URZĄD MARSZAŁKOWSKI
WOJEWÓDZTWA POMORSKIEGO

CyberPomorze 2030

Gdańsk, lipiec 2026 r.

Departament Cyfryzacji

CyberPomorze 2030: Dlaczego?

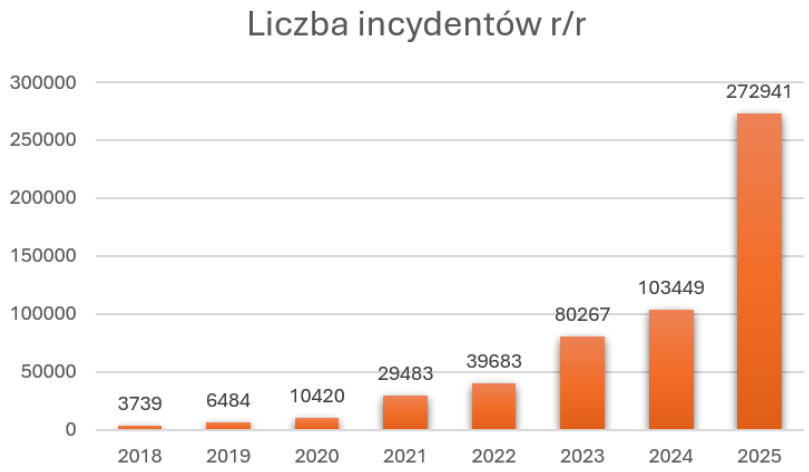


Tabela 3. Zestawienie liczby incydentów w klasyfikacji zgodnej z UKSC

Rodzaje incydentów zgodnie z art. 2 pkt. 5-9 UKSC	Krytyczne (2024)	Krytyczne (2025)	Poważne (2024)	Poważne (2025)	Istotne (2024)	Istotne (2025)	W podmiotach publicznych (2024)	W podmiotach publicznych (2025)
CSIRT NASK	0	0	57	27	0	0	3 450	5 111
CSIRT GOV	0	0	6	13	0	1	3	39
CSIRT MON	0	0	0	0	0	0	35	54
Suma:	0	0	63	40	0	1	3 488	5 204
Zmiana:		0%		-36,5%		+100%		+49,2%

Ataki na stacje uzdatniania wody (Szczytno, Małdyty, Tolkmicko, Sierakowo, Jabłonna Lacka) 2025/26

Samodzielny Publiczny Wojewódzki Szpital Zespolony w Szczecinie poinformował o zawieszeniu do odwołania części swoich usług (ransomware)

Bonifraterskie Centrum Medyczne - odpowiada za funkcjonowanie trzech szpitali oraz ośmiu innych placówek medycznych (ransomware)

Wyciek danych osób powiązanych z partią Nowa Nadzieja cyberdefence24.pl

STYCZEŃ — LUTY — MARZEC — KWIECIEŃ — MAJ — CZERWIEC 2026

Dane rodziców i dzieci żłobka w Łodzi niebezpiecznik.pl

Fałszywe maile od mObywatela, Ergo Hestia, mBanku, o zwrocie ze „skarbówki", NFZ, gov.pl

Wyciekły dane prawie 40 tys. osób operatora Słupskiej i Usteckiej Karty Mieszkańca - włamanie cyberdefence24.pl

Centrum Medyczne „Eskulap" w Raciborzu (ransomware)

Ataki na oczyszczalnie ścieków – (Chodaczów, woj. podkarpackie, Wydminy, Kuźnica, Witkowo) 2025/26

Włamanie do Szpitala Uniwersyteckiego (przejęcie konta pocztowego) i Szpitala MSWiA w Krakowie (ransomware).

Raport ENISA 2026, opublikowany przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa, potwierdza, że administracja publiczna jest najbardziej atakowanym sektorem w całej UE – odpowiada za ok. 38,5 proc. wszystkich incydentów

CyberPomorze 2030: Dlaczego?

Nowelizacja Ustawy o Krajowym Systemie Cyberbezpieczeństwa

- Dzieli podmioty na: kluczowe i ważne
- Nakłada na podmioty szereg obowiązków w obszarze: zarządczym, organizacyjnym, technicznym, np.:

Zidentyfikować bądź zaktualizować spis **aktywów informacyjnych** wykorzystywanych przy świadczeniu usług

Prowadzić **systematyczne szacowanie ryzyka** wystąpienia incydentu oraz **zarządzać** tym ryzykiem

Przygotowywać i wdrażać **plany awaryjne** oraz **plany odtworzenia działalności** umożliwiające odtworzenie systemu informacyjnego po zdarzeniu i świadczenie usług

Objąć system informacyjny wykorzystywany do świadczenia usługi **systemem monitorowania w trybie ciągłym 24/7**

Zapewnić **bezpieczeństwo łańcucha dostaw produktów i usług**, dokonać przeglądu posiadanych produktów i usług

Stosować polityki i procedury stosowania **kryptografii**, w tym **szyfrowania, zabezpieczenia MFA**

Wdrażać, dokumentować, testować i utrzymywać **plany ciągłości działania** umożliwiające ciągłe i niezakłócone świadczenie usługi

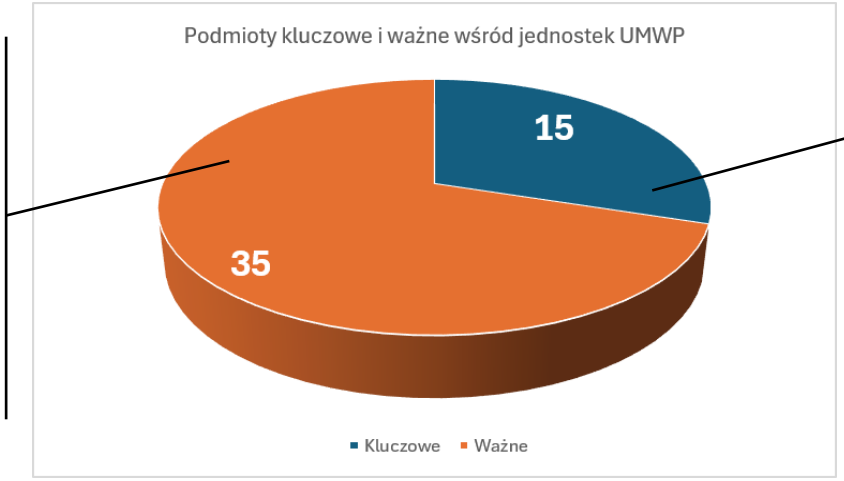
Zaktualizować/wdrożyć procedury dot. **bezpieczeństwa fizycznego, zasobów ludzkich i środowiskowego** uwzględniające kontrole dostępu

Stosować **środki zapobiegające i ograniczające wpływ incydentów** na bezp. systemu informacyjnego wykorzystywanego do świadczenia usługi

- Nakłada kary administracyjne na kierowników jednostek

m.in.:

- Wojewódzki Ośrodek Medycyny Pracy
- Muzeum Zachodniokaszubskie w Bytowie
- Pomorska Biblioteka Pedagogiczna w Słupsku
- Opera Bałtycka w Gdańsku
- Wojewódzki Urząd Pracy
- Centrum Zdrowia Psychicznego w Słupsku
- Pomorska Medyczna Szkoła Policealna, Gdańsk

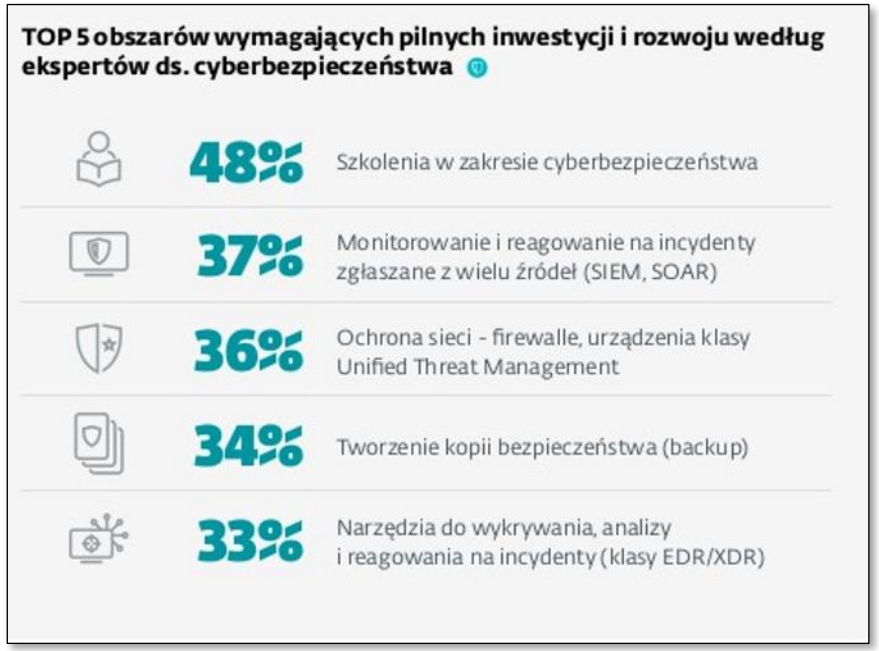


m.in.:

- Pomorska Kolej Metropolitalna
- Copernicus – podmiot leczniczy
- Szpitale Pomorskie
- Zarząd Dróg Wojewódzkich
- Pomorskie Biuro Planowania Regionalnego

CyberPomorze 2030: na czym się koncentrujemy?

Cel: Zapewnienie efektywnego wsparcia w działaniach na rzecz podniesienia poziomu cyberbezpieczeństwa i dostosowania się do wymogów ustawy o Krajowym Systemie Cyberbezpieczeństwa



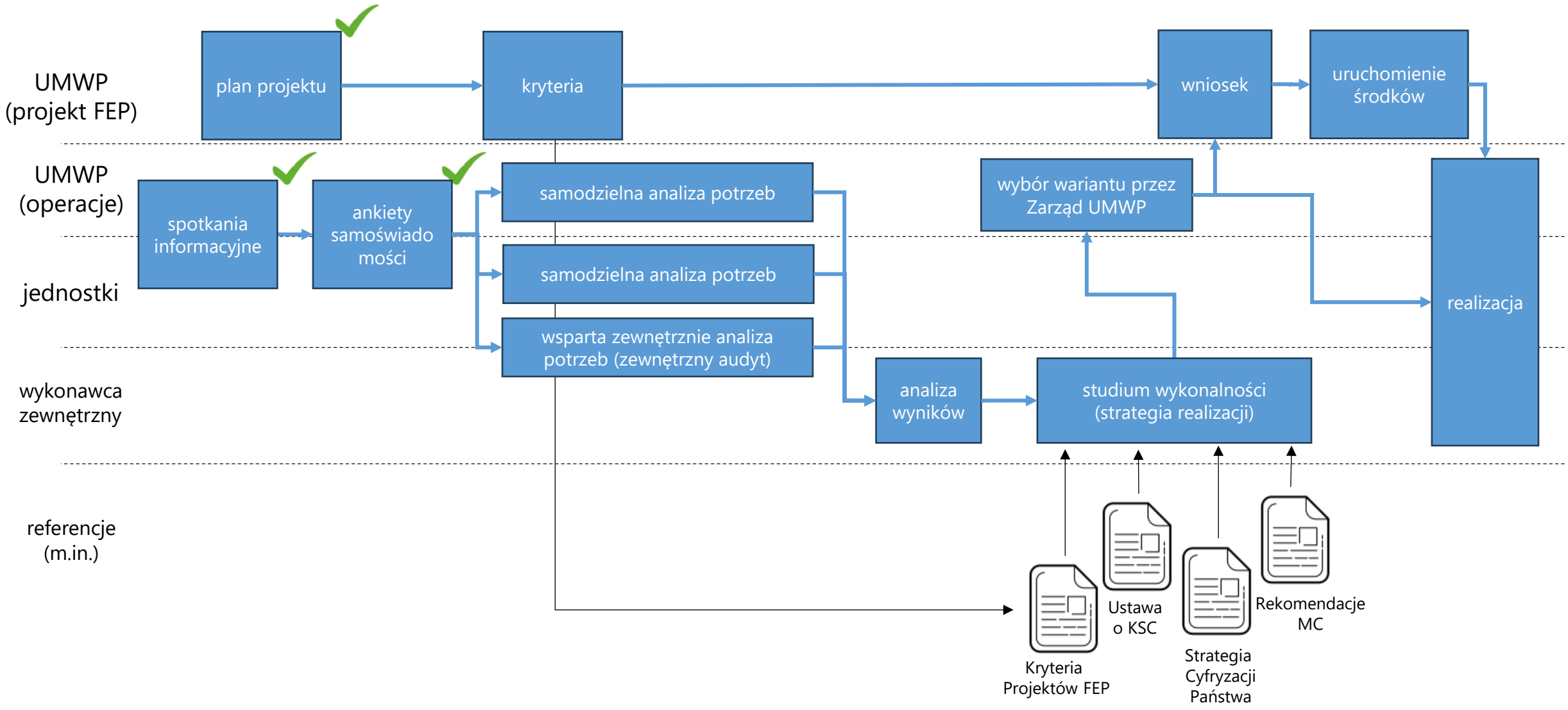
- Obszary pierwszoplanowe (techniczne):
  - Migracja do chmury jako odpowiedź na braki infrastrukturalne, zasobowe, kompetencyjne
  - Kopie zapasowe w chmurze jako element georedundancji
  - Ochrona stacji roboczych (oprogramowanie XDR)
  - Ochrona sieci informatycznych (Firewall)
  - Środki i narzędzia do utrzymania ciągłości działania (UPS)
  - Monitorowanie i reagowanie na incydenty (usługi SOC, oprogramowanie SIEM, SOAR)
  - Audyty bezpieczeństwa i gotowości do UKSC
- Obszary drugoplanowe (organizacja i wiedza):
  - Polityki bezpieczeństwa, procedury, etc.
  - Szkolenia z cyberbezpieczeństwa i cyberhigieny

Sprzymierzeńcy: efekt synergii, efekt skali

skomplikowane, trudne, drogie

łatwe, dostępne

CyberPomorze 2030: gdzie jesteśmy?



URZĄD MARSZAŁKOWSKI
WOJEWÓDZTWA POMORSKIEGO

Dziękuję za uwagę