



Europejski i Krajowy System Cyberbezpieczeństwa

13 października 2026 r.

Tomasz Chomicki

Cyberbezpieczeństwo w Polsce w 2025 r.



blisko

273 tys.

incydentów obsługanych przez krajowe zespoły CSIRT

wzrost

+144,4%

w stosunku do 2024 roku

Bezprecedensowy wzrost cyberataków. Źródło: Sprawozdanie Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa za 2025 rok.

AI – KLUCZOWE NARZĘDZIE GRUP CYBEROFENSYWNYCH W 2025 R.



Phishing generowany przez modele językowe

Automatyczne generowanie wysoce spersonalizowanych i bezbłędnych językowo wiadomości phishingowych.



Deepfake – syntetyczne audio i wideo

Podszywanie się pod urzędników czy osoby publiczne w celu manipulacji.

Strategia UE w zakresie cyberbezpieczeństwa



Ursula von der Leyen

REZULTAT DZIAŁAŃ



2020 r. – Strategia działań w zakresie cyberbezpieczeństwa



Strategia UE w zakresie bezpieczeństwa

CEL NOWEJ STRATEGII UE: OCHRONA INTERNETU, A JEDNOCZEŚNIE GWARANCJE BEZPIECZEŃSTWA I PRAW



Ochrona globalnego i otwartego Internetu



Bezpieczeństwo



Ochrona europejskich wartości i praw podstawowych ludności

Joint Cyber Unit (2021) i zdolność operacyjna UE

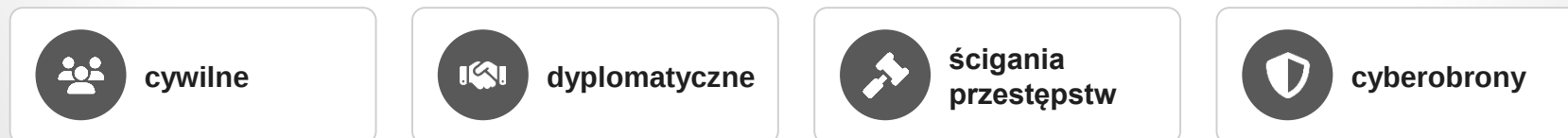


BUDOWANIE ZDOLNOŚCI OPERACYJNEJ – NOWA WSPÓLNA JEDNOSTKA DS. CYBERPRZESTRZENI (ENISA)

Cel: zacieśnienie współpracy między organami UE i organami państw członkowskich odpowiedzialnymi za:



obejmującą środowiska:



Dyrektywa NIS 2 – odporność krytycznych sektorów

ODPORNOŚĆ, SUWERENNOŚĆ TECHNOLOGICZNA I PRZYWÓDZTWO

CZYM JEST

Reforma przepisów o bezpieczeństwie sieci i systemów informatycznych: dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii (zmieniona dyrektywa w sprawie bezpieczeństwa sieci i informacji).

CEL

Zwiększenie poziomu cyberodporności krytycznych sektorów publicznych i prywatnych.

KOGO DOTYCZY

Średnich i dużych podmiotów z większej liczby sektorów – stosownie do ich krytyczności dla gospodarki i społeczeństwa.

SEKTORY OBJĘTE OCHRONĄ



Szpital



Sieci energetyczne



Koleje



Ośrodki przetwarzania danych



Administracja publiczna



Laboratoria badawcze



Produkcja wyrobów medycznych i leków o kluczowym znaczeniu



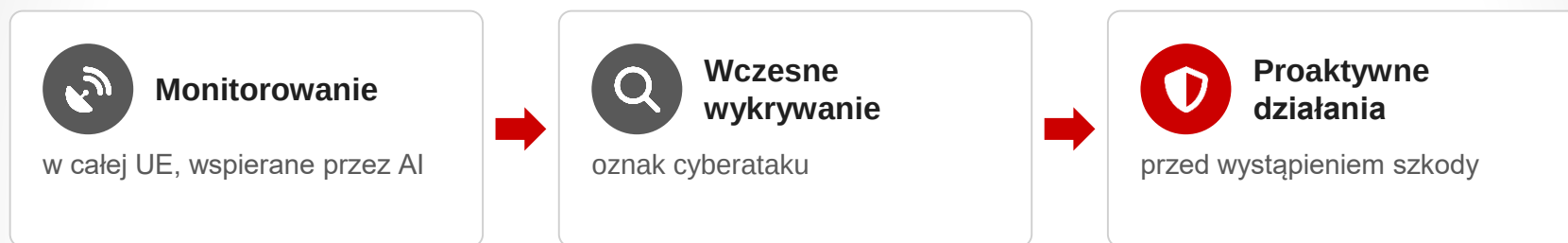
Pozostała infrastruktura krytyczna i usługi krytyczne

...muszą pozostać poza zasięgiem cyberataków w coraz szybciej zmieniającym się i złożonym środowisku zagrożeń.

Sieć centrów monitorowania i nowe akty rynku cyfrowego

SIEĆ CENTRÓW MONITOROWANIA BEZPIECZEŃSTWA W CAŁEJ UE

Propozycja Komisji: sieć centrów wspieranych przez sztuczną inteligencję (AI) – „tarcza przed zagrożeniami dla cyberbezpieczeństwa”.



Zespoły CSIRT i sieć CSIRT w UE

CSIRT

Computer Security Incident Response Team

**Zespół Reagowania na Incydenty
Bezpieczeństwa Komputerowego**

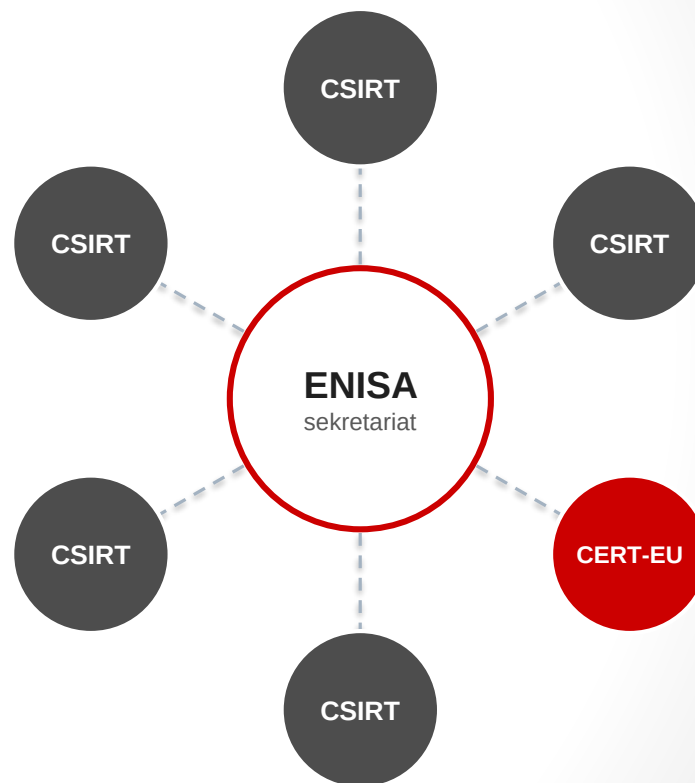
PRAKTYCZNA KONSEKWENCJA REGULACJI: SIEĆ CSIRT



Sieć CSIRT składa się z przedstawicieli CSIRT państw członkowskich i CERT-EU.



ENISA zapewnia sekretariat oraz aktywnie wspiera współpracę między CSIRT.



CSIRT – zespoły państw członkowskich

Krajowy System Cyberbezpieczeństwa (PL)

Cel: zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym:



niezakłóconego świadczenia usług kluczowych i usług cyfrowych

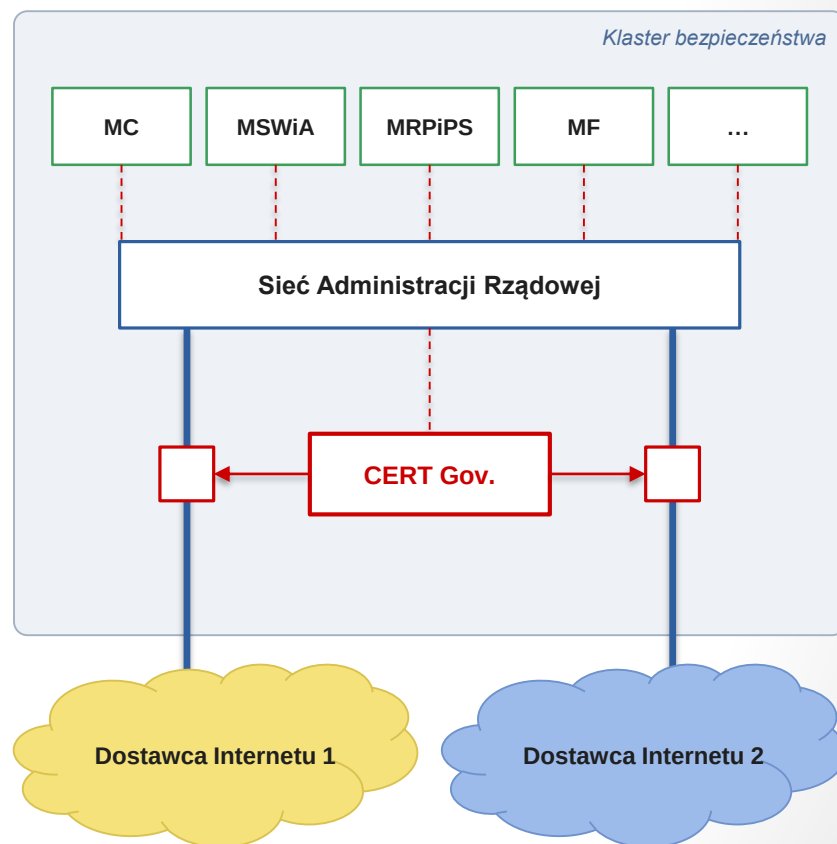


przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług



oraz zapewnienie obsługi incydentów

Bezpieczna architektura sieci



Polska struktura – trzy CSIRT poziomu krajowego

Każdy z nich to Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym.



CSIRT GOV

PROWADZI

Szef Agencji Bezpieczeństwa
Wewnętrznego

OBSZAR ZGŁOSZEŃ

- administracja publiczna
- infrastruktura krytyczna państwa

Główne zadanie: rozpoznawanie,
zapobieganie i wykrywanie zagrożeń
dla systemów teleinformatycznych
ważnych dla funkcjonowania państwa.



CSIRT Ministerstwa Obrony Narodowej

CSIRT MON

PROWADZI

Minister Obrony Narodowej

OBSZAR ZGŁOSZEŃ

- systemy podmiotów objętych
właściwością CSIRT MON
- przede wszystkim podległych MON
lub przez niego nadzorowanych



CSIRT NASK (CERT Polska)

PROWADZI

Naukowa i Akademicka Sieć
Komputerowa – Państwowy Instytut
Badawczy

OBSZAR ZGŁOSZEŃ

- obywatele
- przedsiębiorstwa i firmy prywatne
- samorządy
- szkoły i uczelnie
- organizacje pozarządowe
- instytucje nieobsługiwane przez
CSIRT GOV ani CSIRT MON

Przykładowe zgłoszenia i zasada wyboru CSIRT

CSIRT GOV

incydenty zagrażające bezpieczeństwu danych i działaniu systemów:

- phishing
- złośliwe oprogramowanie
- włamania
- wycieki danych
- ataki DDoS

CSIRT MON

- phishing i kradzież haseł
- malware i ransomware
- włamania i przejęcia kont
- wycieki danych
- DDoS i zakłócenia usług
- zmiany lub usuwanie danych

CSIRT NASK

- phishing (fałszywe e-maile i SMS-y)
- oszustwa internetowe
- złośliwe oprogramowanie
- włamania na konta internetowe
- fałszywe sklepy internetowe



Zasada: o wyborze CSIRT decyduje to, czyjego systemu dotyczy zdarzenie, a nie sam rodzaj ataku.

Prywatny phishing czy infekcję domowego komputera kieruje się co do zasady do CERT Polska (CSIRT NASK).

Systemy niejawne: incydenty zgłasza się wyłącznie dedykowanymi kanałami niejawnymi, zgodnie z dokumentacją bezpieczeństwa.

Zamówienia: ochrona danych i bezpieczeństwo płatności

Art. 18 PZP

Udostępnienie wykazu rozwiązania technicznego dopiero po podpisaniu umowy o poufności.

STUDIUM PRZYPADKU: BEC (BUSINESS EMAIL COMPROMISE) – PGZ CENZIN

1



Podszycie pod kontrahenta

Oszuści wysłali e-maile udające korespondencję od czeskiego dostawcy.

2



Fałszywa zmiana rachunku

Poinformowali, że płatności za dostawy należy kierować na nowe konto.

3



Przekierowanie środków

Pracownicy zmienili dane w systemie płatności. Przez kilka miesięcy spółka realizowała przelewy na podstawiony rachunek.

2018

ok. 4 mln zł

trafiło na konto oszustów –
podmiana rachunku dostawcy
(wg RMF FM)



Wniosek: każdą zmianę rachunku kontrahenta należy potwierdzić niezależnym kanałem, np. telefonicznie pod wcześniej znanym numerem.

Umowy ICT: niezależność od dostawcy i usługi chmurowe

OCHRONA PRZED UZALEŻNIENIEM OD DOSTAWCY IT

Vendor lock-in: zabezpieczenie zamawiającego przed monopolem jednego dostawcy przy zakupie rozwiązań chmurowych i infrastruktury.



Pola eksploatacji

Precyzyjne określenie zakresu korzystania z zamawianego rozwiązania.



Kody źródłowe

Uregulowanie praw do kodów źródłowych.



Biblioteki open-source

Uwzględnienie ich wykorzystania w architekturze rozwiązania.



Otwarte interfejsy API

Wymóg otwartych interfejsów jako element ograniczania monopolu wykonawczego.

BEZPIECZNE ZAKUPY USŁUG CHMUROWYCH

Zakres zamówienia:

usługi chmurowe w modelach

SaaS

PaaS

IaaS



SLA i dostępność

Kluczowe metryki SLA oraz gwarancje dostępności usług.



Audytoralność danych

Możliwość kontroli danych i spełniania wymagań zamawiającego.



Exit strategy

Procedury bezpiecznego wyjścia z usługi i zmiany dostawcy.

Przesłanki odrzucenia oferty ICT

Zamawiający odrzuca ofertę, jeżeli:



pkt 17

Rekomendacja – art. 33 ust. 4 UKSC

obejmuje ona produkt ICT, usługę ICT lub proces ICT wskazane w rekomendacji, o której mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20 i 252), stwierdzającej ich negatywny wpływ na podstawowy interes bezpieczeństwa państwa;



pkt 19

Dostawca wysokiego ryzyka – art. 67b ust. 15 UKSC

obejmuje ona produkt ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 67b ust. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, lub usługę ICT, lub proces ICT, określone w tej decyzji.

Nowe podstawy odrzucania ofert obowiązują od 3 kwietnia 2026 r.

Weryfikacja ICT w SWZ i wymagane dokumenty

Zamawiający opisuje mechanizm weryfikacji już w SWZ. Nie odkłada jego określenia do etapu badania ofert.

MECHANIZM WERYFIKACJI

- 1 Zakaz w SWZ**
Zakaz stosowania niedozwolonych rozwiązań ICT.
- 2 Elementy ICT w ofercie**
Obowiązek wskazania przez wykonawcę elementów ICT jako części oferty.
- 3 Zmiany ICT w umowie**
Zabezpieczenie zmian komponentów w projektowanych postanowieniach umowy (PPU).
- 4 Jasne wymagania**
Wykonawca zna oczekiwane informacje, oświadczenia i dokumenty. Zamawiający uzyskuje wiedzę potrzebną do oceny ryzyka.

INFORMACJE I DOKUMENTY DOTYCZĄCE ICT

Produkty: Oświadczenie o producencie i pochodzeniu kluczowych produktów ICT.

Łańcuch dostaw: Informacje o łańcuchu dostaw.

Utrzymanie: Zasady aktualizacji i serwisu oraz informacje o podwykonawcach uczestniczących w utrzymaniu systemu.

Dokumentacja techniczna: Potwierdzenie zgodności oferty z wymaganiami SWZ.

Status dokumentu: Czy dokument stanowi część oferty, czy przedmiotowy środek dowodowy.

Realizacja umowy ICT



Co w sytuacji, gdy niedozwolony komponent ICT pojawia się w trakcie realizacji umowy?



Podział odpowiedzialności

Nie należy przerzucać całego ryzyka przyszłych rekomendacji i decyzji na wykonawcę. Zamawiający odpowiada za przebieg postępowania i jest jego gospodarzem.



Weryfikacja oferty

Same oświadczenia wykonawcy nie wystarczą. Zamawiający sprawdza ofertę z rekomendacjami i decyzjami.



Zabezpieczenie umowy

Projektowane postanowienia umowy powinny uwzględniać zmiany elementów ICT.

DOWODY, ASYSTA TECHNICZNA I ODBIORY ICT



Przedmiotowe środki dowodowe

Weryfikacja raportów z testów, norm ISO i certyfikatów bezpieczeństwa.



Dedykowana Asysta Techniczna (DAT)

Zakres asysty a dopuszczalne modyfikacje kodu.



Zmiany umowy

Ocena modyfikacji w kontekście art. 454 i 455 PZP.



Odbiory systemu

Procedury FAT/SAT oraz klasyfikacja błędów systemowych.

Rekomendacje

PRZED POSTĘPOWANIEM

- 1** Analiza ryzyka przed każdym zamówieniem ICT i klasyfikacja: krytyczny, wysoki, średni lub niski poziom ryzyka.
- 2** Aktualizacja SWZ, OPZ i PPU: NIS 2, UKSC, SBOM, podatności, incydenty i audyty.
- 3** Proporcjonalne wymagania, które nie ograniczają konkurencji.

W POSTĘPOWANIU

- 4** Weryfikacja wykonawców pod kątem dostawców wysokiego ryzyka.
- 5** Ocena ofert także według czasu reakcji, obsługi podatności i ciągłości działania.

W UMOWIE I REALIZACJI

- 6** Plan wyjścia w umowie: bezpieczna zmiana dostawcy i migracja danych.
- 7** Symetria kar umownych i zrównoważona odpowiedzialność stron.
- 8** Regularne audyty dostawców i usług ICT, zwłaszcza o wysokiej i krytycznej istotności.
- 9** Ciągły monitoring zmian regulacyjnych i zagrożeń cyber.

Kluczowy wniosek: zamówienia publiczne jako element zarządzania ryzykiem cyber – a nie wyłącznie procedura zakupowa.

Warsztat: klauzule IT i audyt SLA

01



Analiza PPU

Porównanie wzorcowych i wadliwych klauzul projektowanych postanowień umowy w branży IT.

02



Audyt SLA

Analiza zapisów dotyczących poziomu świadczenia usług.

03



Studia przypadków

Omówienie nieudanych wdrożeń oraz postępowań kontrolnych RIO/NIK.



Dziękuję za uwagę
Zapraszam do kontaktu

[linkedin.com/in/tomasz-chomicki](https://www.linkedin.com/in/tomasz-chomicki)

Tomasz.Chomicki@piit.org.pl