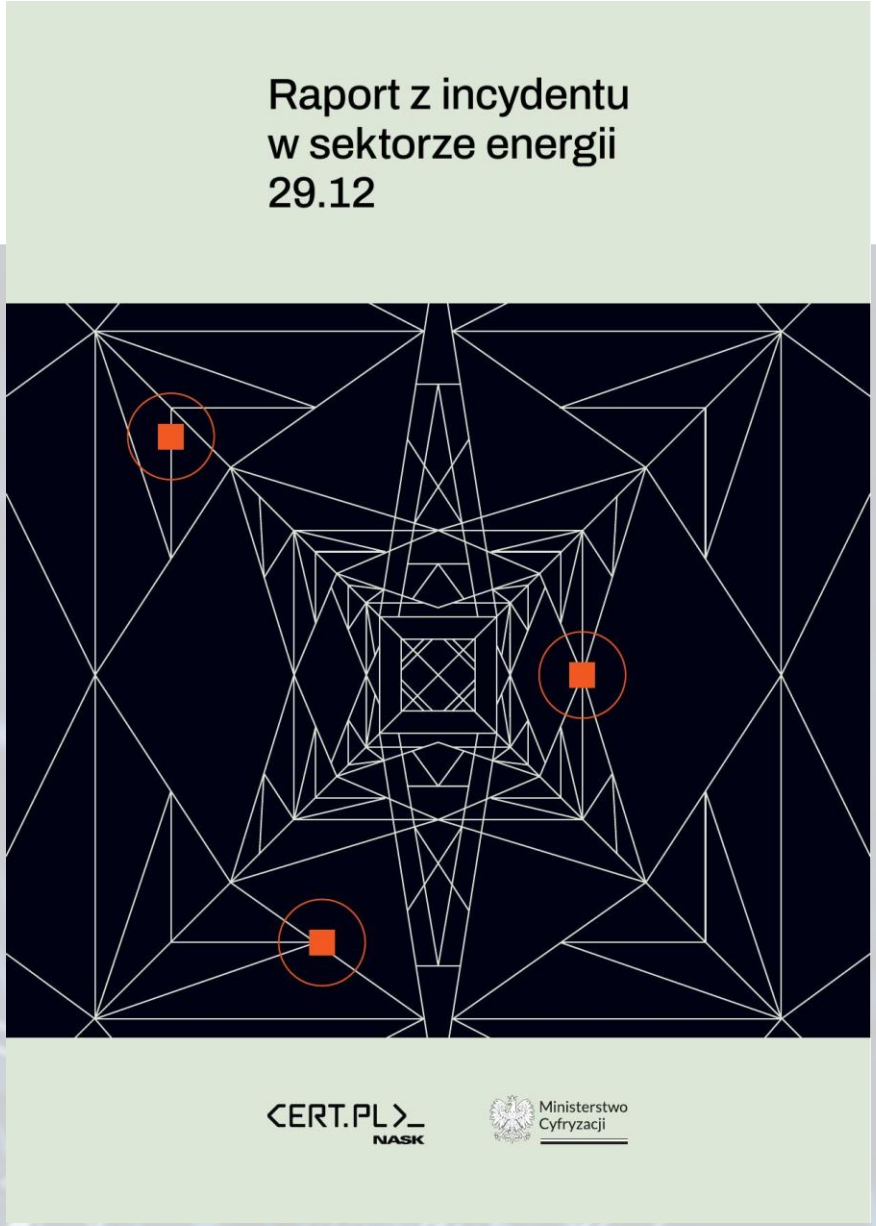
Atak na GPO

- Atak miał charakter destrukcyjny dla urządzeń komunikacyjnych. Unieruchomiona została komunikacja między farmami a OSD.
- Żaden z obiektów nie wstrzymał produkcji energii z powodu ataku.
- Atakujący miał poziom dostępu, który pozwalał na wyłączenie tych obiektów, ale tego nie zrobił.



Co się stało w grudniu 2025?

- Elektrociepłownia (objęta KSC) w dużym mieście wojewódzkim (prawie pół miliona odbiorców).
  - Analiza powłamaniowa wykazała, że pierwszy atak w marcu 2025 – wykradziono bazę haseł z kontrolera domeny.
  - Nie zmieniono wykradzionych haseł do listopada/grudnia 2025.
  - Systemy bezpieczeństwa zarejestrowały oba ataki, ale nikt tego nie obsłużył.
  - Ok. 100 stacji roboczych zostało zaszyfrowanych. Atak został zatrzymany przez systemy bezpieczeństwa.
  - Poziom uprawnień atakującego pozwalał na wyłączenie tego systemu bezpieczeństwa, ale atakujący tego nie zrobił.



Jaki jest dziś obraz cyberbezpieczeństwa OZE?

Grzechy główne:

- Fabryczne lub znane konta i hasła na urządzeniach i systemach
- Brak aktualizacji i poprawek bezpieczeństwa
- Niedobór kompetencji i zasobów ludzkich do zarządzania i obsługi cyberbezpieczeństwa.
- Brak segmentacji i separacji ruchu w sieciach obiektowych, a czasami w sieciach rozległych.
- Brak dokumentacji informatycznej i dokumentacji zabezpieczeń obiektu.

Jaki jest dziś obraz cyberbezpieczeństwa OZE?

Cyberbezpieczeństwo a ekonomia

MIKRONIKA

Jaki jest dziś obraz cyberbezpieczeństwa OZE?

Cyberbezpieczeństwo a regulacje

MIKRONIKA

Co robić?
Jak żyć?

- Zabezpieczyć co się da,
  z wykorzystaniem posiadanych środków
  - fabryczne hasła
  - aktualizacje bezpieczeństwa
- Wykonać przegląd cyberbezpieczeństwa instalacji i obiektów
  - audyt bezpieczeństwa
- Ocenić ryzyko, zaplanować i realizować działania
  - kompetencje w zakresie utrzymania
  - separacja sieci
  - monitorowanie i reakcja na incydenty

Dziękuję

Tomasz Szała

Dyrektor działu wdrożeń i utrzymania systemów IT

Mikronika