



NEWSLETTER

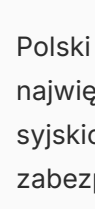
CHRONA DANYCH • CYBERBEZPIECZEŃSTWO • REGULACJE

Luty 2026 – Rosyjski cyberatak na polską energetykę – lekcje z incydentu

SPIS TREŚCI

- 01 ● Artykuł autorski
- 02 ● Przegląd newsów
- 03 ● Orzeczenia i decyzje
- 04 ● NIS2
- 05 ● AI Act
- 06 ● Kalendarz

ARTYKUŁ AUTORSKI



Tekst: **Lukasz Onysyk**

Rosyjski cyberatak na polską energetykę – lekcje z incydentu, który zmienia krajobraz zagrożeń

Pod koniec grudnia 2025 roku polski sektor energetyczny padł ofiarą poważnego cyberataku. **Raport CERT Polska z 30 stycznia 2026 r. wskazuje, że infrastruktura atakujących pokrywa się z klasternami związanymi z rosyjskim FSB (m.in. „Berserk Bear”, „Ghost Blizzard”), natomiast ESET ze średnim prawdopodobieństwem przypisuje operację grupie Sandworm (GRU). Atak uderzył bezpośrednio w farmy OZE, elektrociepłownię i firmę z sektora produkcyjnego – a przez zerwanie łańcuch komunikacyjnych dotknął pośrednio także operatorów systemów dystrybucyjnych (OSD). To najpoważniejszy znany incydent wymierzony w polską infrastrukturę krytyczną od czasu wejścia w życie znowelizowanych przepisów o krajowym systemie cyberbezpieczeństwa – i pierwszy poważny test gotowości sektora energetycznego na zagrożenia, przed którymi ostrzega dyrektywa NIS2.**

Anatomia ataku

Incydent z 29 grudnia 2025 roku nie był przypadkowy. Wybróń daty – okres świąteczno-noworoczny, kiedy obsady dyżurne są ograniczone, a czas reakcji wydłużony – to klasyczne tatyka zaawansowanych grup cyberprzestępczych powiązanych z państwami. Grupy APT powiązane z rosyjskimi służbami od lat atakują sektor energetyczny – wystarczy przypomnieć BlackEnergy (2015) i Industroyer (2016), które spowodowały wielogodzinne przerwy w dostawach prądu w wybranych regionach Ukrainy.

Polski sektor energetyczny stał się celem z oczywistych powodów geopolitycznych. Polska jest jednym z największych sojuszników Ukrainy w NATO, konsekwentnie dywersyfikuje dostawy energii z dala od rosyjskich źródeł, a dynamicznie rozwija OZE tworząc nową, rozproszoną powierzchnię ataku – często gorzej zabezpieczoną niż tradycyjna infrastruktura elektroenergetyczna.

Z opublikowanych informacji wynika, że atak dotknął bezpośrednio farmy OZE, elektrociepłownię i firmę z sektora produkcyjnego, a pośrednio – przez zakłócenie komunikacji – także operatorów systemów dystrybucyjnych (OSD). To szczególnie niepokojące, ponieważ sektor OZE w Polsce rozwija się w tempie, które często wyprzedza wdrażanie adekwatnych zabezpieczeń. Małe i średnie podmioty operujące farmami fotowoltaicznymi czy wiatrowymi rzadko dysponują dedykowanymi zespołami cyberbezpieczeństwa, a ich systemy SCADA i zdalne zarządzanie bywają podłączone do internetu bez odpowiedniej segmentacji sieci.

Kontekst prawny – NIS2 i krajowy system cyberbezpieczeństwa

Incydent ten należy analizować w kontekście dyrektywy NIS2 (2022/2555), której termin transpozycji upłynął 17 października 2024 roku. Polska, podobnie jak większość państw członkowskich UE, wciąż finalizuje implementację – nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa przechodzi przez proces legislacyjny. Niezależnie od stanu legislacji, NIS2 radykalnie rozszerza zakres podmiotów zobowiązanych do stosowania środków cyberbezpieczeństwa.

Sektor energetyczny to w terminologii NIS2 „sektor o wysokiej krytyczności” (Załącznik I). Operatorzy systemów dystrybucyjnych są jednoznacznie klasyfikowani jako podmioty kluczowe, co oznacza najwyższy poziom obowiązków:

- **Zarządzanie systemem** (art. 21 NIS2) – obowiązek wdrożenia polityk analizy ryzyka i bezpieczeństwa systemów informacyjnych, obsługi incydentów, ciągłości działania, bezpieczeństwa łańcucha dostaw oraz szyfrowania.
- **Zgłaszanie incydentów** (art. 23 NIS2) – wcześnie ostrzeżenie w ciągu 24 godzin, zgłoszenie incydentu w ciągu 72 godzin, sprawozdanie końcowe w ciągu miesiąca.
- **Odpowiedzialność zarządu** (art. 20 NIS2) – organy zarządzające muszą zatwierdzać środki zarządzania ryzykiem i odbywać szkolenia z cyberbezpieczeństwa. Niezwykle istotne: ponoszą osobistą odpowiedzialność za naruszenia.
- **Kary administracyjne** (art. 34 NIS2) – do 10 mln EUR lub 2% całkowitego rocznego światowego obrotu, w zależności od tego, która kwota jest wyższa.

Pojawia się jednak kluczowe pytanie: co z podmiotami z sektora OZE? Wiele z nich to małe i średnie przedsiębiorstwa, które mogą zostać zaklasyfikowane jako „podmioty ważne” (nie „kluczowe”), ale i tak podlegają obowiązkowi NIS2 – choć z łagodniejszym reżimem nadzoru. Problem w tym, że świadomość tych obowiązków w sektorze jest niska, a gotowość techniczna – często niewystarczająca.

Szerszy obraz zagrożeń – styczeń i luty 2026

Incydent w sektorze energetycznym nie był odosobnionym wydarzeniem. Przegląd alertów CERT Polska z ostatnich tygodni rysuje obraz rosnącej aktywności – zarówno grup APT, jak i cyberprzestępczych oportunistycznych:

- **Podatności w routerach** (CVE-2025-12386 w LV-WR21Q) i **kamerach IP** (Vivotek IP7137 – alert CERT Polska ze stycznia 2026) – to urządzenia powszechnie stosowane w infrastrukturze energetycznej i przemysłowej. Niezatluszone podatności w urządzeniach sieciowych i IoT to wciąż jeden z głównych wektorów wejścia do sieci OT.
- **Podatność w mObywatelu na iOS** (CVE-2025-11598) – choć to inna kategoria ryzyka, pokazuje, że nawet krytyczne aplikacje państwowe nie są wolne od luk.
- **Podatności w oprogramowaniu Quick.Cart** – dwa osobne alerty w ciągu miesiąca sugerują systemowy problem z bezpieczeństwem tego popularnego w Polsce oprogramowania e-commerce.

Równoległe Niebezpiecznik donosił o fali włamań na konta nauczycieli w e-dziennikach, publicznie dostępnych danych dzieci ze żłobków oraz jawnym monitorowaniu wizyjnym w sieci sklepów. Wszystkie te incydenty łączy wspólny mianownik: niedostateczna higiena cyberbezpieczeństwa w podmiotach, które przetwarzają dane osobowe na dużą skalę.

Praktyczne wnioski dla organizacji

1. Audyt gotowości NIS2 – teraz, nie po uchwaleniu ustawy. Nie czekajcie na polską implementację. Dyrektywa NIS2 ma bezpośredni skutek w zakresie, w jakim przepisy krajowe są niezgodne z jej celami. Organizacje powinny już teraz przeprowadzić gap analysis wobec wymagań art. 21 NIS2.

2. Segmentacja sieci OT/IT to priorytet. Atak na sektor energetyczny po raz kolejny potwierdza, że brak separacji między sieciami korporacyjnymi (IT) a systemami sterowania przemysłowego (OT) to krytyczna luka. Minimalna architektura musi uwzględnić DMZ z demilitaryzowaną strefą (DMZT) między warstwami.

3. Plan reakcji na incydenty musi uwzględniać okres świąteczny. Atakujący celowo wybierają momenty obniżonej gotowości. Organizacje powinny wdrożyć procedury eskalacji i dyżury on-call, które zapewnią odpowiednią czas reakcji 24/7/365.

4. Łańcuch dostaw pod lupą. Podmioty z sektora OZE często korzystają z rozwiązań chmurowych i zdalnego zarządzania dostarczanych przez zewnętrznych dostawców. Bezpieczeństwo tych dostawców bezpośrednio przekłada się na bezpieczeństwo operatora – a NIS2 wprost wymaga zarządzania ryzykiem łańcucha dostaw.

5. Szkolenia zarządu to nie formalność. Art. 20 NIS2 wymaga, aby organy zarządzające podmiotów kluczowych i ważnych odbywały regularne szkolenia z zakresu cyberbezpieczeństwa. Po incydencie w polskiej energetyce argument „to sprawa działu IT” nie obstoi – ani przed regulatorem, ani przed sądem.

6. Inwentaryzacja i aktualizacja urządzeń brzegowych. Routery, kamery IP, urządzenia IoT – to z reguły pierwsze cele rekonesansu. Każde urządzenie podłączone do sieci musi być zainwentaryzowane, regularnie aktualizowane i objęte monitoringiem.

Podsumowanie

Grudniowy atak na polską energetykę to nie abstrakcyjna groźba – to konkretny incydent, który dotknął konkretne organizacje. W połączeniu z nadchodzącym wdrożeniem NIS2 oraz rosnącą aktywnością grup APT stanowi jasny sygnał: czas na reaktywne podejście do cyberbezpieczeństwa infrastruktury krytycznej się skończył. Organizacje, które nie podejmą działań teraz, ryzykują nie tylko przerwanie ciągłości działania, ale też wielomilionowe kary i osobistą odpowiedzialność zarządu.

Źródła

- Raport z incydentu w sektorze energii z 29 grudnia 2025 roku – CERT Polska, 30.01.2026
- Jak Rosjanie zhackowali polski sektor energetyczny miesiąc temu? – Niebezpiecznik, 30.01.2026
- Podatności w oprogramowaniu routera LV-WR21Q (CVE-2025-12386) – CERT Polska, 27.01.2026
- Podatności w oprogramowaniu kamery Vivotek IP7137 – CERT Polska, 09.01.2026
- Podatność w aplikacji mObywatel na iOS (CVE-2025-11598) – CERT Polska, 03.02.2026
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. (NIS2)

PRZEGLĄD NEWSÓW

Przegląd najważniejszych wiadomości

Podatność w aplikacji mObywatel na iOS (03.02.2026)

Na początku lutego CERT Polska ostrzegł przed podatnością bezpieczeństwa (CVE-2025-11598) w aplikacji mObywatel na iOS. Luka mogła pozwolić na nieautoryzowany dostęp do danych identyfikacyjnych użytkowników i – mObywatel to narzędzie, z którego miliony Polaków korzystają do potwierdzania tożsamości i przechowywania dokumentów cyfrowych. Skala ryzyka jest poważna: chodzi o dane najwyższej kategorii wrażliwości. Organizacje, w których pracownicy używają mObywatela służbowo, powinny zweryfikować aktualność wersji aplikacji na wszystkich urządzeniach.

Źródło: CERT Polska

Zarzuty karne w sprawie wycieku danych z Morele.net (09.02.2026)

Sprawa Morele.net wchodzi w nowy etap. 30 stycznia 2026 r. prokuratura postawiła zarzuty 29-latkowi w związku z głośnym wyciekami danych osobowych z platformy (informacja medialna ukazała się 9 lutego). Przypomnijmy: UODO nałożył na Morele.net pierwotnie karę 2,83 mln zł, która została uchylona przez NSA. W ponownym postępowaniu organ wymierzył karę wyższą – 3,82 mln zł. Dotychczas przypadek ten funkcjonował w świadomości branży głównie jako precedens administracyjny. Teraz okazuje się, że naruszenia ochrony danych mogą skutkować również odpowiedzialnością karną sprawców. W przypadku poważnych incydentów warto pamiętać o możliwości zawiadomienia organów ścigania – nie tylko organu nadzorczego.

Źródło: Niebezpiecznik

Konferencja EDPB o współpracy międzyregulacyjnej – zapisy otwarte (03.02.2026)

17 marca 2026 r. Europejska Rada Ochrony Danych organizuje konferencję poświęconą współpracy między organami regulacyjnymi w UE. Rejestracja jest już otwarta. Temat przewodni: jak skoordynować działania organów ochrony danych, regulatorów konkurencji i nadzorców rynków cyfrowych, gdy równocześnie obowiązują RODO, AI Act, DSA i DMA. Pytanie niebagatelne, bo granice kompetencji między tymi reżimami wciąż pozostają rozmyte.

Źródło: EDPB

Reklama polityczna pod lupą EDPB (29.01.2026)

Rada otworzyła nabór zgłoszeń zainteresowania udziałem w spotkaniu dotyczącym ochrony danych w kontekście reklamy politycznej. Temat wiąże się z unijnym rozporządzeniem o przejrzystości i targetowaniu reklam politycznych, które ma zacząć obowiązywać przed kolejnymi wyborami europejskimi. EDPB zapowiada prace nad szczegółowymi wytycznymi. Podmioty zajmujące się marketingiem politycznym i organizacje przetwarzające dane wyborców mają więc jeszcze czas, by włączyć się w konsultacje i wpłynąć na kształt przyszłych regul.

Źródło: EDPB

Błąd w systemie e-toli na A4 – niesłuszne mandaty (06.02.2026)

Kierowcy jeżdżący autostradą A4 zaczęli otrzymywać wezwania do zapłaty 500 zł za nieprawidłowo naliczone opłaty. Przyczyną okazał się błąd w systemie poboru opłat. Z perspektywy ochrony danych sprawa jest interesująca – systemy e-toli przetwarzają dane geolokalizacyjne i identyfikacyjne pojazdów, a pośrednio także ich właścicieli. Błędne naliczenie to nie tylko kłopot finansowy, ale też potencjalne naruszenie zasady prawidłowości danych z art. 5 ust. 1 lit. d RODO. Przypadek dobrze ilustruje, jak ważny jest regularny audyt jakości danych w systemach automatycznego przetwarzania.

Źródło: Niebezpiecznik

Międzynarodowa współpraca w cyberbezpieczeństwie – nowe dokumenty strategiczne ENISA (luty 2026)

ENISA opublikowała zaktualizowane dokumenty dotyczące strategii międzynarodowej i współpracy z interesariuszami w zakresie cyberbezpieczeństwa. Dla podmiotów objętych dyrektywą NIS2 to lektura obowiązkowa – międzynarodowe mechanizmy wymiany informacji o zagrożeniach przekładają się bezpośrednio na krajowe wymogi zgłaszania incydentów i współpracy transgranicznej. Szczególnie dotyczy to organizacji działających w sektorach, które NIS2 klasyfikuje jako kluczowe lub ważne.

Źródło: ENISA

Luki w Quick.Cart – zagrożenie dla sklepów internetowych (05.02.2026)

Kolejne ostrzeżenie CERT Polska, tym razem dotyczące podatności w Quick.Cart (CVE-2026-23796) – silniku sklepów internetowych typu dane wśrask polskich e-commerce'ów. Platformy handlowe przetwarzają dane osobowe klientów, w tym dane finansowe i adresowe, więc luki w ich oprogramowaniu zawsze niosą podwyższone ryzyko. Administratorzy sklepów opartych na Quick.Cart powinni sprawdzić, czy korzystają z wersji wolnej od wykrytych podatności.

Źródło: CERT Polska

ORZECZENIA I DECYZJE

Orzeczenia i decyzje – luty 2026

FREE MOBILE i FREE – 42 mln EUR (13.01.2026)

- **Organ:** CNIL (francuski organ ochrony danych)
- **Podmiot:** FREE MOBILE (27 mln EUR) i FREE (15 mln EUR) – spółki grupy Iliad
- **Kara/nakaz:** łącznie 42 000 000 EUR
- **Istota:** W październiku 2024 r. atakujący uzyskał dostęp do systemów informatycznych obu spółek i wkradł dane osobowe powiązane z 24 milionami umów abonenckich, w tym numery IBAN. CNIL stwierdziła naruszenie art. 32 RODO – procedury uwierzytelniania przy dostępie do VPN nie były wystarczająco odporne, a mechanizmy wykrywania anomalii w systemach informatycznych okazały się nieskuteczne. Dodatkowo FREE MOBILE nie wdrożyła polityki usuwania danych byłych abonentów, przekraczając ją bez uzasadnionej potrzeby.
- **Znaczenie dla praktyki:** Sama ochrona brzegowa (firewall, szyfrowanie) nie wystarczy – organ nadzorczy ocenił też jakość uwierzytelniania wewnętrznych, politykę retencji danych i zdolność organizacji do wykrywania incydentów w czasie rzeczywistym. Warto zweryfikować, czy organizacja posiada aktualne procedury minimalizacji i usuwania danych.

France Travail – 5 mln EUR (22.01.2026)

- **Organ:** CNIL (francuski organ ochrony danych)
- **Podmiot:** France Travail (dawniej Pôle emploi) – francuski urząd pracy
- **Kara/nakaz:** 5 000 000 EUR + nakaz wdrożenia środków naprawczych pod groźbą 5 000 EUR dziennie kary za każdy dzień zwłoki
- **Istota:** Na początku 2024 r. hakerzy metodą socjotechniki przejęli konta doradców zawodowych CAP EMPLOI i uzyskali dostęp do danych osób zarejestrowanych jako bezrobotne w ciągu ostatnich 20 lat – łącznie z numerami dostawczymi spłecznego, adresami i telefonami. CNIL stwierdziła naruszenie art. 32 RODO: brak wystarczająco silnego uwierzytelniania, zbyt szerokie uprawnienia i obowiązkii informacyjne jako temat skoordynowanej akcji egzekucyjnej na 2026 r. – warto przeprowadzić przegląd zgodności klauzul informacyjnych we wszystkich kanałach komunikacji.
- **Znaczenie dla praktyki:** Ataki socjotechniczne omijają zabezpieczenia techniczne – kluczowe jest wieloskładnikowe uwierzytelnianie (MFA) dla wszystkich użytkowników z dostępem do danych osobowych, stosowanie zasady minimalnych uprawnień (least privilege) oraz wdrożenie systemów wykrywania anomalii w logach dostępowych.

LDI NRW – 300 tys. EUR (styczeń 2026)

- **Organ:** Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (organ ochrony danych Nadrenii Północnej-Westfalii)
- **Podmiot:** firma telekomunikacyjna (nazwa nieujawniona)
- **Kara/nakaz:** 300 000 EUR
- **Istota:** Firma od 2022 r. rozsyłała spersonalizowane listy reklamowe zawierające wstępnie wypiecone umowy na usługi internetowe i telefoniczne – do osób, które nigdy nie kontaktowały się z tą firmą. Listy nie zawierały wymaganej informacji o przetwarzaniu danych (tożsamość administratora, dane IOD). Co więcej, firma systematycznie ignorowała wnioski o dostęp do danych, żądania usunięcia danych i sprzeciw wobec przetwarzania – zaprzeczając otrzymaniu korespondencji, mimo potwierdzenia jej doręczenia.
- **Znaczenie dla praktyki:** Obowiązki informacyjne z art. 13-14 RODO dotyczą także komunikacji marketingowej. Ignorowanie wniosków osób, których dane dotyczą, jest traktowane jako odrębne i poważne naruszenie. Europejska Rada Ochrony Danych (EDPB) wybrała właśnie przejrzystość i obowiązkii informacyjne jako temat skoordynowanej akcji egzekucyjnej na 2026 r. – warto przeprowadzić przegląd zgodności klauzul informacyjnych we wszystkich kanałach komunikacji.

Poczta Polska S.A. – 978 tys. zł (styczeń 2026)

- **Organ:** Prezes UODO
- **Podmiot:** Poczta Polska S.A.
- **Kara/nakaz:** 978 000 zł
- **Istota:** Prezes UODO stwierdził, że Poczta Polska przez ponad sześć lat (od wejścia RODO w życie w maju 2018 r. do listopada 2024 r.) nie zapewniała niezależności sprawowania funkcji Inspektora Ochrony Danych. IOD był jej swoją funkcją – ze stanowiskiem kierowniczym odpowiedzialnym za przetwarzanie danych osobowych, w tym za bezpieczeństwo i ochronę informacji niejawnych – co stanowiło ewidentny konflikt interesów naruszający art. 38 ust. 6 RODO. Poczta Polska zapowiedziała zaskarżenie decyzji do sądu administracyjnego.
- **Znaczenie dla praktyki:** Niezależność IOD to nie formalność organizacyjna – organ nadzorczy weryfikuje, czy IOD faktycznie może wykonywać swoje zadanie bez konfliktu interesów. IOD nie powinien łączyć tej funkcji z rolami, w których podejmuje decyzje o celach i sposobach przetwarzania danych. Warto dokonać audytu struktury organizacyjnej pod kątem zgodności z art. 38 RODO.

WSA potwierdza karę dla Komendanta Głównego Policji – 75 tys. zł (28.01.2026)

- **Organ:** Wojewódzki Sąd Administracyjny w Warszawie (utrzymanie decyzji Prezesa UODO)
- **Podmiot:** Komendant Główny Policji
- **Kara/nakaz:** 75 000 zł
- **Istota:** WSA oddalił skargę KGP na decyzję Prezesa UODO, który nałożył karę za ujawnienie podczas konferencji prasowej danych dotyczących zdrowia i życia prywatnego obywatelki – w tym informacji o leczeniu psychiatrycznym. Sąd potwierdził, że doszło do naruszenia art. 6 ust. 1 oraz art. 9 ust. 1 RODO (przetwarzanie danych w szczególności kategorii biometrycznych). Publiczne ujawnienie danych wrażliwych przez organ ścigania, nawet w kontekście obrony przed zarzutami medialnymi, nie znajduje oparcia w żadnej z przesłanek legalizujących przetwarzanie.
- **Znaczenie dla praktyki:** Organy publiczne nie korzystają z wyjątku od RODO – są administratorami danych i podlegają pełnemu reżimowi rozporządzenia. Konferencje prasowe, odpowiedzi na zapytania medialne i komunikaty publiczne wymagają uprzedniej oceny, czy nie dochodzi do ujawnienia danych osobowych, w szczególności danych szczególnych kategorii (zdrowie, życie seksualne, poglądy).

Podsumowanie trendów

- **Bezpieczeństwo techniczne pod lupą** – CNIL w dwóch głośnych decyzjach (FREE, France Travail) pokazuje, że niedostateczne uwierzytelnianie, brak MFA i słaby monitoring to naruszenia art. 32 RODO skutkujące wielomilionowymi karami.
- **Przejrzystość – priorytet 2026** – Europejska Rada Ochrony Danych (EDPB) wybrała obowiązkii informacyjne (art. 12-14 RODO) jako temat skoordynowanej akcji egzekucyjnej. Decyzja LDI NRW to pierwszy sygnał tego trendu.
- **Niezależność IOD w Polsce** – kara dla Poczty Polskiej to jasny sygnał do PUODO: konflikt interesów w funkcji IOD będzie ścigany. Czas na audyty struktur organizacyjnych.
- **Organy publiczne nie stoją ponad RODO** – potwierdzone przez WSA w sprawie KGP. Nawet działania w interesie publicznym nie uzasadniają ujawniania danych wrażliwych bez podstawy prawnej.

NIS2

NIS2 – co nowego

Stan wdrażania w Polsce

Polska kontynuuje prace nad implementacją dyrektywy NIS2. Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa przechodzi przez kolejne etapy legislacyjne. Tymczasem – niezależnie od stanu polskich przepisów – dyrektywa NIS2 ma bezpośredni skutek w zakresie, w jakim państwa członkowskie nie dokonały transpozycji w terminie (17 października 2024 r.).

Kluczowe elementy polskiej implementacji: - **Rozszerzony zakres podmiotowy** – NIS2 obejmuje znacznie więcej sektorów: produkcję żywności, zarządzanie odpadami, usługi pocztowe, administrację publiczną i sektor kosmiczny. - **Podział na podmioty kluczowe i ważne** – z różnym poziomem nadzoru i sankcji. - **Osobista odpowiedzialność zarządu** – członkowie kierownictwa będą odpowiedzialni za zapewnienie zgodności z wymogami cyberbezpieczeństwa.

Incydent w sektorze energetycznym – test NIS2 w praktyce

Raport CERT Polska z 30 stycznia 2026 r. dokumentuje poważny cyberatak na polski sektor energetyczny z 29 grudnia 2025 r. Incydent – warty uwagi z grupami APT powiązanymi z rosyjskimi służbami wywołany – uderzył bezpośrednio w farmy OZE, elektrociepłownię i firmę produkcyjną, a pośrednio dotknął także operatorów systemów dystrybucyjnych (OSD). To pierwszy przypadek na taką skalę od wejścia w życie wymogów NIS2, który ujawnił luki w gotowości sektora:

- Brak segmentacji sieci IT/OT w wielu podmiotach z sektora OZE
- Niewystarczające zabezpieczenie zdalnego zarządzania infrastrukturą
- Ograniczone zdolności detekcji i reakcji w okresie świątecznym

Nowe wytyczne i dokumenty

- **ENISA: Threat Landscape 2025** (zaktualizowany w styczniu 2026) – raport obejmujący okres lipiec 2024 – czerwiec 2025 wskazuje ransomware na infrastrukturę krytyczną, wykorzystanie AI do socjotechniki i ataki na łańcuchy dostaw jako kluczowe zagrożenia.
- **Komisja Europejska: propozycja zmian NIS2** (20 stycznia 2026 r.) – ukierunkowane modyfikacje dotyczące raportowania incydentów i współpracy transgranicznej.
- **CERT Polska: seria alertów** – podatności w routerach (CVE-2025-12386), kamerach IP (Vivotek), oprogramowaniu Quick.Cart i aplikacji mObywatel – przypomnienie o znaczeniu zarządzania podatnościami.

Praktyczne wskazówki

1. **Nie czekaj na polską ustawę** – przeprowadz gap analysis wobec wymagań art. 21 NIS2 już teraz. Planowany termin pierwszego audytu zgodności to 30 czerwca 2026 r. – zależy on jednak od finalnego kształtu polityki ustawy implementującej dyrektywę.
2. **Segmentacja sieci OT/IT** – po ataku na energetykę to absolutny priorytet. Model Purdue z DMZ między warstwami IT i OT to minimum.
3. **Zarządzanie ryzykiem łańcucha dostaw** – NIS2 wymaga oceny bezpieczeństwa dostawców. Zacznij od inwentaryzacji i klasyfikacji dostawców krytycznych.
4. **Procedury na okres obniżonej gotowości** – dyżury on-call, eskalacja 24/7, szczególna czujność w weekendy i święta.
5. **Szkolenia zarządu** – art. 20 NIS2 wymaga regularnych szkoleń kadry zarządzającej z cyberbezpieczeństwa. Argument „to sprawa działu IT” nie obstoi przed regulatorem.

AI ACT

AI Act – aktualności

Stopizowanie

Rezultatem o sztucznej inteligencji (AI Act) weszło już w fazę aktywnego stosowania. Od 2 lutego 2025 r. obowiązuje zakaz praktyk niedopuszczalnych (art. 5) – w tym social scoringu, manipulacji progowej i biometrycznej kategoryzacji opartej na cechach wrażliwych. Od 2 sierpnia 2025 r. stosuje się przepisy dotyczące modeli ogólnego przeznaczenia (GPAI), obowiązkii kompetencji AI (art. 4) oraz sankcji. Przed nami jeszcze dwa kluczowe progi:

- **2 sierpnia 2026** – pełne stosowanie przepisów dla systemów AI wysokiego ryzyka (załącznik III), w tym obowiązków dotyczących zarządzania ryzykiem, dokumentacji technicznej, ludzkiego nadzoru i transparentności.
- **2 sierpnia 2027** – rozszerzenie na systemy AI wbudowane w produkty regulowane sektorowo (wyroby medyczne, zabawki, maszyny itp.).

Najważniejsze zmiany

Wytyczne i Kodeksy praktyk dla modeli GPAI. Europejski Urząd ds. Sztucznej Inteligencji (AI Office) opublikował wytyczne dotyczące obowiązków dostawców modeli ogólnego przeznaczenia – obejmują one m.in. zasady sporządzania dokumentacji technicznej, politykę praw autorskich oraz wymogi transparentności. Równolegle trwają prace nad Kodeksem praktyk (Code of Practice), który ma pełnić rolę domyślnego standardu zgodności dla dostawców GPAI. Dokument – opracowywany we współpracy z branżą, środowiskiem akademickim i organizacjami społeczeństwa obywatelskiego – precyzuje, jak w praktyce realizować obowiązki wynikające z rozporządzenia. Dostawcy, którzy przystąpią do kodeksu, będą mogli wykazać zgodność z AI Act w uproszczony sposób.

Kompetencje AI art. 4.4 już obowiązują. Od sierpnia 2025 r. wszystkie organizacje wdrażające AI lub stosujące systemy AI mają obowiązek zapewnienia odpowiedniego poziomu kompetencji (AI literacy) wśród pracowników. Kilka państw skutecznie uruchomiło już programy szkoleniowe wspierające realizację tego wymogu. To obowiązek, który dotyczy każdej organizacji korzystającej z narzędzi AI – nie tylko dostawców.

Piaskownice regulacyjne nabierają kształtu. Państwa członkowskie uruchamiają piaskownice regulacyjne (regulatory sandboxes) umożliwiające testowanie innowacyjnych rozwiązań AI w kontrolowanym środowisku prawnym. Podjęcie takich inicjatyw – albo piaskownic sektorowych po modelu ogólne. Polska jest wśród państw planujących uruchomienie piaskownicy, choć szczegółowy organizacyjny wciąż się kształtuje.

Modyfikacja systemów AI w kontekście AI Act. Praktyka stosowania AI Act ujawnia istotny problem: modyfikacja istniejącego systemu AI – np. zmiana danych treningowych, parametrów modelu lub zakresu zastosowania – może skutkować rekasyfikacją systemu do wyższej kategorii ryzyka. Dostawcy muszą na bieżąco monitorować, czy wprowadzane zmiany nie przesuwają produktu do kategorii wysokiego ryzyka i związanych z nią obowiązków.

Ochrona sygnalizatorów w kontekście AI Act. Rozporządzenie przewiduje mechanizmy ochrony osób zgłaszających naruszenia przepisów dyrektywy AI. Organizacje powinny uwzględnić AI Act w swoich procedurach sygnalizacyjnych – osoby zgłaszające nieprawidłowości związane z systemami AI (np. nielegalne praktyki, brak wymaganej dokumentacji) podlegają ochronie na zasadach analogicznych do dyrektywy o ochronie sygnalizatorów.

Panel naukowy AI. Urząd ds. AI powołuje Naukowy Panel ds. AI (AI Scientific Panel), złożony z niezależnych ekspertów. Panel będzie doradzał Komisji w kwestiach klasyfikacji modeli GPAI o systemowym ryzyku, wspierał opracowywanie standardów oraz monitorował rozwój technologii AI pod kątem nowych zagrożeń.

Co to oznacza w praktyce

Dla dostawców systemów i modeli AI: - Dostawcy modeli GPAI (w tym dużych modeli językowych) mają już obowiązek prowadzenia dokumentacji technicznej, polityki praw autorskich i zapewnienia transparentności. Warto rozważyć przystąpienie do Kodeksu praktyk jako ścieżki wykazania zgodności. - Każda istotna modyfikacja systemu AI wymaga ponownej oceny klasyfikacji ryzyka – brak takiej weryfikacji może oznaczać naruszenie rozporządzenia.

Dla organizacji stosujących AI (deployers): - Obowiązek kompetencji AI (art. 4) już obowiązują – organizacje powinny zadbać o szkolenia pracowników w zakresie zasad działania, ograniczeń i ryzyk związanych z wykorzystywaniem narzędziów AI. - Organizacje korzystające z systemów AI wysokiego ryzyka (rekrutacja, ocena zdolności kredytowej, biometria) muszą przygotować się na pełne stosowanie wymogów od sierpnia 2026 r. – w tym zapewnić ludzki nadzór, dokumentację i mechanizmy przejrzystości. - Konieczne jest uwzględnienie AI Act w procedurach sygnalizacyjnych.

Dla IOD i specjalistów ds. compliance: - AI Act RODO nakładają się w obszarze przetwarzania danych osobowych przez systemy AI. IOD powinien uczestniczyć w ocenie ryzyka systemów AI i koordynować ją z procesem DPIA. - Piaskownice regulacyjne mogą stanowić okazję do testowania innowacyjnych rozwiązań w bezpiecznych ramach prawnych i warto śledzić prace krajowe w tym zakresie. - MSP mogą liczyć na uproszczenia i wsparcie, a AI Act przewiduje proporcjonalne wymagania dla mniejszych podmiotów, a Komisja publikuje dedykowane przewodniki.

KALENDARZ

Kalendarz

Data	Wydarzenie	Kategoria
2026-03-04/05	European Cybersecurity Skills Conference 2026 – Larnaka, Cypr	Cyberbezpieczeństwo (ENISA)
2026-03-11	Security Masters & MS POS – konferencja Security Masters	Cyberbezpieczeństwo
2026-03-12	Cybersecurity Standardisation Conference – Bruksela (ENISA + CEN/CENELEC/ETSI)	Cyberbezpieczeństwo
2026-03-20	ENISA Telecom & Digital Infrastructure Security Forum – Pafos, Cypr	Cyberbezpieczeństwo / NIS2
2026-03-24/26	EU Cyber Acts Conference 2026 – Bruksela; CRA, NIS2 i DORA	Cyberbezpieczeństwo