Ministerstwo Cyfryzacji

Departament Cyberbezpieczeństwa

SPRAWOZDANIE

Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa

za 2025 rok

2026

TLP: CLEAR

2026

Sprawozdanie

Pełnomocnika Rządu
do Spraw Cyberbezpieczeństwa

za 2025 rok

TOM I – PODSUMOWANIE ZARZĄDCZE

SPIS TREŚCI TOM I

WSTĘP

Rok 2025 zapisał się w historii polskiej administracji jako czas wyjątkowej próby dla krajowego systemu cyberbezpieczeństwa (KSC). Dynamiczna ewolucja zagrożeń, napędzana zarówno przez postęp technologiczny, jak i niestabilną sytuację geopolityczną, wymusiła na instytucjach państwa nie tylko wzmożoną czujność operacyjną, ale przede wszystkim głęboką refleksję nad modelem ochrony infrastruktury krytycznej. Niniejsze Sprawozdanie stanowi próbę syntetycznego ujęcia działań podjętych w odpowiedzi na te wyzwania, kreśląc obraz polskiej cyberprzestrzeni jako obszaru ścierania się nowoczesnych metod ochrony z coraz bardziej wyrafinowanymi formami agresji cyfrowej.

Główną cechą dominującą dla minionego roku była transformacja architektury bezpieczeństwa, wynikająca z konieczności dostosowania krajowego porządku prawnego do wymogów unijnej dyrektywy NIS 2. Proces ten, zbiegający się w czasie z historycznym wyzwaniem, jakim była prezydencja Rzeczypospolitej Polskiej w Radzie Unii Europejskiej, postawił cyberbezpieczeństwo w samym centrum agendy politycznej państwa. W niniejszym dokumencie analizujemy, w jaki sposób Polska wykorzystała ten czas do wzmocnienia swojej pozycji lidera w regionie, jednocześnie mierząc się z systemowymi problemami, takimi jak deficyt wyspecjalizowanych kadr czy potrzeba automatyzacji procesów analitycznych w obliczu powszechnego wykorzystania sztucznej inteligencji przez adwersarzy.

Podstawą prawną opracowania dokumentu jest art. 63 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (UKSC). Zgodnie z jego brzmieniem, Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa przedkłada Radzie Ministrów roczne sprawozdanie, będące zapisem aktywności państwa w zakresie zapewnienia bezpieczeństwa teleinformatycznego na poziomie krajowym. Dokument jest efektem szerokiej współpracy międzyresortowej – został przygotowany przez Departament Cyberbezpieczeństwa Ministerstwa Cyfryzacji w oparciu o dane przekazane przez zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) poziomu krajowego, organy właściwe do spraw cyberbezpieczeństwa, sektorowe zespoły cyberbezpieczeństwa, służby specjalne, organy ścigania i inne instytucje publiczne.

W strukturze sprawozdania szczególną uwagę poświęcono nie tylko analizie ryzyk i incydentów, ale także inicjatywom edukacyjnym i technologicznym, które mają na celu budowanie cyfrowej odporności całego społeczeństwa. Całość zamyka diagnoza wyzwań oraz strategiczne rekomendacje na rok 2026, mające służyć jako drogowskaz dla dalszego wzmacniania suwerenności cyfrowej Rzeczypospolitej Polskiej.

Z uwagi na znaczną objętość materiału analitycznego, niniejsze sprawozdanie zostało podzielone na trzy części:

- **Tom I – Podsumowanie zarządcze**: zawierające kluczowe wnioski strategiczne oraz syntetyczne ujęcie stanu cyberbezpieczeństwa państwa.
- **Tom II – Wkłady informacyjne podmiotów KSC**: obejmujący szczegółowe dane i raporty przekazane przez podmioty wchodzące w skład KSC.
- **Załącznik niejawny**: przekazany wyłącznie podmiotom ustawowo uprawnionym, obejmujący informacje o szczególnym znaczeniu dla bezpieczeństwa państwa.

Niniejszy dokument stanowi zestawienie dwóch pierwszych elementów: Tomu I oraz Tomu II.

PODSUMOWANIE ZARZĄDCZE

Miniony rok był okresem wyraźnej dynamiki w polskiej cyberprzestrzeni oraz czasem intensywnych przygotowań KSC do zmian strukturalnych. Cyfryzacja procesów państwowych i gospodarczych, w połączeniu z kluczową pozycją geopolityczną Polski – w tym trwającą wojną na Ukrainie i działaniami hybrydowymi obcych służb – sprawiły, że krajowa infrastruktura znajdowała się pod stałą presją zaawansowanych cyberataków. Odzwierciedlają to dane operacyjne. **CSIRT poziomu krajowego obsłużyły łącznie blisko 273 tys. incydentów (wzrost o 144,4%) z czego sam tylko zespół CSIRT NASK odnotował skokowy wzrost obsłużonych incydentów do ponad 260 tysięcy, co stanowi wzrost o 152% w stosunku do roku ubiegłego, CSIRT MON – 7 125 incydentów (wzrost o blisko 69%), a CSIRT GOV obsłużył 5 033 incydenty (wzrost o 26%).**

Krajobraz zagrożeń w 2025 r. zdominowały zjawiska związane z profesjonalizacją cyberprzestępczości oraz aktywnością grup APT powiązanych ze służbami specjalnymi Rosji i Białorusi. Kluczowym wektorem ataków stało się wykorzystanie sztucznej inteligencji (AI), która umożliwiła m.in. masową automatyzację kampanii socjotechnicznych. Równolegle, największe straty operacyjne i systemowe generowały ataki typu ransomware, ataki wolumetryczne DDoS oraz coraz precyzyjniejsze uderzenia w łańcuchy dostaw i dostawców usług zewnętrznych (IT/OT) obsługujących podmioty kluczowe.

Największym systemowym wyzwaniem dla KSC w minionym roku był niedobór wysoko wykwalifikowanych specjalistów oraz ograniczenia finansowe w sektorze publicznym. Nowelizacja KSC skokowo zwiększy liczbę objętych systemem podmiotów kluczowych i podmiotów ważnych, z których wiele – szczególnie w sektorze ochrony zdrowia czy samorządach – charakteryzuje się stosunkowo niską odpornością i będzie wymagało znacznego wsparcia technicznego, merytorycznego i finansowego.

Odpowiedzią na te wyzwania była mobilizacja wewnątrz systemu. Zainicjowano proces budowy i rozwoju nowych sektorowych CSIRT-ów m.in. dla sektora infrastruktury, energii czy cyfryzacji. Systematycznie rozwijano kluczowe platformy wymiany informacji, w tym system S46, a dla obywateli i firm wdrożono innowacyjne narzędzia –jak portal cyber.gov.pl czy moje.cert.pl. Ogromną rolę w bieżącej koordynacji działań międzyresortowych, wymianie wiedzy operacyjnej i analitycznej odgrywało Połączone Centrum Operacyjne Cyberbezpieczeństwa (PCOC) jako komórka koordynacyjna.

Podsumowując, KSC w 2025 r. kolejny raz dowiódł swojej sprawności reagowania na bieżące kryzysy. Jednak sprostanie wyzwaniom kolejnych lat – w szczególności masowemu użyciu AI przez adwersarzy oraz gigantycznemu poszerzeniu systemu w ramach implementacji dyrektywy NIS2 do polskiego prawa – będzie bezwzględnie wymagało zwiększenia finansowania na etaty eksperckie, silniejszej automatyzacji procesów analizy zagrożeń oraz ustandaryzowanego wsparcia dla tysięcy nowych podmiotów KSC. Niezbędne jest przy tym wzmocnienie koordynacji na szczeblu krajowym poprzez centralizację nadzoru w ramach jednej instytucji nadrzędnej. Skuteczne zarządzanie rozproszoną strukturą CSIRT-ów sektorowych wymaga silnego ośrodka decyzyjnego, takiego jak PCOC, który zapewni jednolity standard operacyjny i spójną strategię obrony państwa.

Krzysztof Gawkowski

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa

Wiceprezes Rady Ministrów

Minister Cyfryzacji

STRUKTURA KSC

KSC w Polsce opiera się na strukturze zdefiniowanej UKSC. Architektura tego systemu została zaprojektowana w sposób wielopoziomowy, aby zapewnić skuteczną współpracę między podmiotami na szczeblu strategicznym, operacyjno-koordynacyjnym oraz technicznym.

Zgodnie z zapisami ustawy oraz dotychczasową praktyką funkcjonowania KSC, jego struktura przedstawia się następująco:

1. Poziom strategiczny i decyzyjny:

- **Prezes Rady Ministrów, Rada Ministrów i Pełnomocnik Rządu ds. Cyberbezpieczeństwa** - stanowią centralny element decyzyjny kształtujący politykę KSC. W 2025 r. funkcję Pełnomocnika pełnił Minister Cyfryzacji (w randze Wiceprezesa Rady Ministrów), co zapewnia efektywną koordynację działań.
- **Kolegium do Spraw Cyberbezpieczeństwa**. Pełni funkcję organu opiniodawczo-doradczego przy Radzie Ministrów. W jego skład wchodzą przedstawiciele najważniejszych instytucji odpowiedzialnych za bezpieczeństwo narodowe i publiczne (m.in. MSWiA, MON, służby specjalne, Rządowe Centrum Bezpieczeństwa).

2. Poziom koordynacyjny i wymiany informacji:

- **Ministerstwo Cyfryzacji**. Odpowiada za bezpieczeństwo cyberprzestrzeni w wymiarze cywilnym, zapewnia obsługę Pełnomocnika i pełni funkcję Pojedynczego Punktu Kontaktowego do spraw cyberbezpieczeństwa na arenie międzynarodowej (m.in. we współpracy z Unią Europejską).
- **PCOC.** Ta nieformalna platforma koordynacyjna ułatwiająca szybką, techniczną wymianę danych o zdarzeniach i incydentach między CSIRT-ami poziomu krajowego, służbami i kluczowymi resortami.
- **Zespół do Spraw Incydentów Krytycznych (ZIK**). Gremium koordynacyjno-kryzysowe zwoływane w sytuacjach zakłócenia poufności, integralności lub dostępności krytycznych zasobów państwa.

3. Poziom operacyjny i techniczny (Reagowanie na incydenty):

- Zespoły CSIRT poziomu krajowego: Trzy główne zespoły odpowiedzialne za monitorowanie i obsługę incydentów w przydzielonych im sektorach:
  - CSIRT GOV (prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego) – odpowiada m.in. za administrację państwową i infrastrukturę krytyczną.
  - CSIRT MON (prowadzony przez Ministra Obrony Narodowej) – zabezpiecza resort obrony narodowej oraz Siły Zbrojne RP.
  - CSIRT NASK (prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy) – obsługuje m.in. samorządy, obywateli, przedsiębiorstwa i podmioty z wybranych sektorów.
- Sektorowe zespoły cyberbezpieczeństwa: Wyspecjalizowane jednostki wspierające konkretne dziedziny gospodarki. W 2025 r. aktywnie funkcjonowały:
  - CSIRT KNF (dla sektora bankowego i infrastruktury rynków finansowych);
  - CSIRT CeZ (dla sektora ochrony zdrowia).

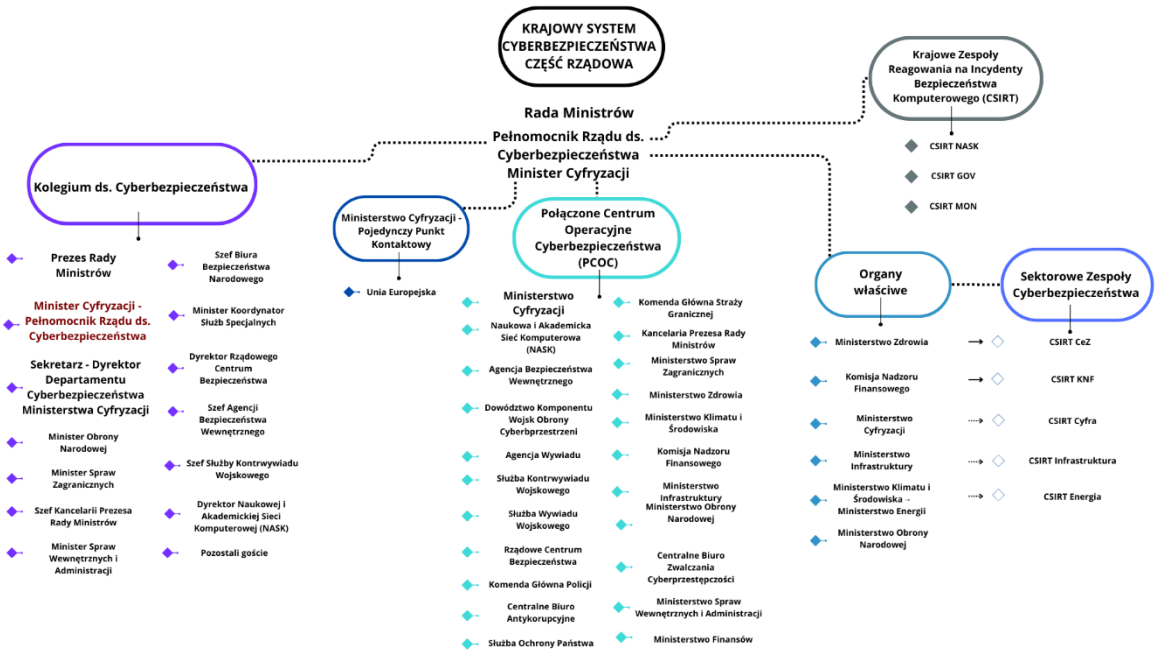
Ponadto w 2025 r. trwały intensywne prace (wspierane z funduszy KPO) nad budową nowych zespołów, m.in. CSIRT Infrastruktura oraz CSIRT Cyfra.

4. Poziom nadzorczy:

- **Organy właściwe do spraw cyberbezpieczeństwa** - Ministrowie kierujący odpowiednimi działami administracji rządowej (Minister Klimatu i Środowiska, Minister Energii, Minister Infrastruktury, Minister Zdrowia, Minister Obrony Narodowej oraz Minister Cyfryzacji, Minister Zdrowia oraz Komisja Nadzoru Finansowego, odpowiedzialni za prowadzenie nadzoru nad podmiotami KSC, kontrolę, audyty i ustanawianie sektorowch zespołów cyberbezpieczeństwa.

5. Uczestnicy systemu (odbiorcy obowiązków i wsparcia):

- **Podmioty chronione**. Składają się na nie m.in. operatorzy usług kluczowych (OUK), dostawcy usług cyfrowych (DUC), jednostki sektora finansów publicznych, instytuty badawcze oraz przedsiębiorcy telekomunikacyjni. *W obliczu wdrażania znowelizowanej UKSC (dyrektywa NIS2), kategoria ta ulegnie głębokiej transformacji, obejmując szeroki katalog "podmiotów kluczowych i ważnych".*



Ilustracja 1 Schemat KSC

PEŁNOMOCNIK RZĄDU DO SPRAW CYBERBEZPIECZEŃSTWA

PRZEGLĄD KRAJOBRAZU CYBERPRZESTRZENI 2025 R.

Rok 2025 w polskiej cyberprzestrzeni charakteryzował się bezprecedensowym natężeniem wrogich działań i dynamiczną ewolucją wektorów ataków, co znalazło odzwierciedlenie w skokowym wzroście liczby rejestrowanych incydentów. **Zespół CSIRT NASK obsłużył aż 260 783 incydenty (wzrost o 152% w stosunku do roku ubiegłego), CSIRT MON – 7 125 incydentów (wzrost o blisko 69%), a CSIRT GOV obsłużył 5 033 incydenty (wzrost o 26%).** Sytuacja ta była bezpośrednio zdeterminowana kluczową pozycją geopolityczną Polski jako głównego węzła logistycznego wspierającego walczącą Ukrainę oraz masową adaptacją nowych technologii przez cyberprzestępców.

ZDIAGNOZOWANE PRZEZ PODMIOTY KSC TRENDY W 2025 R:

1. Sztuczna inteligencja (AI) jako "mnożnik siły" adwersarzy W 2025 roku sztuczna inteligencja stała się kluczowym narzędziem dla grup cyberofensywnych. Modele językowe były powszechnie wykorzystywane do automatycznego generowania wysoce spersonalizowanych i bezbłędnych językowo wiadomości phishingowych, trudnych do odróżnienia od prawdziwej komunikacji. Ponadto technologia *deepfake* (syntetyczne nagrania audio i wideo) służyła do podszywania się pod urzędników czy osoby publiczne w celu manipulacji. AI przyspieszyło również etap techniczny ataków, automatyzując rekonesans, omijając reguły detekcji oraz wspomagając pisanie złośliwych skryptów.

2. Zaawansowana aktywność grup państwowych (APT) i destrukcyjny haktywizm Trwający konflikt sprawił, że polska infrastruktura znajdowała się pod stałą presją grup APT powiązanych ze służbami specjalnymi Federacji Rosyjskiej i Białorusi. Działania te obejmowały cyberszpiegostwo, kradzież danych i operacje destrukcyjne. Najpoważniejszym tego przykładem był **skoordynowany atak z końca grudnia 2025 r. wymierzony w sektor energii** – adwersarze wykorzystali oprogramowanie typu *wiper* (mające na celu nieodwracalne zniszczenie danych) do ataku na ponad 30 farm wiatrowych i fotowoltaicznych oraz dużą elektrociepłownię. Ponadto obserwowano wysoką aktywność prorosyjskich grup haktywistycznych, przeprowadzających potężne ataki wolumetryczne DDoS (sięgające 1.3 Tbps) m.in. na infrastrukturę finansową w trakcie wyborów prezydenckich w Polsce. Aby utrudnić atrybucję i ukryć swoje działania, aktorzy państwowi powszechnie wykorzystywali jako infrastrukturę anonimizacyjną podatne, domowe routery brzegowe (urządzenia SOHO).

3. Cyberprzestępczość jako usługa (CaaS) i ewolucja Ransomware Rozwój czarnego rynku IT doprowadził do popularyzacji modelu usługowego, takiego jak *Ransomware-as-a-Service* (RaaS) czy usługi brokerów dostępu początkowego (IAB). Obniżyło to barierę wejścia dla cyberprzestępców, umożliwiając masowe ataki na mniejsze, słabiej zabezpieczone podmioty. Ataki ransomware pozostawały jednym z najbardziej niszczycielskich zagrożeń, opierając się na tzw. podwójnym wymuszeniu – szyfrowaniu systemów połączonym z kradzieżą danych i groźbą ich publikacji w *darknecie*. Silnie dotknięty tym wektorem był m.in. sektor zdrowia, czego przykładem był poważny paraliż infrastruktury podmiotu medycznego MSWiA w Krakowie.

4. Uderzenia w łańcuchy dostaw (Supply Chain Attacks) Dostrzegając rosnące koszty i trudności w atakowaniu dobrze chronionych podmiotów kluczowych, adwersarze coraz częściej obierali za cel ich słabiej zabezpieczonych kontraktorów i dostawców usług zewnętrznych (IT/OT). Kompromitacja pojedynczego dostawcy lub serwisanta (np. urządzeń brzegowych) pozwalała atakującym na łatwy dostęp do środowisk informatycznych wielu instytucji rządowych i operatorów infrastruktury krytycznej jednocześnie.

5. Masowe oszustwa i inżynieria społeczna ewoluująca do prywatnych komunikatorów Oszustwa komputerowe były w 2025 r. najpowszechniejszym cyberzagrożeniem – stanowiły aż 97% wszystkich incydentów obsłużonych przez CSIRT NASK (ponad 253 tysiące zgłoszeń). Dominowały fałszywe inwestycje promowane w mediach społecznościowych, bezprawnie wykorzystujące wizerunki znanych firm (np. koncernów energetycznych) i polityków. Znaczącym nowym trendem w omijaniu korporacyjnych systemów bezpieczeństwa (takich jak filtry anty-spamowe poczty elektronicznej) stało się przenoszenie komunikacji na prywatne, szyfrowane end-to-end komunikatory (Signal, WhatsApp), co pozwala na ominięcie korporacyjnych systemów monitorowania i prewencji.

ZGŁOSZENIA I INCYDENTY CYBERBEZPIECZEŃSTWA

INCYDENTY:

Sumaryczne zestawienie zarejestrowanych incydentów przez CSIRT-y poziomu krajowego zwarto w tabeli poniżej:

Tabela 1. Zestawienie liczby zarejestrowanych incydentów za 2025 r.

CSIRT poziomu krajowego:	2024 r.	2025 r.	Zmiana procentowa:
CSIRT NASK	103 449	260 783	+152%
CSIRT GOV	3 991	5 033	+26,1%
CSIRT MON	4 220	7 125	+68,9%
Sumaryczna roczna liczba zarejestrowanych incydentów:	**111 660**	**272 941**	**+144,4%**

Tabela 2. Zestawienie incydentów

Zespół CSIRT	2023 r.	Zmiana 2023/2024	2024 r.	Zmiana 2024/2025	2025 r.
CSIRT NASK	80 267	+29%	103 449	+152%	260 783
CSIRT GOV	4 676	-15%	3 991	+26,1%	5 033
CSIRT MON	5 841	-28%	4 220	+68,9%	7 125
SUMA (Kraj)	**90 784**	**+23%**	**111 660**	**+144,4%**	**272 941**

Kluczowe wnioski z zestawienia:

- **Skokowy wzrost w 2025 r.:** Łączna liczba incydentów w skali całego kraju w 2025 roku wzrosła w sposób bezprecedensowy, osiągając blisko 273 tysiące. Stanowi to drastyczny wzrost o ponad 144% w stosunku do roku poprzedniego.
- **Dominacja CSIRT NASK:** Zespół NASK odpowiada za przytłaczającą większość (ok. 95%) rejestrowanych w Polsce incydentów. To właśnie w tym zespole odnotowano największą dynamikę wzrostu (+152% w 2025 r.), co wynika m.in. z masowych kampanii phishingowych uderzających w obywateli i podmioty samorządowe.
- **Odwrócenie trendu dla GOV i MON:** W roku 2024 CSIRT GOV oraz CSIRT MON zanotowały spadki liczby incydentów (odpowiednio o 15% i 28%). Jednak rok 2025 przyniósł ponowny, wyraźny wzrost złośliwej aktywności w ich zakresie odpowiedzialności – CSIRT GOV odnotował wzrost o 26,1%, a CSIRT MON aż o blisko 69%.

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%

ZGŁOSZENIA:

W zakresie zgłoszeń w 2025 r. CSIRT-y poziomu krajowego otrzymały łącznie **682 245** zgłoszeń naruszeń bezpieczeństwa systemów teleinformatycznych, co stanowi wzrost o ponad 10% w stosunku do roku poprzedniego (619 486 zgłoszeń).

Szczególnie istotna dynamika nastąpiła w zestawieniu obsługiwanym przez CSIRT NASK. Chociaż liczba samych zgłoszeń wzrosła r/r o 10% (do 658 320), to liczba potwierdzonych incydentów wzrosła aż o 152%. Średnia dzienna liczba obsługiwanych przez ten zespół incydentów wzrosła z 283 w 2024 r. do 714 w roku 2025. Stosunek liczby incydentów do zarejestrowanych zgłoszeń wzrósł z 17% do niemal 40%.

Tabela 4. Zestawienie zgłoszeń i incydentów dla CSIRT NASK

Rok	Zgłoszenia	Średnia dzienna	Incydenty	Średnia dzienna	Stosunek incydentów do zgłoszeń
2024	600 990	1 646	103 449	283	17%
2025	658 320	1 803	260 783	714	39,6%
Zmiana	**+9,5%**	**+9,5%**	**+152%**	**+152%**	**+22,6 p.p.**

Tabela 5. Zestawienie zgłoszeń i incydentów dla CSIRT NASK (2023-2025) uwzględniające zmiany r/r

Rok	Całkowita liczba zgłoszeń	Zmiana zgłoszeń (r/r)	Średnia dzienna zgłoszeń	Potwierdzone incydenty	Zmiana incydentów (r/r)	Średnia dzienna incydentów	Stosunek inc. do zgł.	Zmiana stosunku (r/r)
2023	371 089	-	1 017	80 267	-	220	22%	-
2024	609 900*	**+64%**	1 671*	103 449	**+29%**	283	17%	**-5 p.p.**
2025	658 320	**+9,5%****	1 803	260 783	**+152%**	714	39,6%	**+22,6 p.p.**

Kluczowe wnioski z analizy dynamiki zmian: Tabela dobitnie ukazuje, że choć dynamika napływu samych zgłoszeń od obywateli i instytucji ustabilizowała się (wzrost zaledwie o 9,5% r/r w 2025 r., wobec skoku o 64% w 2024 r.), to dynamika realnych zagrożeń (potwierdzonych incydentów) wystrzeliła w sposób bezprecedensowy, osiągając wzrost aż o 152% r/r w 2025 r. Pokazuje to również drastyczny wzrost wskaźnika "skuteczności" lub celności ataków – stosunek potwierdzonych incydentów do wszystkich zgłoszeń zwiększył się o 22,6 punktu procentowego i zbliżył się do granicy 40%.

Zestawienie zgłoszeń i incydentów obsługiwanych przez CSIRT GOV również uległo zauważalnemu wzrostowi po spadkach w roku ubiegłym. Liczba zgłoszeń w ujęciu rocznym zwiększyła się o blisko 33% z 17 439 do 23 136, natomiast liczba incydentów wzrosła o 26% z 3 991 do 5 033, co dało średnią w wysokości blisko 14 zarejestrowanych incydentów dziennie.

Tabela 6. Zestawienie zgłoszeń i incydentów dla CSIRT GOV

Rok	Całkowita liczba zgłoszeń	Zmiana zgłoszeń (r/r)	Średnia dzienna zgłoszeń	Potwierdzone incydenty	Zmiana incydentów (r/r)	Średnia dzienna incydentów	Stosunek inc. do zgł.	Zmiana stosunku (r/r)
2023	19 888	-	54	4 676	-	13	24%	-
2024	17 439	**-12%**	48	3 991	**-15%**	11	23%	**-1 p.p.**
2025	23 136	**+32,6%**	63	5 033	**+26,1%**	14	21,7%	**-1,3 p.p.**

Liczba zgłoszeń zarejestrowanych w 2025 r. w CSIRT MON spadła o 25% (z 1 057 do 789), jednakże w tym samym czasie liczba potwierdzonych incydentów skokowo wzrosła o blisko 69% (z 4 220 do 7 125), dając średnio blisko 20 incydentów zarejestrowanych każdego dnia.

Tabela 7. Zestawienie zgłoszeń i incydentów dla CSIRT MON

Rok	Zgłoszenia	Średnia dzienna	Incydenty	Średnia dzienna
2024	1 057	3	4 220	12
2025	789	2	7 125	20
Zmiana	**-25,3%**	**-33%**	**+68,9%**	**+66%**

UMOCOWANIE INSTYTUCJONALNE PEŁNOMOCNIKA

Zgodnie z art. 60 UKSC, Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa (Pełnomocnik) odpowiada za koordynowanie działań i realizowanie polityki rządu w zakresie zapewnienia cyberbezpieczeństwa w Rzeczypospolitej Polskiej.

W 2025 r., analogicznie do lat poprzednich, funkcję Pełnomocnika pełnił Minister Cyfryzacji (stanowisko to, wraz z funkcją Wiceprezesa Rady Ministrów, piastuje Krzysztof Gawkowski). Tak skonstruowane umocowanie instytucjonalne Pełnomocnika, przybierające postać swoistej unii personalnej z kierownictwem resortu cyfryzacji odpowiedzialnego za KSC, zapewnia maksymalizację efektywności realizowanych przedsięwzięć. Jest to zadanie niezwykle istotne w czasie dynamicznie postępującej cyfryzacji życia publicznego, rosnącej skali i poziomu zaawansowania cyberzagrożeń oraz intensywnych przygotowań państwa do strukturalnych zmian wynikających z nowelizacji UKSC (wdrożenia dyrektywy NIS2).

Dzięki wyżej opisanej konstrukcji, rosnąca liczba oraz ogromna złożoność zadań podejmowanych na poziomie krajowym przez Ministerstwo Cyfryzacji (realizującego zadania ministra właściwego ds. informatyzacji) mogły zostać poprawnie i efektywnie skoordynowane z działaniami realizowanymi przez pozostałe podmioty odpowiadające za zapewnienie cyberbezpieczeństwa RP.

Pełnomocnik wraz z Ministerstwem Cyfryzacji stanowią centralny element decyzyjny i koordynacyjny kształtujący KSC. Zgodnie z art. 4 UKSC, system ten tworzony jest wspólnie przez zróżnicowane podmioty, do których należą m.in.: operatorzy usług kluczowych, dostawcy usług cyfrowych, CSIRT-y poziomu krajowego (CSIRT GOV, CSIRT MON, CSIRT NASK), sektorowe zespoły cyberbezpieczeństwa, organy właściwe do spraw cyberbezpieczeństwa, jednostki sektora finansów publicznych, instytuty badawcze, urzędy centralne, spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej, podmioty świadczące usługi z zakresu cyberbezpieczeństwa, a także Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa.

KOLEGIUM DO SPRAW CYBERBEZPIECZEŃSTWA

Na podstawie art. 64 UKSC przy Radzie Ministrów działa Kolegium do Spraw Cyberbezpieczeństwa. Pełni ono funkcję organu opiniodawczo-doradczego w sprawach cyberbezpieczeństwa oraz działalności w tym zakresie zespołów m.in. CSIRT poziomu krajowego (CSIRT GOV, CSIRT MON, CSIRT NASK), sektorowych zespołów cyberbezpieczeństwa, służb specjalnych i organów właściwych do spraw cyberbezpieczeństwa.

Do zadań Kolegium należy opracowywanie rekomendacji dla Rady Ministrów dotyczących działań w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym. Ponadto, Kolegium odgrywa kluczową rolę w procesie przyznawania środków z Funduszu Cyberbezpieczeństwa – po złożeniu przez uprawnione podmioty wniosków do ministra właściwego ds. informatyzacji, dokumenty spełniające wymagania formalne przekazywane są do Kolegium, które na ich podstawie wydaje opinie w zakresie wnioskowanych kwot (m.in. na świadczenia teleinformatyczne dla specjalistów).

Posiedzenia Kolegium są organizowane przez Ministerstwo Cyfryzacji, które obsługuje również Sekretarza Kolegium. Przebieg prac Kolegium oraz treść wyrażonych stanowisk, rekomendacji i opinii mają charakter niejawny w rozumieniu przepisów ustawy o ochronie informacji niejawnych.

W 2025 r. odbyły się trzy posiedzenia Kolegium. Prace organu w raportowanym okresie koncentrowały się przede wszystkim na zapewnieniu stabilności kadrowej systemu poprzez ewaluację wniosków o wsparcie z Funduszu Cyberbezpieczeństwa oraz na strategicznym opiniowaniu wymogów bezpieczeństwa dla krytycznej infrastruktury telekomunikacyjnej (sieci 5G). Istotnym elementem obrad była również problematyka systemowego zwalczania dezinformacji oraz analiza wniosków płynących z dotychczasowej działalności systemu w świetle rocznego Sprawozdania Pełnomocnika. Szczegółowe zagadnienia omówione podczas posiedzeń zestawiono w poniższej tabeli:

Tabela 8. Zestawienie tematyki Kolegium ds. Cyberbezpieczeństwa w 2025 r.

Lp.	Tematyka obrad:	Data
1.	1.Wydanie opinii Kolegium do Spraw Cyberbezpieczeństwa w przedmiocie wniosków o udzielenie wsparcia z Funduszu Cyberbezpieczeństwa w zakresie maksymalnych kwot prognozowanych kosztów związanych z przyznaniem świadczenia teleinformatycznego na rok 2025; 2.Przedstawienie Sprawozdania Pełnomocnika Rządu ds. Cyberbezpieczeństwa za 2024 rok. 3.Omówienie harmonogramu prac Kolegium w br. – przedstawienie propozycji zagadnień przez członków posiedzenia.	27.03.2025
2.	1.Wydanie opinii Kolegium do Spraw Cyberbezpieczeństwa w sprawie aukcji UKE i wymagań bezpieczeństwa dla sieci 5G w paśmie 1710,0–1710,2 MHz oraz 1805,0–1805,2 MHz. 2.Stworzenie krajowych ram przeciwdziałania dezinformacji. 3.Wydanie opinii Kolegium do Spraw Cyberbezpieczeństwa w przedmiocie wniosków o udzielenie wsparcia z Funduszu Cyberbezpieczeństwa w zakresie maksymalnych kwot prognozowanych kosztów związanych z przyznaniem świadczenia teleinformatycznego na rok 2025.	06.10.2025
3.	1.Wydanie opinii Kolegium do Spraw Cyberbezpieczeństwa w sprawie aukcji UKE i wymagań bezpieczeństwa dla sieci 5G w paśmie 1710,0–1710,2 MHz oraz 1805,0–1805,2 MHz. 2.Wydanie opinii Kolegium do Spraw Cyberbezpieczeństwa w przedmiocie wniosków o udzielenie wsparcia z Funduszu Cyberbezpieczeństwa w zakresie maksymalnych kwot prognozowanych kosztów związanych z przyznaniem świadczenia teleinformatycznego na rok 2025 (udział tylko ustawowych członków i uczestników Kolegium).	06.11.2025

POŁĄCZONE CENTRUM OPERACYJNE CYBERBEZPIECZEŃSTWA (PCOC)

W celu efektywnej koordynacji i bieżącego zarządzania cyberbezpieczeństwem na poziomie krajowym Ministerstwo Cyfryzacji, we współpracy z RCB, organizuje spotkania w formacie PCOC. Gremium stanowi dotychczas nieformalną platformę koordynacyjną Ministra Cyfryzacji, która jest wykorzystywana do szybkiej wymiany danych i informacji w zakresie zdarzeń w cyberprzestrzeni na poziomie krajowym. Rozwiązanie to pozwala na znaczące skrócenie czasu reakcji na incydenty oraz podniesienie poziomu cyberbezpieczeństwa państwa.

PCOC funkcjonuje jako cykliczne, zazwyczaj cotygodniowe gremium, zrzeszające przedstawicieli kluczowych dla bezpieczeństwa teleinformatycznego instytucji. W spotkaniach biorą udział m.in. przedstawiciele CSIRT-ów poziomu krajowego (CSIRT MON, CSIRT NASK, CSIRT GOV), sektorowych zespołów cyberbezpieczeństwa, służb specjalnych oraz poszczególnych ministerstw. Spotkania te mają charakter niejawny, a ich tematyka koncentruje się w głównej mierze wokół technicznych aspektów cyberzagrożeń. Do zapewnienia bezpiecznej wymiany danych, w tym informacji objętych klauzulą tajności, uczestnicy PCOC korzystają z urządzeń i sprzętu ICT pozwalających na podłączenie do niejawnej wojskowej sieci do klauzuli zastrzeżone.

W 2025 roku PCOC odgrywało kluczową rolę w bieżącej koordynacji działań międzyresortowych, wymianie informacji sytuacyjnych oraz uzgadnianiu działań pomiędzy kluczowymi interesariuszami. Funkcjonowanie PCOC bezpośrednio przyczyniło się do poprawy przepływu informacji w sytuacjach wymagających szybkiej synchronizacji działań. W minionym roku platforma ta pełniła wyjątkowo istotną funkcję w skracaniu czasu koordynacji działań w przypadku występowania incydentów wielopodmiotowych lub takich o potencjale systemowym. Umożliwiała ona szybkie zwoływanie posiedzeń, bieżącą synchronizację działań, wymianę ocen sytuacyjnych oraz uzgadnianie priorytetów reagowania, co miało bezpośrednie zastosowanie m.in. przy operacyjnym zabezpieczaniu procesu wyborczego w ramach programu "Parasol Wyborczy".

Z uwagi na wysoką skuteczność tego formatu, w dokumentach strategicznych państwa oraz projektach legislacyjnych zdefiniowano jasne perspektywy rozwoju PCOC, mające na celu dalszą instytucjonalizację i centralizację zarządzania cyberbezpieczeństwem.

Sformalizowanie struktury w UKSC. Działające od 2022 r. PCOC zostanie prawnie ustrukturyzowane w nowelizacji UKSC. Będzie ono funkcjonować jako oficjalny organ pomocniczy przy Pełnomocniku. W ustawie ściśle określono jego zadania oraz szeroki, międzyresortowy skład. Kolejnym krokiem rozwoju będzie rozszerzenie charakteru PCOC poprzez transformację w ośrodek decyzyjny, poprzez powołanie stałej struktury administracyjnej pełniącej funkcję zaplecza operacyjnego Pełnomocnika, która dzięki kompetencjom stanie się faktycznym punktem ciężkości polskiego cyberbezpieczeństwa oraz ustandaryzowanym 'jednym okienkiem' dla całego ekosystemu KSC. Jej celem będzie merytoryczna i organizacyjna obsługa prac Pełnomocnika oraz spotkań samego PCOC, a także zarządzanie na poziomie krajowym z ramienia Pełnomocnika działań podmiotów funkcjonujących na poziomie sektorowym. Zmierza to do ujednolicenia formatu i zakresu przekazywanych informacji na styku operacyjno-decyzyjnym.

REKOMENDACJE I KOMUNIKATY PEŁNOMOCNIKA RZĄDU DS. CYBERBEZPIECZEŃSTWA

W 2025 r. Pełnomocnik aktywnie wykorzystywał mechanizm rekomendacji opisany w art. 33 ust. 4a ustawy z dnia 5 lipca 2018 r. o KSC. Rekomendacje zostały udzielone po uprzednich konsultacjach z zespołami CSIRT poziomu krajowego.

REKOMENDACJE:

W minionym roku zostały wydane 3 rekomendacje Pełnomocnika.

Tabela 9. Zestawienie rekomendacji Pełnomocnika w 2025 r.

LP.	Tematyka	Adres pełnej treści	Data
1.	Rekomendacja Pełnomocnika Rządu ds. Cyberbezpieczeństwa dotycząca aktualizacji oprogramowania Roundcube	https://www.gov.pl/web/cyfryzacja/rekomendacja-pelnomocnika-rzadu-ds-cyberbezpieczenstwa-dotyczaca-aktualizacji-oprogramowania-roundcube	20.06.2025
2.	Rekomendacja Pełnomocnika Rządu ds. Cyberbezpieczeństwa: zaprzestanie korzystania z oprogramowania PAD CMS	https://www.gov.pl/web/cyfryzacja/rekomendacja-pelnomocnika-rzadu-ds-cyberbezpieczenstwa-zaprzestanie-korzystania-z-oprogramowania-pad-cms	1.09.2025
3.	Rekomendacja Pełnomocnika Rządu ds. Cyberbezpieczeństwa dotycząca aktualizacji produktów Cisco	https://www.gov.pl/web/cyfryzacja/rekomendacja-pelnomocnika-rzadu-ds-cyberbezpieczenstwa-dotyczaca-aktualizacji-produktow-cisco	16.10.2025

KOMUNIKATY:

Pełnomocnik w 2025 r. wydał 7 komunikatów w sprawach ważnych z perspektywy KSC.

Tabela 10. Zestawienie komunikatów Pełnomocnika w 2025 r.

LP.	Tematyka	Adres pełnej treści	Data
1.	Komunikat Pełnomocnika Rządu ds. Cyberbezpieczeństwa w sprawie zagrożeń związanych z wyborami prezydenckimi	https://www.gov.pl/web/cyfryzacja/ochrona-wyborow-prezydenckich-przed-cyberzagrozeniami	16.01.2025
2.	Komunikat Pełnomocnika Rządu ds. Cyberbezpieczeństwa w sprawie wycieku danych w wyniku cyberataku wobec firmy EUROCERT Sp. z o.o.	https://www.gov.pl/web/cyfryzacja/komunikat-pelnomocnika-rzadu-do-spraw-cyberbezpieczenstwa-ws-wycieku-danych-w-wyniku-cyberataku-wobec-firmy-eurocert-sp-z-oo	17.01.2025
3.	Komunikat Pełnomocnika Rządu do spraw Cyberbezpieczeństwa ws. ataków na przemysłowe systemy sterowania	https://www.gov.pl/web/cyfryzacja/komunikat-pelnomocnika-rzadu-do-spraw-cyberbezpieczenstwa-ws-atakow-na-przemyslowe-systemy-sterowania3	25.02.2025
4.	Komunikat Pełnomocnika Rządu ds. Cyberbezpieczeństwa w sprawie kampanii wymierzonej w użytkowników komunikatora Signal	https://www.gov.pl/web/cyfryzacja/ataki-phishingowe-na-uzytkownikow-signal-w-polsce	14.05.2025
5.	Komunikat Pełnomocnika Rządu do spraw Cyberbezpieczeństwa w sprawie cyberataku na firmę EKOTRADE Sp. z o.o.	https://www.gov.pl/web/cyfryzacja/komunikat-pelnomocnika-rzadu-do-spraw-cyberbezpieczenstwa-w-sprawie-cyberataku-na-firme-ekotrade-sp-z-oo	12.09.2025
6.	Komunikat Pełnomocnika Rządu ds. Cyberbezpieczeństwa w sprawie kampanii wymierzonej w użytkowników komunikatora Signal	https://www.gov.pl/web/cyfryzacja/ataki-phishingowe-na-uzytkownikow-signal--jak-chronic-swoje-konto	22.09.2025
7.	Komunikat Pełnomocnika Rządu do spraw Cyberbezpieczeństwa o kampanii phishingowej	https://www.gov.pl/web/cyfryzacja/pilny-komunikat-pelnomocnika-rzadu-do-spraw-cyberbezpieczenstwa-o-kampanii-phishingowej	30.10.2025

Analiza tematyki wydanych rekomendacji i komunikatów w 2025 r. wskazuje na koncentrację działań Pełnomocnika na trzech kluczowych obszarach: eliminacji podatności w oprogramowaniu serwerowym (Roundcube, Cisco), ochronie procesów demokratycznych (wybory) oraz reagowaniu na incydenty w podmiotach świadczących usługi zaufania i ochrony mienia.

ZESPÓŁ INCYDENTÓW KRYTYCZNYCH (ZIK)

ZIK stanowi istotne gremium o charakterze koordynacyjno-kryzysowym. Posiedzenia Zespołu są zwoływane przede wszystkim w sytuacjach wystąpienia incydentów skutkujących zakłóceniem poufności, integralności lub dostępności krytycznych zasobów teleinformatycznych lub kluczowych usług na terenie Rzeczypospolitej Polskiej. Uczestnictwo w pracach Zespołu pozwala kluczowym podmiotom państwowym dbać o bezpieczeństwo systemów niezbędnych dla ciągłości działania państwa.

Zgodnie z dotychczasowymi ustaleniami, Zespół jest obsługiwany przez RCB. W celu optymalizacji zarządzania i konsolidacji zadań w zakresie cyberbezpieczeństwa, nowelizacja UKSC przewiduje docelowe przeniesienie obsługi Zespołu bezpośrednio do urzędu obsługującego Pełnomocnika. W 2025 roku RCB dokonało również szczegółowego przeglądu istniejących struktur koordynacyjnych i operacyjnych, w tym relacji między PCOC a ZIK, w celu zapewnienia ich komplementarności i uniknięcia dublowania kompetencji w przyszłości.

W 2025 r. odbyły się 2 posiedzenia ZIK. Aktywny udział w pracach ZIK brali przedstawiciele kluczowych instytucji odpowiedzialnych za bezpieczeństwo narodowe, w tym służb specjalnych i organów ścigania.

Warto również zaznaczyć, że organy wchodzące w skład ZIK aktywnie podnosiły swoje kompetencje praktyczne – ich przedstawiciele wzięli udział m.in. w ogólnokrajowych ćwiczeniach KSC-EXE 2025 zorganizowanych przez Ministra Cyfryzacji, których jednym z celów była budowa świadomości w zakresie sprawnego postępowania w sytuacjach kryzysowych oraz weryfikacja procedur koordynacji na najwyższym szczeblu.

ANALIZA I SZACOWANIE RYZYKA DLA KSC NA POZIOMIE STRATEGICZNYM

CELE ANALIZY:

Cele analizy wynikają bezpośrednio z celów wdrożenia KSC zawartych w art. 3 ustawy z dnia 5 lipca 2018 r. o UKSC.

KSC ma na celu zapewnienie:

- cyberbezpieczeństwa na poziomie krajowym;
- niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług;
- zapewnienia obsługi incydentów.

ANALIZA SWOT KSC

Analiza SWOT dla KSC w 2025 r. została opracowana na podstawie danych, raportów z oceny ryzyka oraz wniosków przekazanych przez zespoły CSIRT poziomu krajowego, sektorowe zespoły cyberbezpieczeństwa oraz organy właściwe. Diagnozuje ona obecny stan systemu w dobie drastycznego wzrostu cyberzagrożeń oraz w przededniu wdrożenia nowelizacji ustawy o KSC (implementacji dyrektywy NIS2).

Tabela 11. Analiza SWOT dla KSC w 2025 r.

Mocne strony (Strengths)	Słabe strony (Weaknesses)
1. Sprawna koordynacja i szybka wymiana informacji operacyjnych w ramach PCOC. 2. Ścisła współpraca i rozwój narzędzi wewnątrz CSIRT-ów (S46, ARAKIS GOV, moje.cert.pl). 3. Rosnąca świadomość zagrożeń i realizacja szkoleń dla kadr (m.in. projekt SecureV). 4. Szerokie wsparcie finansowe z programów KPO i FERC dla instytucji publicznych.	1. Krytyczne braki kadrowe i ograniczenia finansowe w instytucjach państwowych, 2. Niska dojrzałość cyfrowa wielu podmiotów (szczególnie w sektorze zdrowia i samorządach). 3. Korzystanie z przestarzałej infrastruktury IT/OT i urządzeń bez wsparcia producenta. 4. Niespójne standardy zgłaszania incydentów oraz ich jakość dowodowa dla organów ścigania.
Szanse (Opportunities)	**Zagrożenia (Threats)**
1. Wdrożenie nowelizacji UKSC (dyrektywa NIS2) i standaryzacja procesów bezpieczeństwa. 2. Utworzenie nowych sektorowych zespołów CSIRT oraz powoływanie branżowych centrów ISAC. 3. Automatyzacja procesów detekcji i analizy zagrożeń przy użyciu Sztucznej Inteligencji (AI). 4. Silna pozycja na arenie międzynarodowej (Polska Prezydencja w UE, Mechanizm Talliński).	1. Skokowy, bezprecedensowy wzrost liczby incydentów i cyberataków. 2. Zaawansowane ataki grup APT i haktywistów powiązanych z Rosją i Białorusią. 3. Złośliwe wykorzystanie AI do automatyzacji ataków (phishing, deepfake). 4. Nasilenie ataków na łańcuchy dostaw i zewnętrznych dostawców IT. 5. Ryzyko przeciążenia organów państwa w wyniku masowego wejścia tysięcy nowych podmiotów do KSC.

OPIS POSZCZEGÓLNYCH ELEMENTÓW ANALIZY SWOT:

Mocne strony (Strengths):

- **Koordynacja i narzędzia systemowe** - KSC wykazuje wysoki poziom współpracy międzysektorowej, w czym ogromną rolę odgrywa PCOC, skracające czas reakcji na incydenty wielopodmiotowe. Systematycznie rozwijane są zaawansowane narzędzia wspierające mitygację zagrożeń, takie jak platforma wymiany informacji S46, system wczesnego ostrzegania ARAKIS GOV, publicznie dostępne skanery podatności (moje.cert.pl, Artemis).
- **Wsparcie finansowe inwestycji** - mocną stroną jest masowe uruchomienie dofinansowań z funduszy europejskich (KPO, FERC), które pozwoliły na realizację projektów podnoszących

odporność, takich jak "Cyberbezpieczny Samorząd" (granty dla niemal 90% samorządów), "Cyberbezpieczny Rząd" czy "Cyberbezpieczne Wodociągi".

Słabe strony (Weaknesses):

- **Kryzys kadrowy -** największą wewnętrzną słabością systemu jest drastyczny niedobór wykwalifikowanych specjalistów oraz ograniczenia finansowe budżetówki, co uniemożliwia organom państwowym skuteczne konkurowanie z sektorem prywatnym o ekspertów. Organy właściwe zmagają się z trwałym przeciążeniem kadrowym.
- **Niska dojrzałość podmiotów i dług technologiczny -** wiele podmiotów (w szczególności w sektorze ochrony zdrowia) charakteryzuje się brakiem specjalistów IT, nieaktualizowanym oprogramowaniem oraz przestarzałą infrastrukturą, w tym urządzeniami brzegowymi wystawionymi na ataki.

Szanse (Opportunities):

- **Impuls legislacyjny i strukturalny (NIS2) - p**rocedowana nowelizacja UKSC wdrażająca dyrektywę NIS2 stanowi szansę na uporządkowanie środowiska KSC i wymuszenie wyższych standardów w tysiącach firm i instytucji. Zmiany te napędzają również budowę nowych, dedykowanych Sektorowych Zespołów Reagowania (CSIRT Infrastruktura, CSIRT Cyfra, zespół dla sektora energii).
- **Rozwój technologiczny i współpraca -** zastosowanie Sztucznej Inteligencji i automatyzacji w systemach typu SOC/CTI daje szansę na skuteczniejszą obronę przed zagrożeniami i odciążenie analityków. KSC zyskuje także na silnej współpracy międzynarodowej – m.in. w ramach Mechanizmu Tallińskiego czy tworzenia unijnego planu reagowania *Cyber Blueprint* podczas polskiej prezydencji w UE.

Zagrożenia (Threats):

- **Ewolucja i masowość ataków - z**agrożeniem krytycznym jest skokowy wzrost incydentów (zespół CSIRT NASK zanotował wzrost obsługiwanych zdarzeń aż o 152% w stosunku do 2024 r.). Wynika to z wykorzystywania AI jako "mnożnika siły" przez adwersarzy do masowej personalizacji phishingu i złośliwych kampanii.
- **Działania państwowe i uderzenia w łańcuch dostaw -g**eopolityczne położenie Polski sprawia, że KSC jest stałym celem zaawansowanych grup APT oraz destrukcyjnego haktywizmu sterowanego przez służby rosyjskie i białoruskie (np. skoordynowane ataki na farmy wiatrowe czy ataki DDoS na sektor finansowy). Nasilają się ataki wektorowe poprzez słabiej chronionych zewnętrznych dostawców i podwykonawców usług IT.
- **Paraliż regulacyjny -i**stnieje poważne ryzyko systemowe, że nagłe wejście w życie nowelizacji KSC i skokowy przyrost tysięcy nowych podmiotów "kluczowych" i "ważnych" spowoduje przeciążenie organów nadzorczych oraz powstawanie czysto "fasadowych" struktur bezpieczeństwa, niezdolnych do realnego reagowania na incydenty.

ANALIZA PESTLE KSC

Analiza PESTLE określa kluczowe czynniki makrootoczenia, które mają wpływ na realizację celów i funkcjonowanie KSC, w tym zapewnienie cyberbezpieczeństwa na poziomie krajowym i niezakłócone świadczenie usług kluczowych.

Tabela 12. Zestawienie głównych czynników w Analizie typu PESTLE dla KSC

Polityczne (Political)	Ekonomiczne (Economic)	Społeczne (Social)	Technologiczne (Technological)	Prawne (Legal)	Środowiskowe (Environmental)
Napięcia geopolityczne **Zmiany legislacyjne**	Bariery finansowe i koszty wdrożenia Wpływ na gospodarkę	Świadomość społeczna. Zaufanie publiczne	Rozwój technologii Dług technologiczny i *Cybercrime-as-a-Service*:	Niezgodność z rygorystycznymi regulacjami Ochrona danych osobowych	Zależność od zasobów fizycznych i infrastruktury: Zmiany klimatyczne i klęski żywiołowe

SZCZEGÓŁOWY OPIS ZIDENTYFIKOWANYCH CZYNNIKÓW RYZYKA DLA KSC (REJESTR RYZYKA):

1. Czynniki Polityczne:

- **Napięcia geopolityczne:** Pozycja Polski jako państwa frontowego wschodniej flanki NATO i głównego węzła logistycznego wspierającego Ukrainę generuje stałą presję działań hybrydowych. Przekłada się to na nieustanne ataki grup APT (m.in. powiązanych z rosyjskim GRU i SVR oraz służbami Białorusi) i grup haktywistycznych wymierzone w infrastrukturę krytyczną, resort obrony i podmioty publiczne. Niesie to ryzyko czasowego ograniczenia działalności newralgicznych systemów państwa.
- **Zmiany legislacyjne:** Implementacja prawa unijnego (m.in. dyrektywy NIS2) i dostosowanie krajowych norm wpływa na konieczność głębokiej reorganizacji struktury KSC oraz powoduje ryzyko przeciążenia regulacyjnego dla instytucji. Zmiany w polityce wewnętrznej i priorytetach mogą ponadto wpływać na płynność finansowania kluczowych projektów IT.

2. Czynniki Ekonomiczne:

- **Bariery finansowe i koszty wdrożenia:** Wdrożenie nowelizacji UKSC wymaga skokowego rozszerzenia KSC o tysiące nowych podmiotów oraz powołania CSIRT-ów sektorowych. Wiąże się to z ogromnymi kosztami po stronie państwa. Brak odpowiedniego i stabilnego finansowania utrudnia zatrudnianie specjalistów w sektorze publicznym i wdrażanie zaawansowanych systemów, co zwiększa podatność na cyberataki.
- **Wpływ na gospodarkę:** Cyberataki o charakterze destrukcyjnym lub ransomware mogą prowadzić do długotrwałych przestojów w działalności usług kluczowych, generując kolosalne straty finansowe i obniżając zaufanie inwestorów do polskiej infrastruktury cyfrowej.

3. Czynniki Społeczne:

- **Świadomość społeczna i braki w edukacji:** Niski poziom świadomości zagrożeń cyfrowych ułatwia cyberprzestępcom prowadzenie masowych kampanii opartych na inżynierii społecznej (np. phishing), co skutkuje wyłudzaniem danych i kradzieżą środków. Brak odpowiedniej higieny cyfrowej wciąż jest wektorem początkowym w wielu incydentach przełamania zabezpieczeń w sieciach państwowych.
- **Zaufanie publiczne:** Niewłaściwe reagowanie na incydenty oraz częste wycieki danych mogą spowodować brak zaufania obywateli do cyfrowego państwa (np. do e-usług), co z kolei osłabi proces cyfrowej transformacji RP.

4. Czynniki Technologiczne:

- **Rozwój technologii (Sztuczna Inteligencja / Quantum):** Błyskawiczny rozwój generatywnej AI staje się potężnym "mnożnikiem siły" dla cyberprzestępców. Pozwala na automatyzację tworzenia wysoce wiarygodnych kampanii phishingowych (bez błędów językowych), ataków *deepfake* czy omijania reguł detekcji. Długoterminowym wyzwaniem dla komunikacji niejawnej będzie również nadejście komputerów kwantowych zdolnych łamać dotychczasowe algorytmy, co wymusi przejście na kryptografię post-kwantową.
- **Dług technologiczny i *Cybercrime-as-a-Service*:** Ewolucja usług hakerskich (np. *Ransomware-as-a-Service*) drastycznie obniża barierę wejścia dla przestępców. Złożoność przestarzałej infrastruktury w podmiotach KSC (często urządzeń brzegowych typu SOHO lub systemów bez wsparcia producenta) jest nieustannie i automatycznie skanowana i przełamywana.

5. Czynniki Prawne:

- **Niezgodność z rygorystycznymi regulacjami:** Skomplikowane wymogi prawne (np. rozporządzenie DORA w sektorze finansowym czy UKSC) rodzą ryzyko nakładania na firmy i instytucje wysokich kar finansowych za opóźnienia we wdrożeniu audytów lub brak zgodności.
- **Ochrona danych osobowych:** Zwiększona liczba wycieków danych w wyniku ataków narusza przepisy o ochronie danych osobowych (RODO), co pociąga za sobą interwencje organów nadzorczych (UODO), odpowiedzialność odszkodowawczą i uderza w reputację.

6. Czynniki Środowiskowe:

- **Zależność od zasobów fizycznych i infrastruktury:** Cyberbezpieczeństwo opiera się na fizycznej ciągłości centrów danych, których praca jest ściśle uzależniona od dostaw energii i chłodzenia (wody). Ich zakłócenie przekłada się na natychmiastowe problemy z dostępnością cyfrową.
- **Zmiany klimatyczne i klęski żywiołowe:** Ekstremalne zjawiska, takie jak katastrofalna powódź z września 2025 r. dowodzą, że środowisko naturalne i zmiany klimatyczne realnie zagrażają ciągłości procesów teleinformatycznych państwa.

REJESTR I OCENA RYZYKA

METEDOLOGIA

Kluczowym wyróżnikiem tegorocznego procesu diagnostycznego, stanowiącym istotny postęp względem lat ubiegłych, było wdrożenie i rygorystyczne zastosowanie jednolitych formularzy analizy ryzyka. Standaryzacja narzędzi sprawozdawczych pozwoliła na wyeliminowanie dotychczasowych rozbieżności metodologicznych i stworzenie spójnej, w pełni porównywalnej macierzy zagrożeń dla całej struktury państwa.

Prezentowany rejestr agreguje dane operacyjne od kluczowych podmiotów systemu, w tym:

- CSIRT-ów poziomu krajowego (GOV, NASK, MON),
- zespołów sektorowych (m.in. KNF, CeZ),
- organów właściwych oraz pozostałych instytucji.

Zidentyfikowane ryzyka zostały pogrupowane tematycznie i uporządkowane hierarchicznie – od scenariuszy o najwyższym współczynniku krytyczności. Tak skonstruowany rejestr nie tylko obrazuje aktualny stan bezpieczeństwa, ale przede wszystkim precyzyjnie wskazuje priorytety w zakresie mitygacji zagrożeń strategicznych dla Rzeczypospolitej Polskiej.

INSTRUKCJA:

- **Wpływ**: 1 – niski, 2 – średni, 3 – wysoki, 4 – krytyczny (np. wpływ na ciągłość działania OUK, bezpieczeństwo państwa);
- **Prawdopodobieństwo**: 1 – niskie, 2 – średnie, 3 – wysokie, 4 – krytyczne;
- **Skala poziomów ryzyka** (interpretacja iloczynu W × P).

Tabela 13. INSTRUKCJA

Iloczyn (W×P)	Poziom ryzyka	Interpretacja
1–4	**Niskie**	Minimalny wpływ na funkcjonowanie KSC, ryzyko akceptowalne
5–8	**Średnie**	Wymaga monitorowania, możliwe działania prewencyjne
9–12	**Wysokie**	Istotne zagrożenie dla ciągłości działania, konieczne wdrożenie środków zaradczych
13–16	**Bardzo wysokie**	Krytyczne ryzyko, wymaga natychmiastowych działań i planów awaryjnych

REJESTR I OCENA RYZYKA

Tabela 14. REJESTR I OCENA RYZYKA

Kategoria / Opis zidentyfikowanego ryzyka	W	P	Wynik (W×P)	Poziom ryzyka	Interpretacja / Wymagane działania	Przykładowe proponowane środki zaradcze
1.Niewystarczające finansowanie państwa i przeciążenie organów właściwych. Brak środków na działanie KSC i nadzór nad podmiotami w obecnej oraz znowelizowanej ustawie (NIS2)	4	4	**16**	**Bardzo wysokie**	Krytyczne ryzyko, wymaga natychmiastowych działań legislacyjnych.	Zwiększenie maksymalnego limitu wydatków przewidzianego w ustawie
2.Ataki Ransomware (w tym na podmioty lecznicze) Szyfrowanie i kradzież danych prowadzące do paraliżu usług medycznych (HIS, EDM) oraz krytycznych procesów	4	3	**12**	**Wysokie**	Istotne zagrożenie dla ciągłości działania życia i zdrowia.	Plany ciągłości działania (BCP/DRP), kopie zapasowe offline, segmentacja sieci, EDR/XDR
3.Ataki wolumetryczne DDoS Ataki na dostępność usług, powodujące efekty kaskadowe i obniżające zaufanie do stabilności państwa	4	3	**12**	**Wysokie**	Istotne zagrożenie dla ciągłości działania e-usług.	Wielowarstwowa ochrona anty-DDoS, redundancja, współpraca z operatorami telekomunikacyjnymi
4.Przestarzała infrastruktura, luki w oprogramowaniu i sprzęcie medycznym Podatności w urządzeniach, brak aktualizacji i korzystanie	4	3	**12**	**Wysokie**	Istotne zagrożenie systemowe, wektor dla masowych włamań.	Inwentaryzacja aktywów (urządzeń), systemowe zarządzanie podatnościami (skrócenie czasu patchowania)

z technologii bez wsparcia producentów						
5.Ewolucja zagrożeń i złośliwe wykorzystanie Sztucznej Inteligencji (AI) Zastosowanie AI do masowego szukania podatności, generowania phishingu, deepfake'ów oraz omijania zabezpieczeń	4	3	**12**	**Wysokie**	Konieczne wdrożenie zaawansowanych środków detekcji.	Wykorzystanie AI do defensywy i automatyzacji SOC, budowa platform klasy Threat Intelligence
6.Uderzenia w łańcuchy dostaw IT/OT i dostawców zewnętrznych Uzależnienie podmiotów od bezpieczeństwa zewnętrznych kontraktorów; kompromitacja usługodawcy dotyka klientów	3	3	**9**	**Wysokie**	Istotne zagrożenie wymagające renegocjacji wymogów.	Identyfikacja dostawców krytycznych, klauzule bezpieczeństwa w umowach, audyty łańcucha dostaw
7.Kryzys kadrowy i kompetencyjny ds. cyberbezpieczeństwa Niedobór ekspertów u operatorów (OUK), podmiotach leczniczych oraz brak możliwości konkurowania z rynkiem prywatnym	3	3	**9**	**Wysokie**	Istotne zagrożenie, osłabia potencjał obronny systemu.	Usługi edukacyjne, outsourcing SOC, dostosowanie wynagrodzeń, rozwój kadr akademickich
8.Niewystarczająca dojrzałość zarządzania ryzykiem i wyzwania nowelizacji (NIS2 Brak spełnienia wymogów KSC przez nowe podmioty, ryzyko powstawania fasadowych CSIRT-ów sektorowych	3	3	**9**	**Wysokie**	Konieczne wdrożenie planów wsparcia dla słabszych podmiotów.	Opracowanie centralnej metodyki oceny ryzyka KSC, cykliczne audyty bezpieczeństwa i wsparcie finansowe
9.Działania grup cyberofensywnych (APT) i ataki na kontraktorów Zaawansowane, ukierunkowane ataki na administrację rządową i operatorów IK z wykorzystaniem zaufanych relacji	3	2	**6**	**Średnie**	Wymaga stałego monitorowania i prewencji technicznej.	Weryfikacja personelu serwisowego, inwentaryzacja podpiętych urządzeń, zamykanie zbędnych usług
10.Dezinformacja w cyberprzestrzeni Kampanie informacyjne towarzyszące cyberatakom, potęgujące panikę, zakłócające obiektywny obraz sytuacji	3	2	**6**	**Średnie**	Wymaga monitorowania i szybkiej reakcji komunikacyjnej.	Monitorowanie przestrzeni informacyjnej, proaktywna komunikacja kryzysowa
11.Niespójna i opóźniona wymiana informacji (system S46)	3	2	**6**	**Średnie**	Wymaga działań optymalizujących	Standaryzacja procedur zgłoszeniowych, szkolenia

Brak spójnych zasad raportowania między podmiotami KSC, ograniczona elastyczność systemu S46					współpracę systemową.	z obsługi S46, integracja platform CTI
12.Ataki grup haktywistycznych i podstawowa socjotechnika Mniej wyrafinowane ataki wolumetryczne oraz masowy phishing ukierunkowany na wyłudzenie poświadczeń	2	2	**4**	**Niskie**	Ryzyko akceptowalne przy zachowaniu podstawowej higieny.	Kampanie edukacyjne, wdrożenie uwierzytelniania dwuskładnikowego (MFA/2FA), filtry pocztowe
13.Uzależnienie KSC od rozwiązań "Big Tech" i sprzętu spoza UE Silna pozycja globalnych dostawców ograniczająca suwerenność oraz ekspozycja sektora energii na ryzykowny sprzęt	4	1	**4**	**Niskie**	Wymaga monitorowania trendów i odpowiedniej polityki zakupowej.	Utrzymanie krytycznych danych on-premise, budowa krajowych kompetencji, zgodność z kryteriami UE

PODSUMOWANIE ANALITYCZNE

Zbudowana matryca wyraźnie obrazuje główne bolączki systemu państwowego:

1. **Ryzyko Krytyczne (16 pkt).** Jedyne ryzyko ocenione na najwyższą możliwą wartość dotyczy sfery budżetowej i zarządczej – braku pieniędzy i ludzi do obsługi KSC (zwłaszcza w kontekście implementacji dyrektywy NIS2).
2. **Ryzyka Technologiczne (12 pkt).** Najgroźniejszymi, bezpośrednimi wektorami ataków są paraliżujące infrastrukturę ataki Ransomware, wykorzystanie AI do automatyzacji ataków, uderzenia DDoS oraz eksploatowanie przestarzałego, nieaktualizowanego sprzętu IT i urządzeń medycznych.

REJESTR RYZYKA

1. Kryzys kadrowy, kompetencyjny i niedofinansowanie systemu

Problem ten ma charakter systemowy i długotrwały, dotykając zarówno organy właściwe, jak i Operatorów Usług Kluczowych (OUK). Ograniczenia budżetowe (szczególnie widoczne m.in. w sektorze ochrony zdrowia) powodują trudności w konkurowaniu z sektorem prywatnym o specjalistów. Niewystarczające środki finansowe przewidziane w obecnie obowiązującej, jak i nowelizowanej UKSC, prowadzą do przeciążenia kadrowego organów właściwych. Skutkuje to brakiem możliwości prowadzenia aktywnego nadzoru nad podmiotami (wymuszając działania doraźne zamiast planowych) oraz obniżeniem poziomu wykonywanych obowiązków. Ponadto, rosnący stopień skomplikowania technologii i wymogów regulacyjnych potęguje trudności w zapewnieniu zgodności z prawem.

2. Wyzwania organizacyjne związane z nowelizacją KSC (wdrożenie NIS 2)

Masowe włączenie nowych podmiotów do KSC wygeneruje nagły i skumulowany wzrost obowiązków regulacyjnych, co doprowadzi do przeciążenia organów właściwych, opóźnień w procesach rejestracyjnych i wydłużenia czasu reakcji na incydenty. Dodatkowo nałożono 18-miesięczny termin na osiągnięcie zdolności operacyjnej przez nowe CSIRT-y sektorowe. Przy drastycznie ograniczonym rynku ekspertów rodzi to realne ryzyko powstawania zespołów „fasadowych" (spełniających wymogi tylko na papierze) i powielania kosztów. Kolejnym problemem jest bardzo zróżnicowany (często niski) poziom

dojrzałości cyfrowej nowych podmiotów. Tworzy to w systemie KSC "słabe ogniwa", które mogą zostać wykorzystane przez atakujących jako punkt wejścia do bardziej chronionych sieci (łańcuchy dostaw), co ułatwi eskalację ataków w skali kraju. Zauważa się również, że powolne wdrażanie wymogów przez nowe podmioty ograniczy skuteczność działania zespołów takich jak CSIRT NASK.

3. Ewolucja zagrożeń: Sztuczna Inteligencja (AI) i nowe technologie
AI działa jako wektor i "mnożnik siły" dla cyberprzestępców. Modele generatywne pozwalają na masowe tworzenie niezwykle przekonujących wiadomości phishingowych, podszywanie się pod ludzi (np. *deepfake* ułatwiający oszustwa „CEO fraud") oraz automatyzację rekonesansu. AI ułatwia także napastnikom szybkie modyfikowanie skryptów i identyfikowanie najsłabszych punktów m. in. w infrastrukturze krytycznej. KSC mierzy się z presją na znacznie szybsze wykrywanie i korelację zdarzeń, ponieważ rośnie wolumen i wariantowość ataków. Pojawiają się również ataki na same systemy AI (np. *data poisoning*, *prompt injection*), które mogą skutkować wymuszeniem błędnych decyzji, a ich wykrycie jest trudne, gdyż nie przypominają klasycznych włamań. Rozwój zaawansowanych technologii (w tym komputerów kwantowych) stwarza trudności w nadążaniu za dostosowaniem zabezpieczeń i wymusza zatrudnianie kosztownych, wysoko wyspecjalizowanych kadr.

4. Dług technologiczny, podatności i uzależnienie od łańcucha dostaw
Wykorzystywanie przestarzałego lub niewspieranego przez producentów oprogramowania i urządzeń (np. sprzętu medycznego) generuje wektory ataku poprzez znane luki bezpieczeństwa, co prowadzi do kompromitacji infrastruktury. Ryzyko to potęguje rosnąca zależność organizacji od zewnętrznych dostawców (usług chmurowych, telekomunikacyjnych, Big Tech), co przenosi koncentrację ryzyka poza bezpośrednią kontrolę podmiotów KSC. Atakujący coraz częściej uderzają w kontraktorów świadczących usługi dla administracji i operatorów infrastruktury krytycznej, wykorzystując relację zaufania na linii usługobiorca-dostawca. Dodatkowym czynnikiem ryzyka jest rosnąca ekspozycja sektora energii na urządzenia pochodzące od dostawców spoza UE, przy ograniczonej możliwości weryfikacji ich bezpieczeństwa.

5. Cyberataki celowane (APT), Ransomware i DDoS
Grupy cyberofensywne prowadzą zaawansowane, ukierunkowane ataki, podczas gdy grupy haktywistyczne skupiają się m.in. na atakach wolumetrycznych DDoS oraz wykorzystywaniu niezabezpieczonych paneli dostępowych do systemów technologii operacyjnej (OT). Ataki typu DDoS mogą wywoływać efekty kaskadowe i obniżać zaufanie do stabilności e-usług państwowych. Z kolei niezwykle niebezpiecznym wektorem pozostaje ransomware (szczególnie w modelu *Ransomware-as-a-Service*), który łączy szyfrowanie systemów z kradzieżą danych i presją reputacyjną. Dla sektora ochrony zdrowia skuteczny atak ransomware oznacza utratę systemów HIS czy EDM i paraliż kluczowych procesów medycznych (rejestracji, diagnostyki, zabiegów), co bezpośrednio zagraża życiu pacjentów.

6. Komunikacja, wymiana informacji i zjawisko dezinformacji
Skuteczność KSC opiera się na szybkim przepływie informacji, jednak brakuje spójnych zasad i narzędzi komunikacji pomiędzy rosnącą liczbą podmiotów. Niewystarczająca wymiana informacji i brak elastyczności w dołączaniu do systemu S46 utrudniają i spowalniają dystrybucję wiedzy o podatnościach i incydentach. Uzupełniającym zagrożeniem jest dezinformacja towarzysząca cyberatakom – manipulacyjne treści potęgują niepokój społeczny i utrudniają skoordynowaną reakcję na incydenty w ramach systemu krajowego. Wciąż obserwowana jest również wysoka częstotliwość kampanii socjotechnicznych ukierunkowanych na bezpośrednie wyłudzenie poświadczeń od użytkowników.

PODSUMOWANIE

Kompleksowa ocena uwarunkowań KSC w 2025 r. wskazuje na bezprecedensowe spiętrzenie wyzwań o charakterze geopolitycznym, technologicznym i legislacyjnym. Polska, pełniąc rolę państwa frontowego wschodniej flanki NATO, stała się głównym poligonem działań hybrydowych, co w połączeniu z masową adaptacją sztucznej inteligencji przez grupy adwersarzy, trwale zmieniło krajobraz zagrożeń.

Kluczowe Wnioski:

- **Prymat ryzyka zasobowego.** Najwyższy poziom krytyczności w matrycy (16 pkt) przypisano **niewystarczającemu finansowaniu i kryzysowi kadrowemu**. To „wąskie gardło" systemu uniemożliwia organom państwowym skuteczną konkurencję o ekspertów z sektorem prywatnym, co przy skokowym wzroście obowiązków (NIS2) grozi niewydolnością nadzorczą.
- **Technologia jako obosieczny miecz.** Podczas gdy AI stanowi „mnożnik siły" dla cyberprzestępców (automatyzacja phishingu, deepfake), dla KSC jest ona jedyną szansą na **automatyzację obrony** i odciążenie nielicznych kadr eksperckich.
- **Dług technologiczny i łańcuch dostaw.** Analiza PESTLE i SWOT zgodnie wskazują, że najsłabszym ogniwem pozostają podmioty o niskiej dojrzałości (zdrowie, samorządy) oraz uzależnienie od zewnętrznych dostawców IT/OT. Ataki na łańcuch dostaw stają się dominującym wektorem uderzeń w infrastrukturę krytyczną.
- **Odporność fizyczna i klimatyczna.** Doświadczenia z katastrofalnej powodzi we wrześniu 2025 r. udowodniły, że cyberbezpieczeństwo jest nierozerwalnie związane z fizyczną stabilnością infrastruktury i dostępnością zasobów energetycznych, co wymusza ściślejszą współpracę z RCB.

WNIOSKI I REKOMENDACJE ZA ROK 2025

Rok 2025 charakteryzował się bezprecedensowym, skokowym wzrostem liczby cyberataków w Polsce (wzrost obsługiwanych incydentów o 144,4% rok do roku). Sytuacja ta była bezpośrednio zdeterminowana kluczową pozycją geopolityczną Polski (zaplecze logistyczne dla Ukrainy) oraz dynamiczną adaptacją nowych technologii przez cyberprzestępców. Raporty instytucji współtworzących KSC (CSIRT-y, służby specjalne, ministerstwa) pozwalają zdefiniować krajobraz zagrożeń wokół dwóch głównych osi: technologiczno-operacyjnej oraz systemowo-kadrowej.

I. Główne wektory ataków i trendy operacyjne

- **Sztuczna Inteligencja (AI) jako „mnożnik siły”**
  Adwersarze masowo wykorzystują generatywną AI do automatyzacji ataków. Pozwala to na tworzenie wysoce spersonalizowanych, bezbłędnych językowo kampanii phishingowych oraz wykorzystanie technologii *deepfake* do manipulacji i omijania systemów uwierzytelniania.

- **Ewolucja socjotechniki i migracja na prywatne komunikatory.**
  Oszustwa komputerowe pozostają najpowszechniejszym zagrożeniem (np. 97% incydentów w CSIRT NASK). Nowym, groźnym zjawiskiem jest przenoszenie przez atakujących komunikacji z ofiarami na szyfrowane komunikatory (Signal, WhatsApp), co pozwala na omijanie systemów bezpieczeństwa poczty e-mail w organizacji.

- **Złożone ataki państwowe (APT) i destrukcyjny haktywizm**
  Polska infrastruktura znajduje się pod stałą presją grup powiązanych ze służbami Rosji i Białorusi. Obserwowane są zmasowane, skoordynowane ataki wolumetryczne DDoS (np. na sektor finansowy w czasie wyborów) oraz zaawansowane uderzenia destrukcyjne, wykorzystujące oprogramowanie typu *wiper* niszczące dane (np. w sektorze energii).

- **Uderzenia w łańcuchy dostaw (Supply Chain)**
  Z uwagi na wysokie zabezpieczenia głównych celów, przestępcy kompromitują słabiej chronionych podwykonawców, zewnętrznych dostawców usług IT/OT oraz wykorzystują luki w nieaktualizowanych urządzeniach brzegowych (np. routerach SOHO) w celu uzyskania dostępu do sieci instytucji rządowych i operatorów infrastruktury krytycznej.

- **Profesjonalizacja cyberprzestępczości (CaaS i Ransomware)**
  Rozwój modelu usługowego (*Crime-as-a-Service, np. Ransomware-as-a-Service*) obniżył barierę wejścia dla atakujących. Ataki ransomware opierają się dziś na podwójnym lub potrójnym wymuszeniu (szyfrowanie, kradzież danych i szantażowanie klientów ofiary), co stanowi krytyczne ryzyko paraliżu np. dla szpitali.

II. Wewnętrzne wyzwania systemowe i organizacyjne KSC

- **Kryzys kadrowy i niedofinansowanie**
  Największą wewnętrzną słabością KSC, zgłaszaną solidarnie przez większość urzędów centralnych (m.in. MSWiA, MKiŚ, MRiT, KPRM), jest drastyczny niedobór wykwalifikowanych ekspertów cyberbezpieczeństwa. Ograniczenia budżetowe uniemożliwiają administracji państwowej skuteczną konkurencję z sektorem prywatnym, co prowadzi do trwałego przeciążenia operacyjnego istniejących kadr.

- **Wyzwania wdrożenia dyrektywy NIS 2 i niska dojrzałość podmiotów**
  Wejście w życie nowelizacji UKSC skokowo rozszerzy system o tysiące nowych podmiotów "kluczowych" i "ważnych". Wiele z tych instytucji (zwłaszcza w sektorze ochrony zdrowia czy w samorządach) cechuje się niską dojrzałością cyfrową, brakiem podstawowych zabezpieczeń i długiem technologicznym. Rodzi to obawy o powstanie struktur "fasadowych" oraz paraliż organów nadzorczych.

W 2025 roku polski system cyberbezpieczeństwa skutecznie reagował na bieżące kryzysy, jednak znalazł się w punkcie zwrotnym. Z jednej strony musi odpierać zautomatyzowane ataki wspierane przez AI i wrogie służby specjalne, z drugiej – zmaga się z potężnym "wąskim gardłem" w postaci braku ludzi i środków finansowych do obsługi rosnących obowiązków regulacyjnych. Wdrożenie mechanizmów automatyzacji ochrony oraz ustabilizowanie finansowania kadr będą warunkować przetrwanie systemu w kolejnych latach.

POZIOM REALIZACJI WNIOSKÓW ZE SPRAWOZDANIA Z 2024 R.

Sprawozdanie Pełnomocnika Rządu ds. Cyberbezpieczeństwa za rok 2024 zawiera wykaz wniosków i rekomendacji płynących z podsumowania ww. Sprawozdania. Tabela poniżej mieści wymienione wnioski wraz z określeniem poziomu ich realizacji w 2025 roku i komentarzem.

Należy pamiętać, iż proces zarządzania KSC jest zarazem dynamiczny i długotrwały. Specyfika implementacji zmian w KSC następuje w średnioterminowym okresie i wynika z charakteru systemu prawnego i legislacyjnego obowiązującego w Polsce.

Wnioski podsumowujące z 2024 roku zostały zaadaptowane w nowelizacji UKSC, i ich pełna realizacja będzie możliwa w czasie następującym po implementacji niezbędnych przepisów prawa.

Tabela 15. Poziom realizacji wniosków ze Sprawozdania Pełnomocnika Rządu ds. Cyberbezpieczeństwa za rok 2024

Nr z 2024	Wniosek ze Sprawozdania Pełnomocnika Rządu ds. Cyberbezpieczeństwa za rok 2024	Poziom realizacji	Komentarz
1.	Platforma wymiany informacji i harmonizacji KSC – CYBER.GOV.PL	W stałej realizacji	Rozbudowywano "Bazę wiedzy" na portalu gov.pl, w której w 2025 r. opublikowano ponad 130 nowych materiałów. Ponadto w aplikacji mObywatel uruchomiono dla obywateli usługę "Bezpiecznie w sieci" oraz przystosowywano system S46 do przyjęcia nowych podmiotów. W grudniu 2025 r. uruchomiono nowy portal CYBER.GOV.PL - nowoczesna platforma przygotowana przez Ministerstwo Cyfryzacji i NASK z myślą o ochronie cyfrowej obywateli, firm oraz instytucji publicznych. W jednym miejscu integruje kluczowe usługi do zgłaszania incydentów, udostępniania informacji o zagrożeniach i oferuje dostęp do narzędzi takich jak S46, moje.cert.pl czy bezpiecznedane.gov.pl.
2.	Wzrost liczby zagrożeń cyberbezpieczeństwa	W stałej realizacji	W 2025 r. odnotowano skokowy wzrost liczby incydentów o 144,4% rok do roku. System KSC nieustannie adaptował się do tej skali poprzez rozwój narzędzi wczesnego ostrzegania (m.in. systemu n6, skanera Artemis, ARAKIS GOV).
3.	Rewolucja AI - konieczne wsparcie podmiotów odpowiedzialnych i rozwój krajowych kompetencji...	W realizacji / Prace koncepcyjne	Wskazano wykorzystanie AI jako kluczowe zagrożenie ("mnożnik siły"). Równolegle, realizowano szkolenia z zakresu sztucznej inteligencji m.in. dla służb (Policja, PSP). W ramach projektu CCN kontynuowano budowę Laboratorium Bezpieczeństwa AI. Powołano IDEAS PIB pod auspicjami Ministra Cyfryzacji.
4.	Rewolucja kwantowa (kryptografia post kwantowa)	W realizacji	Ministerstwo Cyfryzacji współfinansowało i kontynuowało realizację projektu PIONIER-Q (Ogólnopolska Kwantowa Infrastruktura Komunikacyjna), który ma na celu wdrożenie technologii kwantowej dystrybucji kluczy (QKD) i stanowi oficjalny wkład Polski w inicjatywę EuroQCI. Rozpoczęto prace nad przygotowanie Planu migracji do kryptografii postkwantowej.
5.	Wzrost napięć geopolitycznych, w tym związanych z ograniczaniem dostępności technologicznej	W stałej realizacji	W związku z napięciami geopolitycznymi, wspierano budowę własnych, niezależnych zdolności m.in. poprzez konkursy grantowe dla polskich przedsiębiorstw MŚP z branży cyberbezpieczeństwa (w ramach inicjatywy NCC-PL). Rozwijano także mechanizmy współpracy międzynarodowej np. Mechanizm Talliński.

6.	Nowelizacja UKSC – zmiana strukturalna KSC	Procedowanie zmian legislacyjnych / W przygotowaniu	KSC znajdował się w fazie intensywnych przygotowań do wejścia w życie nowelizacji wdrażającej dyrektywę NIS 2. W 2025 r. projekt nowelizacji został przyjęty przez rząd, a w następnym roku zmiana prawa została uchwalona przez parlament i podpisana przez prezydenta. W systemie S46 przygotowywano nowe funkcjonalności rejestracyjne (samoidentyfikacja podmiotów) oraz budowano podwaliny pod nowe CSIRT-y sektorowe.
7.	Uregulowanie działań ofensywnych w cyberprzestrzeni	Prace koncepcyjne	Zadanie pozostaje niesformalizowane operacyjnie na poziomie prawnym. Ministerstwo Obrony Narodowej w swoich rekomendacjach na 2026 rok wciąż wskazuje na pilną konieczność określenia jasnych zasad, procedur i ram prawnych dotyczących działań ofensywnych w cyberprzestrzeni (w czasie pokoju, kryzysu i wojny). Działania w tym zakresie przewidziano w nowej Strategii Cyberbezpieczeństwa RP, nad którą w 2025 r. trwały prace w ramach rządowego procesu legislacyjnego (dokument został przyjęty przez rząd już w 2026 r.). Zadanie wykraczające poza zakres kompetencyjny Pełnomocnika.
8.	Kształtowanie i edukacja świadomości zagrożeń związanych z cyberbezpieczeństwem	W stałej realizacji	Przeprowadzono liczne kampanie i szkolenia dla społeczeństwa, w tym m.in.: Cyberlekcje (dla szkół), projekt "Higiena cyfrowa 2025", "Broń się w necie", eFajfy (dla seniorów) oraz kontynuowano program szkoleń SecureV dla najważniejszych osób w państwie.
9.	Zapewnienie zasobów kadrowych podmiotów KSC	W stałej realizacji	Kryzys kadrowy oceniono na najwyższą punktację ryzyka krytycznego dla całego systemu. Jako metodę mitygacji utrzymano Świadczenie Teleinformatyczne – w 2025 r. wypłacono je dla prawie 7 000 specjalistów (budżet ok. 377 mln zł).
10.	Utworzenie podmiotu koordynującego KSC, w związku z planowanym powstaniem CSIRTów sektorowych	Procedowanie zmian legislacyjnych	Rolę centralnego koordynatora pełnić będzie PCOC, które świetnie sprawdziło się podczas incydentów. Przyjęta nowelizacja zformalizuje działanie PCOC jako stałego organu pomocniczego Pełnomocnika ("jednego okienka" dla KSC) w 2026 r.
11.	Publikacja dobrych praktyk przez Pełnomocnika Rządu	W stałej realizacji	W 2025 roku Pełnomocnik Rządu wydał 3 oficjalne rekomendacje techniczne (m.in. dot. oprogramowania Roundcube i produktów Cisco) oraz 7 komunikatów. Dodatkowo w Bazie Wiedzy opublikowano 5 nowych zaleceń i standardów opracowanych wspólnie z partnerami programu PWCyber.
12.	Ćwiczenia KSC na poziomie krajowym	Zrealizowano	W dniu 26 listopada 2025 r. zorganizowano ogólnokrajowe ćwiczenia "KSC-EXE 2025", w których wzięło udział ponad 100 przedstawicieli kluczowych instytucji, organów właściwych i CSIRT-ów z całej Polski. Skupiły się one na testowaniu współpracy w warunkach kryzysowych.
13.	Wsparcie podmiotów lokalnych w zwiększaniu poziomu cyberbezpieczeństwa	W realizacji	Systematycznie wdrażano potężny program dotacyjny "Cyberbezpieczny Samorząd", w ramach którego do końca 2025 roku jednostki terytorialne w Polsce otrzymały realne wsparcie finansowe (około 1,3 mld zł na sprzęt, organizację i szkolenia) obejmujące swym zasięgiem zdecydowaną większość JST.

PLANOWANE DZIAŁANIA NA ROK 2026

W 2026 roku funkcjonowanie i ewolucja KSC zostaną oparte na dwóch fundamentalnych filarach: pełnym wdrożeniu znowelizowanej UKSC (implementującej dyrektywę NIS 2) oraz realizacji priorytetów nowej Strategii Cyberbezpieczeństwa RP[1]. Zmiany te zapoczątkują głęboką transformację strukturalną, operacyjną i regulacyjną systemu ochrony cyfrowej państwa. Główne kierunki działań zaplanowane na rok 2026 obejmują:

IMPLEMENTACJA DYREKTYWY NIS2 I OPERACJONALIZACJA UKSC

Kluczowym wyzwaniem będzie płynne przejście do nowego modelu klasyfikacji podmiotów. Dotychczasowy podział na operatorów usług kluczowych i dostawców usług cyfrowych zostanie zastąpiony szeroką kategorią **„podmiotów kluczowych”** oraz **„podmiotów ważnych”**. Rozszerzenie systemu pociągnie za sobą:

- **Nowe standardy odporności.**

  Wdrożenie rygorystycznych wymogów w zakresie zarządzania ryzykiem oraz procedur obsługi incydentów w nowo objętych sektorach gospodarki.

- **Bezpieczeństwo łańcucha dostaw.**

  Uruchomienie procedur oceny dostawców sprzętu i oprogramowania (ICT Supply Chain Risk Management), pozwalających na identyfikację i eliminację rozwiązań od tzw. dostawców wysokiego ryzyka (HRV) w systemach krytycznych.

- **Zarządzanie kryzysowe.**

  Wprowadzenie w życie „Krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę”, precyzującego kanały wymiany informacji w warunkach zagrożeń przekraczających standardowe zdolności reagowania państwa.

CENTRALIZACJA KOORDYNACJI I BUDOWA FORMALNEJ STRUKTURY PCOC

Zgodnie z założeniami Strategii, dotychczasowa formuła PCOC zostanie sformalizowana i rozbudowana. W 2026 r. PCOC przekształci się w ustrukturyzowaną komórkę wspierającą Pełnomocnika Rządu ds. Cyberbezpieczeństwa. Działanie to stanowi kluczowy etap w drodze do powołania centralnej i silnej instytucji koordynującej KSC, działającej jako „jedno okienko” dla wszystkich podmiotów KSC. W dalszym kroku PCOC zostanie przeistoczony w centralną instytucję tworząc jednolity oraz silny ośrodek decyzyjny i koordynacyjny odpowiedzialny za odporność cyfrową państwa. W zakres kompetencji ww. instytucji weszłyby skonsolidowane cywilne funkcję i potencjały CSIRT-ów poziomu krajowego (NASK i GOV), tworząc silną jednostkę o dużych możliwościach reagowania i przeciwdziałania zagrożeniem cyfrowym i zoptymalizowanych zasobach kadrowych i technicznych.

BUDOWA GOTOWOŚCI OPERACYJNEJ CSIRT-ÓW SEKTOROWYCH

Rok 2026 będzie okresem intensywnego rozwoju sieci sektorowych zespołów reagowania na incydenty. Priorytetem będzie utworzenie CSIRT-ów w strategicznych gałęziach gospodarki:

- **CSIRT Infrastruktura** dla sektorów transportu i gospodarki wodnej.
- **CSIRT Cyfra** dla infrastruktury cyfrowej.

[1] https://monitorpolski.gov.pl/MP/2026/309

- **CSIRT Energia** dla sektora paliwowo-energetycznego. Zespoły te zapewnią proaktywne wsparcie merytoryczne, będą prowadzić oceny bezpieczeństwa oraz koordynować obsługę incydentów na poziomie sektorowym w ścisłej współpracy z CSIRT-ami poziomu krajowego.

Ponadto nowelizacja UKSC rozszerza KSC na ponad 20 różnych sektorów i podsektorów gospodarki, nakładając na właściwych ministrów obowiązek ustanowienia CSIRT-u sektorowego w terminie 18 miesięcy od wejścia w życie przepisów. Stąd zakłada się powstanie kilkunastu zespołów tego typu.

MODERNIZACJA TECHNOLOGICZNA: S46 I PLATFORMA CYBER.GOV.PL

Rozwój zaplecza technologicznego KSC w nadchodzącym okresie zostanie ukierunkowany na strategiczną rozbudowę trzech kluczowych filarów, dostosowujących państwo do wymogów dyrektywy NIS2 oraz rosnących cyberzagrożeń:

- **System S46.** W związku ze skokowym wzrostem liczby podmiotów objętych znowelizowaną UKSC (wstępne szacunki wskazują na potrzebę podłączenia ponad 60 tys. nowych podmiotów), system zostanie wyposażony w moduł rejestru podmiotów umożliwiający ich samorejestrację w sposób bezpieczny przez internet. Funkcjonalność systemu zostanie rozszerzona o nową usługę pozwalającą podmiotom na automatyczne dokonywanie zgłoszeń naruszeń ochrony danych osobowych bezpośrednio do Prezesa UODO, co zostało już sformalizowane odpowiednim porozumieniem o współpracy.

- **Portal cyber.gov.pl.** W 2025 r. uruchomiona została publiczna platforma stanowiąca centralny punkt kontaktowy dla wszystkich uczestników KSC: obywateli, przedsiębiorców oraz instytucji publicznych. Będzie następował rozwój portalu poprzez zintegrowanie rozproszone dotąd narzędzia operacyjne, w tym: portal moje.cert.pl (zapewniający skanowanie podatności systemem Artemis i powiadomienia z systemu n6), bezpiecznedane.gov.pl, bezpiecznapoczta.cert.pl oraz platformy szkoleniowe z programu PWCyber. Platforma umożliwi zgłaszanie incydentów, wymianę informacji operacyjnych, dostęp do bazy wiedzy, ostrzeżeń, komunikatów Pełnomocnika oraz praktycznych wytycznych związanych z UKSC i dyrektywą NIS2. Bezpieczne korzystanie z serwisu zapewni integracja z węzłem krajowym identyfikacji elektronicznej.

- **Inwestycje w NASK (Centrum Cyberbezpieczeństwa NASK - CCN).** Zintensyfikowane zostaną prace nad budową fizycznego Centrum Cyberbezpieczeństwa NASK. Jest to strategiczna inwestycja o wartości 310 mln zł, której zakończenie zaplanowano na 2029 r. Znacznie rozszerzy ona zdolności KSC poprzez uruchomienie 7 dedykowanych, specjalistycznych jednostek badawczo-operacyjnych: Krajowego Centrum Odzyskiwania Danych, Krajowego Centrum Operacyjnego Cyberbezpieczeństwa, Modelowego Ośrodka Treningowo-Szkoleniowego w obszarze Cyberbezpieczeństwa, Laboratorium Bezpieczeństwa AI, Laboratorium Fuzzingu i Badania Złośliwego Oprogramowania, Krajowego Centrum Wsparcia Security dla jednostek samorządu terytorialnego oraz Ośrodka Modelowania Certyfikacji Cyberbezpieczeństwa. Dodatkowo w ramach tego przedsięwzięcia jest dążenie do powstania prywatnej, bezpiecznej chmury usługowej i obliczeniowej zlokalizowana przeznaczonej na potrzeby NASK.

KRAJOWY SYSTEM CERTYFIKACJI CYBERBEZPIECZEŃSTWA (KSCC)

W oparciu o ustawę o KSCC, wdrożony zostanie krajowy system certyfikacji produktów, usług i procesów ICT. Celem jest umożliwienie wydawania certyfikatów zgodnych z europejskimi programami (np. EUCC). Laboratoria badawcze (m.in. IŁ-PIB i NASK) uzyskają pełną zdolność do certyfikacji na najwyższych poziomach zaufania, co wzmocni suwerenność technologiczną państwa.

WZMOCNIENIE KAPITAŁU LUDZKIEGO I WSPARCIE REGIONÓW

W odpowiedzi na deficyt ekspertów, w 2026 r. zakłada się:

- **Utrzymanie kadr.**
  Kontynuację finansowania dodatków teleinformatycznych z Funduszu Cyberbezpieczeństwa dla kluczowego personelu odpowiedzialnego za cyberbezpieczeństwo w administracji publicznej.
- **Lokalne Centra Cyberbezpieczeństwa.**
  Utworzenie centrów usług wspólnych (CUW), które zapewnią wsparcie techniczne i merytoryczne dla jednostek samorządu terytorialnego.
- **Programy edukacyjne.**
  Dalszą realizację szkoleń SecureV dla kadry kierowniczej państwa oraz specjalistycznych kursów dla pracowników podmiotów KSC.

DZIAŁANIA KSC UWZGLĘDNIĄ WYZWANIA ZWIĄZANE Z NOWYMI TECHNOLOGIAMI

- **Wspólna Infrastruktura Informatyczna Państwa (WIIP).**
  Rozwój standardów „chmury niejawnej” w celu zwiększenia odporności systemów administracji.
- **Kryptografia postkwantowa (PQC).**
  Opracowanie krajowego planu migracji systemów krytycznych do standardów odpornych na ataki komputerów kwantowych.
- **Sztuczna Inteligencja.**
  Wykorzystanie AI w procesach Security Operations Center (SOC) do detekcji zagrożeń oraz wdrożenie regulacji chroniących przed atakami typu „adversarial AI”.

Sprawozdanie

Pełnomocnika Rządu

do Spraw Cyberbezpieczeństwa

za 2025 rok

TOM II – WKŁADY INFORMACYJNE PODMIOTÓW KSC

SPIS TREŚCI - TOM II – WKŁADY INFORMACYJNE PODMIOTÓW KSC

CSIRT-Y POZIOMU KRAJOWEGO

W ramach KSC na poziomie operacyjnym funkcjonują trzy zespoły CSIRT poziomu krajowego:

1) CSIRT GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;
2) CSIRT MON – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, prowadzony przez Ministra Obrony Narodowej;
3) CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy.

Zadania CSIRT-ów określa rozdział 6. UKSC. Każdy z nich cechuje się swoją specyfiką z uwagi na obszar odpowiedzialności (*constituency*). W pewnym uproszczeniu można stwierdzić, że CSIRT GOV odpowiada za administrację państwową i infrastrukturę krytyczną; CSIRT NASK za administrację samorządową, niektóre instytucje publiczne, operatorów usług kluczowych i dostawców usług cyfrowych (za wyjątkiem tych podległych pod MON), sektor przedsiębiorstw i „zwykłych obywateli"; a CSIRT MON za Siły Zbrojne RP, resort obrony narodowej (w tym jego jednostki i komórki organizacyjne), jak również niektóre inne podmioty realizujące zadania na rzecz Sił Zbrojnych RP, jak np. część przedsiębiorstw zbrojeniowych.

CSIRT GOV

PODSUMOWANIE ROCZNE:

Zespół CSIRT GOV w 2025 r. kontynuował rozpoznanie zagrożeń w cyberprzestrzeni RP w odniesieniu do organów i instytucji administracji państwowej oraz operatorów infrastruktury krytycznej (IK). **W ramach realizowanych zadań zarejestrował 23 136 zgłoszeń, z czego 5033 nosiło znamiona incydentu teleinformatycznego, w tym 13 incydentu powołanego, tj. takiego, który zgodnie z UKSC spowodował lub mógł spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej (według przeprowadzonej przez Zespól CSIRT GOV analizy zgłoszonych incydentów poważnych, żaden z nich nie nosił znamion ukierunkowanego ataku cybernetycznego). Pomimo wzrostu liczby samych incydentów (w tym tych zaklasyfikowanych jako incydenty w podmiotach publicznych, incydenty istotne oraz incydenty poważne), działania podejmowane przez Zespół CSIRT GOV przyczyniły się do mitygacji identyfikowanych cyberzagrożeń oraz rozpoznania nowych ryzyk**. Potwierdziła to m.in. współpraca z innymi Zespołami CSIRT poziomu krajowego mająca na celu wypracowywanie wspólnych praktyk oraz rekomendacji w zakresie cyberbezpieczeństwa, rozbudowa systemu wczesnego ostrzegania przez cyberzagrożeniami ARAKIS GOV czy też regularna ocena bezpieczeństwa teleinformatycznego podmiotów administracji rządowej oraz operatorów IK.

STATYSTYKI INCYDENTÓW:

Tabela 16.Statystki CSIRT GOV

Kategoria	Liczba (rok bieżący)	Liczba (rok poprzedni)	Zmiana r/r (%)
Łączna liczba zarejestrowanych z Roszeń	23136	17439	
Łączna liczba obsłużonych incydentów	5033	3991	+26,1%
- w tym: incydenty poważne (operatorzy usług kluczowych	13	6	+116,7%
- w tym: incydenty istotne (dostawcy usług w firmach	1		
- w tym: incydenty w podmiotach publicznych	39	3	
- incydenty krytyczne**	0	0	0%

* Duży wzrost w liczbie incydentów w podmiotach publicznych wynika m.in. ze zmian w procedurze zgłaszania incydentów do Zespołu CSIRT GOV, co mogło wpłynąć pozytywnie na wykrywalność zdarzeń tego typu.

** Do celów statystycznych incydenty krytyczne uwzględniają jedynie incydenty, w ramach których CSIRT GOV pełnił rolę CSIRTu wiodącego.

STATYSTYKI INCYDENTÓW W PODZIALE NA GŁÓWNE KATEGORIE TAKSONOMII REFERENCYJNEJ:

W tabeli zamieszczono incydenty zgodnie z nomenklaturą przyjętą w poprzednim opracowaniu ABW na potrzeby Sprawozdania celem wyliczenia poprawnego trendu.

Tabela 17. STATYSTYKI INCYDENTÓW W PODZIALE NA GŁÓWNE KATEGORIE TAKSONOMII REFERENCYJNEJ

Lp.	Kategoria incydentu (wg taksonomii referencyjnej)	Liczba (rok bieżący)	Liczba (rok poprzedni	Zmiana r/r (%)
1.	Podatność	1879	1105	
2.	Publikacja	860	902	
3.	Socjotechnika	1054	815	+29,3%
4.	Niedostępność	636	478	
5.	Atak	171	261	-34,5%
6.	Kaskada	119	235	
7.	Skanowanie	227	108	+110,2%
8.	Treści	72	56	+28,6%
9.	Wirus	15	31	

NAJWAŻNIEJSZE ZAGROŻENIA:

Trend 1: Kampanie socjotechniczne ukierunkowane na ominięcie zabezpieczeń organizacyjnych m.in. poprzez wykorzystanie komunikatorów internetowych:
Zespół CSIRT GOV zidentyfikował zwiększającą się liczbę ataków wykorzystujących komunikatory internetowe, co pozwala na obchodzenie wymagań i zabezpieczeń wprowadzanych przez administratorów systemów teleinformatycznych. W ramach prowadzonych kampanii socjotechnicznych adwersarze coraz częściej nakłaniają ofiarę do kontynuowania korespondencji przy pomocy komunikatorów takich jak Signal czy WhatsApp, ponieważ nie podlegają one tak ścisłej kontroli jak np. poczta elektroniczna obsługiwana przez instytucję, a jednocześnie przetwarzane są w nich dane wartościowe dla atakujących. Takie działania umożliwiają adwersarzom lepsze maskowanie prowadzonej przez siebie aktywności przy równoczesnym pozyskiwaniu kluczowych informacji, m.in. z uwagi na to, że wartościowe dane są także przetwarzane w ramach grup pracowniczych zakładanych we wspomnianych komunikatorach.

Trend 2: Ataki ukierunkowane na kontraktorów uczestniczących w łańcuchu dostaw:
W 2025 r. Zespół CSIRT GOV zidentyfikował intensyfikację ataków na kontraktorów świadczących usługi dla administracji państwowej oraz operatorów IK. W ujawnionych incydentach adwersarze skupiali się głównie na atakach ukierunkowanych na urządzenia brzegowe infrastruktury teleinformatycznej, m.in. stacje robocze serwisantów oraz innych pracowników podmiotów świadczących usługi dla zarządców IK. Osoby takie często stanowią punkt styku pomiędzy podmiotami w formie np. stacji operatorskich czy serwisowych). Wskazuje to na istotne znaczenie regularnych aktualizacji oprogramowania celem eliminacji potencjalnych wektorów ataku, jak też konieczność prowadzenia inwentaryzacji podłączonych do infrastruktury urządzeń zewnętrznych (wykorzystywanych m.in. w ramach prac serwisowych).

Trend 3: Wykorzystanie AI w kampaniach socjotechnicznych:
Wraz z rozwojem technologii opartych na sztucznej inteligencji Zespół CSIRT GOV zaobserwował pojawienie się zagrożeń związanych z wykorzystaniem AI w kampaniach socjotechnicznych, co może mieć różnorodny charakter. W tym zakresie zidentyfikowano m.in. wykorzystanie interfejsów AI do generowania komend wiersza poleceń mających wywołać szkodliwe dyspozycje na zainfekowanej stacji

roboczej, jednocześnie omijając automatyczne reguły detekcji. Ujawniono także użycie motywu narzędzi opartych na sztucznej inteligencji w ramach zachęty zawartej w wiadomości socjotechnicznej mającej na celu skłonienie odbiorcy do uruchomienia złośliwego oprogramowania. Zaobserwowane zostały również przypadki wykorzystania ogólnodostępnych narzędzi AI do generowania treści wiadomości socjotechnicznych mających brzmieć wiarygodnie dla odbiorcy lub ich tłumaczenia z języków obcych celem nadania kampanii międzynarodowego charakteru, w tym z wykorzystaniem tzw. technologii deepfake.

OPIS JEDNEGO, NAJWAŻNIEJSZEGO INCYDENTU (CASE STUDY):

Od 29 do 31 grudnia 2025 r. Agencja Bezpieczeństwa Wewnętrznego zidentyfikowała problemy z komunikacją po stronie niektórych operatorów infrastruktury krytycznej z sektora energetycznego. Dotyczyły one łączności z systemami odpowiedzialnymi za produkcję energii w ramach OZE oraz systemami zarządzającymi dwoma elektrociepłowniami na terytorium RP. W ramach przeprowadzonej analizy ustalono, że zaobserwowane ataki miały charakter skoordynowany, a ich celem była destabilizacja systemów kluczowych z punktu widzenia usług dostarczania energii elektrycznej. Zidentyfikowanym wektorem ataku były między innymi próby wykorzystania podatności urządzeń sieciowych celem pozyskania dostępu do infrastruktury podmiotu, a następnie prowadzenie działań o charakterze destrukcyjnym.

DZIAŁANIA STRATEGICZNE:

Projekt A: ARAKIS GOV
Zespół CSIRT GOV rozwijał system wczesnego ostrzegania o zagrożeniach w sieci Internet i automatycznej detekcji — ARAKIS GOV. W ramach tych działań podłączonych do niego zostało 9 nowych instytucji, co znacząco przełożyło się na bezpieczeństwo ich systemów teleinformatycznych. **System ARAKIS GOV w 2025 r. zanotował 2 298 217 251 zdarzeń, co przyczyniło się do wygenerowania 5 547 672 alarmów.**

Projekt B: Ocena bezpieczeństwa systemów teleinformatycznych:
W ramach prowadzonych testów penetracyjnych oraz oceny bezpieczeństwa infrastruktury podmiotów administracji rządowej oraz operatorów infrastruktury krytycznej przeprowadzono czynności w 18 instytucjach publicznych oraz obiektach IK. Działania te mają na celu stałe wzmacnianie bezpieczeństwa wykorzystywanej tam infrastruktury teleinformatycznej, zwłaszcza w obecnym okresie intensyfikacji ataków ukierunkowanych na zaburzenie funkcjonowania posiadanych systemów IT, a także proaktywne wyszukiwanie podatności infrastrukturalnych i technicznych, które mogłyby w przyszłości stać się wektorem ataku cybernetycznego.

Projekt C; Analiza zagrożeń związanych z publikacją w sieci Internet zasobów IT podmiotów administracji rządowej oraz operatorów IK:
W ramach bieżącej działalności CSIRT GOV związanej z proaktywnym zabezpieczaniem podmiotów będących we właściwości Zespołu realizowane są zadania w zakresie ujawnienia wycieków ich zasobów do sieci internetowej. W przypadku zidentyfikowania zagrożeń przesyłane są do poszczególnych podmiotów rekomendacje bezpieczeństwa mające na celu ograniczenie ryzyk.

DZIAŁANIA I WSPÓŁPRACA:

DZIAŁANIA EDUKACYJNE I BUDOWANIE ŚWIADOMOŚCI:

Tabela 18. DZIAŁANIA EDUKACYJNE I BUDOWANIE ŚWIADOMOŚCI

	Nazwa działania/kampanii	Grupa docelowa	Liczba odbiorców
1	Publikacja na stronie internetowej CSIRT GOV „Raportu o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku”	Administracja państwowa, operatom IK, obywatele RP zainteresowani tematyką bezpieczeństwa wewnętrznego i cyberbezpieczeństwa	Publikacja w domenie publicznej
2	Cykliczna publikacja „Tygodniowego biuletynu informacyjnego dot. istotnych zagrożeń dla zasobów teleinformatycznych”	Administracja państwowa, operatorzy IK	Podmioty we właściwości CSIRT Zespołu GOV
3	Dystrybucja ostrzeżeń o zidentyfikowanych zagrożeniach w cyberprzestrzeni	Administracja państwowa, operatorzy IK	Podmioty we właściwości Zespołu CSIRT GOV
4	Prowadzenie szkoleń dla osób sprawujących funkcje publiczne z zakresu zagrożeń w cyberprzestrzeni oraz sposobów ochrony przed nimi	Osoby sprawujące funkcje publiczne	Szkolenia realizowane były stosownie do identyfikowanych zagrożeń i potrzeb uczestników

WSPÓŁPRACA KRAJOWA:

Zespół CSIRT GOV prowadził regularną współpracę z zespołami CSIRT poziomu krajowego w ramach realizowania obowiązków KSC oraz obsługi incydentów mających wpływ na bezpieczeństwo RP w cyberprzestrzeni. Zgodnie z ustawową właściwością w ramach wymiany informacyjnej przekazywał zgłoszenia, a także obsługiwał incydenty dot. administracji rządowej oraz IK.

Zespół CSIRT GOV kooperował również z sektorowymi zespołami CSIRT. Prowadzono m.in. regularną wymianę informacji z Zespołem CSIRT CEZ (w zakresie zagrożeń dla sektora medycznego) oraz Zespołem CSIRT KNF (w kwestii ryzyk dla sektora bankowości). Współpraca ta umożliwiła obu stronom poszerzenie posiadanych informacji w zakresie krajobrazu zagrożeń w cyberprzestrzeni RP oraz budowę odpowiedniej świadomości sytuacyjnej.

ĆWICZENIA I WSPÓŁPRACA MIĘDZYNARODOWA:

Tabela 19. ĆWICZENIA I WSPÓŁPRACA MIĘDZYNARODOWA

	Nazwa inicjatywy	Data	Rola CSIRT	Zasięg	Opis scenariusza i cel współpracy
1	KSC-EXE 2025	11.2025	Uczestnik	Krajowy	Ocena gotowości kluczowych podmiotów KSC do skutecznej współpracy i wymiany informacji w warunkach symulowanego kryzysu teleinformatyczne.
2	Seminarium „Cyberbezpieczeństwo Infrastruktury Krytycznej”	05.2025, 11.2025	Uczestnik	Krajowy	Podnoszenie cyberodporności operatorów infrastruktury krytycznej, a także identyfikacja zagrożeń specyficznych dla te o rodzaju podmiotów.
3	CSIRT Summit	03.2025	Obserwator	Międzynar.	Zacieśnianie współpracy pomiędzy Zespołami Reagowania na Incydenty Bezpieczeństwa Komputerowego z całego świata.
4	NATO Locked Shields 2025	04.2025, 05.2025	Uczestnik	Międzynar.	Ćwiczenie obrony infrastruktury teleinformatycznej przed nieustannymi atakami, w warunkach presji politycznej, kampanii dezinformacyjnych i kryzysów infrastrukturalnych.

ANALIZA I OCENA FUNKCJONOWANIA KSC

Funkcjonowanie KSC z punktu widzenia Zespołu CSIRT GOV należy ocenić jednoznacznie — pozytywnie. Wdrożone za pośrednictwem UKSC procedury w zakresie zgłaszania obsługi incydentów teleinformatycznych usprawniły współpracę pomiędzy zespołami CSIRT poziomu krajowego, przyczyniając się do poprawy jakości pracy na rzecz wzmocnienia bezpieczeństwa cyberprzestrzeni RP.

PROGNOZY I PRZEWIDYWANIA DLA KSC NA ROK 2026:

Planowana nowelizacja UKSC przyczynić się powinna do rozwoju odporności RP w obliczu identyfikowanych zagrożeń w cyberprzestrzeni. W związku ze wdrożonymi działaniami m.in. grup cyberofensywnych oraz haktywistycznych istotne pozostanie stałe wzmacnianie bezpieczeństwa systemów teleinformatycznych organów i instytucji publicznych oraz podmiotów infrastruktury krytycznej. W tym kontekście kluczowym z punktu widzenia działań Zespołu CSIRT GOV będzie stałe monitorowanie ryzyk oraz identyfikowanie nowych wektorów ataku ze strony adwersarzy.

PLANY NA ROK 2026:

W kontekście ustawowych zadań nałożonych na Zespół CSIRT GOV za istotne należy uznać:

- kontynuację działań w zakresie identyfikacji i ostrzegania o zagrożeniach, rejestracji i obsługi incydentów teleinformatycznych, prowadzenia ocen bezpieczeństwa systemów i sieci teleinformatycznych oraz rozbudowy systemu ARAKIS GOV; bieżące zaangażowanie w proces rozpoznania i minimalizowania zagrożeń systemowych i technicznych związanych z cyberbezpieczeństwem.
- wzmocnienie potencjału kadrowego, organizacyjnego i technicznego w kontekście skutecznego i efektywnego rozpoznawania współczesnych zagrożeń, w tym dotyczących cyberszpiegostwa i cyberterroryzmu.

REKOMENDACJE NA 2026 REKOMENDACJE DLA PEŁNOMOCNIKA RZĄDU DS. CYBERBEZPIECZEŃSTWA:

W kwestii wzmocnienia cyberbezpieczeństwa RP zasadne wydaje się m.in.:

- kontynuowanie inicjatyw takich jak ćwiczenia Cyber-EXE oraz KSC-EXE, które pozwalają na testowanie procedur oraz rozwiązań prawnych w sytuacjach kryzysowych oraz wspomagają współpracę podmiotów związanych z bezpieczeństwem cyberprzestrzeni RP;
- prowadzenie celem rozwoju kompetencji kadr w zakresie cyberbezpieczeństwa szkoleń dla pracowników sektorów kluczowych z punktu widzenia bezpieczeństwa RP. Powinny one obejmować zarówno rozwój umiejętności technicznych w zakresie nowoczesnych rozwiązań z obszaru informatyki i cyberbezpieczeństwa, jak również zdolności analitycznych pozwalających na sprawniejszą identyfikację ryzyk.

CSIRT MON

CSIRT MON to funkcjonalna struktura organizacyjna tworzona przez komórki organizacyjne DK WOC oraz jednostki podporządkowane Dowódcy KWOC.

PODSUMOWANIE ROCZNE:

Zasadnicza aktywność w cyberprzestrzeni w 2025 r., podobnie jak w 2024 r., została przede wszystkim zdeterminowana kluczową pozycją geopolityczną Polski jako państwa frontowego NATO na wschodniej flance oraz głównego węzła logistycznego wspierającego Ukrainę w wojnie z Rosją. Od 2022 roku Polska jest krytycznym korytarzem dla transport uzbrojenia, pomocy humanitarnej i szkolenia ukraińskich żołnierzy, co uczyniło ją jednym z priorytetowych celów adwersarzy.

W 2025 roku, podobnie jak w latach ubiegłych, znaczący wpływ na stan bezpieczeństwa systemów IT resortu obrony narodowej (ron) miały zagrożenia związane z adwersarzami typu APT. Aktywność ta kojarzona jest głównie z działalnością sponsorowaną lub pozostającą w strukturach państwa. Są to zaawansowane, długotrwałe ataki, których celem jest zapewnienie atakującym skrytej oraz możliwie najdłuższej obecności w środowisku ofiary. Spektrum działań zagrożeń typu APT obejmuje różnorodne czynności – od systematycznie realizowanego rozpoznania infrastruktury teleinformatycznej, poprzez cyberszpiegostwo, zakłócanie działania, aż po działania destrukcyjne.

Od momentu rozpoczęcia pełnoskalowej inwazji Rosji na Ukrainę obserwowany jest wzrost aktywności prorosyjskich grup haktywistycznych. Większość działań tego typu aktywności ma charakter propagandowy i maskujący, mogący stanowić rodzaj zasłony dla rzeczywistych działań rosyjskich struktur państwowych. Ataki generują widoczny ruch medialny, wzmacniają narrację prorosyjską i są wykorzystywane jako źródło informacji dla oficjalnych mediów rosyjskich, które następnie amplifikują te treści - część z nich jest cytowana za granicą, zwiększając zasięg propagandy. Pomimo, że grupy haktywistyczne dysponują narzędziami umożliwiającymi ingerencję w systemy przemysłowe, ich główny wpływ operacyjny pozostaje w sferze medialnej i psychologicznej, mając na celu kreowanie wrażenia skuteczności i aktywności prorosyjskiej. W 2025 roku krajobraz zagrożeń cybernetycznych można podzielić na kilka głównych kategorii, które różnią się motywacją sprawców, poziomem zaawansowania technicznego oraz potencjalnym wpływem na bezpieczeństwo narodowe i funkcjonowania państwa są to:

- zagrożenia o charakterze APT (ang. *Advanced Persistent Threat*) – dobrze zorganizowanych, sponsorowanych przez państwa lub będących ich częścią. Działania tych grup charakteryzują się wysokim poziomem motywacji oraz umiejętności, praktycznie niewyczerpanymi zasobami i zaawansowaniem technologicznym;
- usługi Cyberecrime-as-a-Service – skomercjalizowane ekosystemy oferujące specjalistyczne usługi takie jak ransomware-as-a-service, initial access broker, phisihing-as-a-service, motywowane przede wszystkim zyskiem finansowym. Coraz częściej są także wykorzystywane przez podmioty państwowe jako proxy do działań prowadzonych przez zagrożenia klasy APT;
- grupy haktywistyczne – samozwańcze kolektywy, nie działające na zlecenie państwa, wspierające i angażujące się na rzecz działania w cyberprzestrzeni w określonej sprawie;

- zagrożenia z pogranicza cyberprzestrzeni i WRE[2], w zakresie odnoszącym się do spektrum elektromagnetycznego, dotyczą łączności bezprzewodowej (w tym komórkowej, radiowej, satelitarnej, GPS);
- zagrożenia od osób, działających świadomie lub przypadkowo (adwersarz, insider threat).

STATYSTYKI INCYDENTÓW:

Tabela 20. STATYSTYKI INCYDENTÓW MON

Kategoria[3]	Liczba (rok bieżący)	Liczba (rok poprzedni)	Zmiana r/r (%)[4]
Łączna liczba zarejestrowanych zgłoszeń	789	1057	-26%
Łączna liczba obsłużonych incydentów	7125	4220	+68,9%
- w tym: incydenty poważne (OUK)	-	-	-
- w tym: incydenty istotne (DUC)	-	-	-
- w tym: incydenty w podmiotach publicznych	54	35	+54,3%
- w tym: incydenty krytyczne	-	-	-

STATYSTYKI INCYDENTÓW W PODZIALE NA GŁÓWNE KATEGORIE TAKSONOMII REFERENCYJNEJ:

Tabela 21. STATYSTYKI INCYDENTÓW W PODZIALE NA GŁÓWNE KATEGORIE TAKSONOMII REFERENCYJNEJ

Lp.	Kategoria incydentu (wg taksonomii referencyjnej)	Liczba (rok bieżący)	Liczba (rok poprzedni)	Zmiana r/r (%)
1.	**Oszustwa komputerowe** *(Fraud)*	131	171	-24%
2.	**Złośliwe oprogramowanie** *(Malicious Code)*	354	555	-36,8%
3.	**Dostępność usług** *(Availability)*	17	20	-15%
4.	**Próby włamań** *(Intrusion Attempts)*	522	257	+101,6%
5.	**Bezpieczeństwo informacji** *(Information Content Security)*	5885	2962	+97,7%
*	*Inne*	216	255	-14,9%

NAJWAŻNIEJSZE ZAGROŻENIA:

Trend 1: phishing

Ataki typu phishing w dalszym ciągu są jednymi z najpopularniejszych wektorów ataku. Są one wykorzystywane zarówno przez zaawansowane klastry aktywności typu APT, jak i przez pomniejsze grupy cyberprzestępców. Adwersarze w celu uzyskania dostępu do systemów oraz kont użytkowników, wysyłają złośliwe oprogramowanie oraz linki do stron podszywających się pod panele logowania. W tym celu wykorzystują techniki socjotechniczne, które wymagają ciągłej obserwacji i adaptacji reguł bezpieczeństwa implementowanych na narzędziach.

Przykładem kampanii phishingowej prowadzonej na szeroką skalę była kampania skierowana na użytkowników aplikacji Signal. Atakujący wykorzystując komunikator podszywa się pod oficjalne konto Signal i rozsyła spreparowane wiadomości, w których:

- informuje o rzekomym naruszeniu bezpieczeństwa konta;
- próbuje wzbudzić niepokój i skłonić do natychmiastowego działania;
- nakłania do podania danych uwierzytelniających (np. kodu weryfikacyjnego);

[2] WRE – Walka Radioelektroniczna
[3] Opis incydentów zgodnie z UKSC
[4] Wzrost należy oznaczyć plusem (+), spadek minusem (-)

- dąży do przejęcia kontroli nad kontem Signal ofiary.

Celem atakującego jest wyłudzenie danych dostępowych i uzyskanie nieautoryzowanego dostępu do kont użytkowników.

Trend 2: łańcuch dostaw

Zaobserwowano intensyfikacje ataków na łańcuchy dostaw. Adwersarze coraz częściej dostrzegają, że bezpośrednie atakowanie dobrze chronionych celów jest kosztowne i niesie wysokie ryzyko. Natomiast kompromitacja ich dostawców, podwykonawców czy usługodawców oferuje znacząco niższe koszty wejścia z potencjalnie większym wpływem, jaki mogą uzyskać. Dostawcy usług zewnętrznych w tym dostawcy usług chmurowych stanowią szczególnie atrakcyjne cele dla adwersarzy, w kontekście prób kompromitacji łańcucha dostaw, gdzie pojedyncza kompromitacja usługi może umożliwić dostęp do wielu organizacji klienckich. Poprzez kompromitację takich dostawców istnieje możliwość instalacji oprogramowania złośliwego, kradzieży danych logowania, prowadzenia działań szpiegowskich wśród podmiotów korzystających ze skompromitowanej usługi. Warto więc zwrócić uwagę na małe i średnie przedsiębiorstwa oraz organizacje lokalne, które dotychczas były uznawane za cele niższego priorytetu, ale coraz częściej rozpoznawane są jako wartościowe wektory ataku zarówno dla zysku finansowego jak i dostępu strategicznego. Małe organizacje mogą posiadać znacząco mniej zasobów na ochronę cyberbezpieczeństwa, ograniczony dedykowany personel bezpieczeństwa informatycznego, przestarzałe oprogramowanie i sprzęt, nieadekwatne procedury tworzenia kopii zapasowych i niewystarczające szkolenia z zakresu świadomości bezpieczeństwa w porównaniu do dużych przedsiębiorstw czy instytucji rządowych. Sami dostawcy usług niekoniecznie muszą zdawać sobie sprawę ze skali negatywnego wpływu kompromitacji ich usług z punktu widzenia funkcjonowania ich klientów.

Trend 3: Cyberecrime-as-a-Service

Zaobserwowano również aktywności typu Cyberecrime-as-a-Service, która polega na oferowaniu specjalistycznych usług takich jak ransomware-as-a-service (RaaS), initial access broker, phisihing-as-a-service (PaaS). W większości przypadków motywowane są one zyskiem finansowym. Ewolucja ekosystemu cyberprzestępczości jako usługi w znacznym stopniu umożliwiła skalowanie ataków przeciwko małym organizacjom przez obniżenie barier technicznych. Czego przykładem może być aktywność brokerów dostępu początkowego, którzy pozyskują w sposób nieautoryzowany dostęp do systemów w małych organizacjach, a następnie oferują przedmiotowe dane innym grupom cybeprzestępczym, w tym o charakterze ransomware, w relatywnie niskich cenach na nielegalnych forach cyberprzestępczych. Zautomatyzowane narzędzia skanujące sprawdzają sieć Internet w poszukiwaniu podatnych systemów małych przedsiębiorstw, wykorzystujących przestarzałe oprogramowanie, słabe/domyślne hasła, błędnie skonfigurowane usługi chmurowe czy nienaprawione znane podatności. Przedmiotowe informacje o systemach są eksploitowane przez adwersarzy lub katalogowane w celu późniejszej sprzedaży, tworząc trwały krajobraz zagrożeń, w którym małe organizacje napotykają niemal ciągłą presję ataków.

OPIS JEDNEGO, NAJWAŻNIEJSZEGO INCYDENTU (CASE STUDY):

W jednej z instytucji nadzorowanych przez Ministra Obrony Narodowej miał miejsce incydent bezpieczeństwa polegający na kradzieży informacji poprzez eksfiltrację kluczowych danych podmiotu na zewnętrzny serwer zlokalizowany poza granicami RP oraz zaszyfrowaniu części danych na serwerze plików. Adwersarz pozostawił notkę ramsomware'ową nakłaniającą decydentów do opłacenia okupu w celu odzyskania zaszyfrowanych danych.

CSIRT MON po otrzymaniu zgłoszenia wydał rekomendacje doraźne dla podmiotu oraz skierował zespół analityków na miejsce, w celu udzielenia wsparcia w procesie obsługi incydentu. W ramach obsługi incydentu analitycy CSIRT MON dokonali oceny środowiska, w ramach której zidentyfikowano m.in.

liczne błędy konfiguracyjne oraz oprogramowanie w wersji posiadającej znane podatności. Analitycy CSIRT MON zabezpieczyli materiał cyfrowy, a następnie przeprowadzili złożoną analizę techniczną.

Dodatkowo przedmiotowa analiza potwierdziła włamanie do środowiska, kompromitację domeny Active Directory. Artefakty cyfrowe wskazywały na co najmniej kilkumiesięczną obecność adwersarza w środowisku ofiary.

Po ustaleniu skali incydentu, etapów złośliwej aktywności oraz TTP (Taktyk, Technik i Procedur) adwersarza, CSIRT MON wydał stosowne rekomendacje.

DZIAŁANIA STRATEGICZNE:

Projekt A: Realizacja prac nad zapewnieniem cyberbezpieczeństwa dla instytutów wojskowych nadzorowanych przez Ministra Obrony Narodowej

CSIRT MON wraz z DKWOC (JDC) od sierpnia 2025 roku w ramach proaktywnych i reaktywnych działań zmierzających do przeciwdziałania zagrożeniom w cyberprzestrzeni, udziela w tym zakresie specjalistycznego wsparcia instytutom wojskowym.

Realizacja najważniejszych zadań:

1. Uzgodniono i podpisano porozumienia w zakresie współpracy dotyczącej cyberbezpieczeństwa i wykrywania cyberzagrożeń w infrastrukturze teleinformatycznej.
2. Przeprowadzono weryfikację oraz ocenę stanu cyberbezpieczeństwa we wszystkich instytutach badawczych, na podstawie przygotowanego kwestionariusza oceny bezpieczeństwa.
3. Została przeprowadzona analiza i ocena ogólnego stanu cyberbezpieczeństwa każdego instytutu (tzw. Security Posture) oraz wydano stosowne rekomendacje cyberbezpieczeństwa instytutom mające na celu zwiększenie poziomu cyberbezpieczeństwa.
4. Zostały zaplanowane i wykonane testy bezpieczeństwa.
5. W 2025 roku uruchomiono działania Proaktywnego Wykrywania Cyberzagrożeń.
6. Wymiana informacji o cyberzagrożeniach (CTI).
7. Prowadzane są analizy bezpieczeństwa zewnętrznej powierzchni ataku (EASM).
8. DKWOC dostarczył usługę „Bezpieczny DNS", umożliwiając tym samym CSIRT MON podniesienie poziomu monitorowania zagrożeń cyberbezpieczeństwa.

Projekt B: Uruchomienie „Usługi Bezpieczny DNS"

W ramach realizacji prac nad zapewnieniem cyberbezpieczeństwa dla instytutów wojskowych nadzorowanych przez Ministra Obrony Narodowej CSIRT MON przy współpracy z DKWOC zwiększył poziom monitorowania cyberzagrożeń przy wykorzystaniu usługi „Bezpiecznego DNS".

Projekt C: Zwiększenie zdolności i możliwości Zespołów Zadaniowych do wsparcia obsługi incydentów komputerowych

Zakończenie etapu 2 budowy zdolności w zakresie działania Zespołów Zadaniowych (CRRT[5]) w bojowym ugrupowaniu wojsk. Przejście do fazy utrzymania zdolności przez cykliczne wykonywanie ćwiczeń z wykorzystaniem rozwiązań pozyskanych w ramach realizacji Wymagań Operacyjnych.

[5] CRRT – Cyber Rapid Response Team

DZIAŁANIA I WSPÓŁPRACA:

DZIAŁANIA EDUKACYJNE I BUDOWANIE ŚWIADOMOŚCI:

Tabela 22.DZIAŁANIA EDUKACYJNE I BUDOWANIE ŚWIADOMOŚCI

LP	Nazwa działania/kampanii	Grupa docelowa	Liczba odbiorców
1	**Dystrybucja informacji o podatnościach**	Jednostki nadzorowane i podporządkowane MON. Jednostki organizacyjne z podpisanym porozumieniem z DKWOC.	Około 300 adresatów
2	**Komunikaty do użytkowników**	Użytkownicy systemów organizowanych przez Dowódcę KWOC	Wszyscy użytkownicy systemów
3	**Wykład na temat bezpieczeństwa łańcucha dostaw**	Przedstawiciele spółek wchodzących PGZ	100
4	**Doraźne prezentacje z obszaru Cyber dla podmiotów KSC**	Instytucje rządowe	10-100

WSPÓŁPRACA KRAJOWA:

CSIRT MON współpracuje z krajowymi CSIRT-ami,(CBZC) organami właściwymi do spraw cyberbezpieczeństwa oraz operatorami usług kluczowych w celu zapewnienia bezpieczeństwa systemów teleinformatycznych o znaczeniu obronnym i państwowym. Współpraca ta opiera się na zasadach koordynacji, wymiany informacji oraz wzajemnego wsparcia eksperckiego.

W relacjach z CSIRT-ami poziomu krajowego CSIRT MON realizuje bieżącą wymianę informacji o zagrożeniach, podatnościach i incydentach, uczestniczy w skoordynowanym reagowaniu na incydenty o charakterze transsektorowym oraz wspólnych działaniach analitycznych. Współdziałanie z CBZC i Żandarmerią Wojskową koncentruje się na wsparciu technicznym i analitycznym postępowań dotyczących cyberprzestępczości, w szczególności w zakresie incydentów mogących nosić znamiona czynów zabronionych.

Na mocy podpisanych porozumień o współpracy w zakresie cyberbezpieczeństwa, CSIRT MON nawiązał współpracę z przedsiębiorcami z sektora zbrojeniowego, wojskowymi instytutami badawczymi oraz innymi podmiotami istotnymi dla KSC.

ĆWICZENIA I WSPÓŁPRACA MIĘDZYNARODOWA:

Tabela 23. ĆWICZENIA I WSPÓŁPRACA MIĘDZYNARODOWA

LP	Nazwa ćwiczenia / Inicjatywy współpracy	Data (MM.RRRR)	Rola CSIRT (Organizator / Uczestnik / Obserwator)	Zasięg (Krajowy / Międzynarodowy)	opis scenariusza / Cel współpracy
1	KSC−EXE	26.11.2025	Uczestnik	Krajowy	Celem KSC−EXE 2025 była ocena gotowości kluczowych podmiotów KSC do skutecznej współpracy i wymiany informacji w warunkach symulowanego kryzysu teleinformatycznego. Weryfikowano zasady współdziałania organów, CSIRT-ów poziomu krajowego oraz innych podmiotów krajowego systemu cyberbezpieczeństwa.
2	Uzupełnienie ćwiczeń jest spójne z ćwiczeniami DKWOC/CSIRT MON wskazanymi w tabeli pod linkiem.				

ANALIZA I OCENA FUNKCJONOWANIA KSC

KSC działa efektywnie. W ramach współpracy pomiędzy podmiotami KSC, CSIRT MON:

- uczestniczy w cyklicznych spotkaniach PCOC – połączone centrum operacji cyberbezpieczeństwa;
- bierze czynny udział w komunikacji z CSIRTami poziomu krajowego w ramach obsługi incydentów komputerowych jak i wymiany wiedzy o zagrożeniach.

PROGNOZY I PRZEWIDYWANIA DLA KSC NA ROK 2026:

Aktywność adwersarzy w polskiej cyberprzestrzeni pozostaje na wysokim poziomie intensywności, co w znaczącym stopniu determinowane jest trwającą wojną w Ukrainie oraz aktywną postawą Polski w zakresie wsparcia i donacji na rzecz Ukrainy. W ocenie DKWOC aktywności te będą wciąż rejestrowane, zwłaszcza przeciwko mniejszym organizacjom, których poziom zabezpieczeń jest dużo niższy. Ponadto celami mogą być podmioty w ramach łańcucha dostaw celem uzyskania danych i dostępu do istotnych danych z punktu widzenia bezpieczeństwa Polski.

Do głównych zmian w krajobrazie zagrożeń cybernetycznych dla Polski w 2025 roku można zaliczyć, przede wszystkim masowe wykorzystanie modeli sztucznej inteligencji do prowadzenia ataków, co zmieniło skalę i efektywność operacji ofensywnych, zarówno ze strony aktorów państwowych jak i cyberprzestępców. Wykorzystanie dużych modeli językowych do generowania spersonalizowanych treści phishingowych w języku polskim osiągnęło poziom, gdzie nawet świadomi zagrożeń użytkownicy mają trudność z rozróżnieniem prawdziwej komunikacji od złośliwej. Adwersarze wykorzystują modele językowe do automatycznego tworzenia wiadomości phishingowych uwzględniających kontekst organizacyjny ofiary, aktualne wydarzenia, specyficzną terminologię sektorową oraz naturalny styl komunikacji charakterystyczny dla danych organizacji.

Technologia „deep fake" będzie coraz powszechniejszym wektorem ataku w kampaniach inżynierii społecznej, gdzie syntetyczne nagrania audio i wideo będą wykorzystywane do podszywania się pod urzędników, menedżerów czy zaufanych współpracowników, w celu manipulowania osobami do wykonywania nieautoryzowanych działań, ujawniania danych logowania czy obchodzenia procedur weryfikacyjnych. Treści generowane przez sztuczną inteligencję są również wykorzystywane w operacjach wpływu i dezinformacji. Gdzie automatyczne generowanie fałszywych artykułów, postów w mediach społecznościowych oraz całkowicie sfabrykowanych person umożliwia na ogromną skalę rozprzestrzenianie fałszywych narracji. Prognozowanym jest zwiększenie poziomu wykorzystania AI w operacjach ofensywnych przez adwersarzy.

PLANY NA ROK 2026:

Realizacja zadań wynikających z „Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025-2029:

- Dostosowanie systemu cyberbezpieczeństwa Sił Zbrojnych (RON) do nowych regulacji „Dostosowanie systemu cyberbezpieczeństwa RON do wymagań nowelizacji UKSC (wdrażającej dyrektywę NIS 2)" – instytucja wiodąca: MON (Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni, DKWOC), termin: 2025–2026."
- Dostosowanie struktur MON odpowiedzialnych za cyberbezpieczeństwo - „Dostosowanie struktur resortu obrony narodowej odpowiedzialnych za cyberbezpieczeństwo do realizacji nowych zadań" – instytucja wiodąca: MON (DKWOC + jednostki podległe MON), termin: 2025–2026.
- Wzmocnienie współpracy międzynarodowej z udziałem MON - „Wzmocnienie wizerunku Rzeczypospolitej Polskiej jako kraju o wysokim poziomie profesjonalizmu i kompetencji kadr w obszarze cyberbezpieczeństwa" – instytucje współpracujące m.in.: MON (termin 2025–2029).

- Współpraca bilateralna/multilateralna w obszarze cyberbezpieczeństwa - „Ustanawianie dwustronnego i multilateralnego dialogu i współpracy na podstawie porozumień w wymiarze militarnym” – instytucja wiodąca: MON (DKWOC), termin: 2025–2029.

REKOMENDACJE NA 2026 - REKOMENDACJE DLA PEŁNOMOCNIKA RZĄDU DS. CYBERBEZPIECZEŃSTWA:

Wytworzenie dokumentów lub instrukcji budowania zdolności w zakresie cyberbezpieczeństwa w sektorowych CSIRT. Dokument powinien opisywać w sposób praktyczny budowę i organizację komórki zapewniających odpowiednie funkcje cyberbezpieczeństwa z uwzględnieniem wielkości organizacji oraz możliwości współdziałania z innymi CSIRTami sektorowymi w zakresie wymiana informacji o zagrożeniach, najlepszych praktykach i wiedzy. Dokument mógłby zawierać opis referencyjnego modelu operacyjnego CSIRTu sektorowego.

CSIRT NASK - NAUKOWA I AKADEMICKA SIEĆ KOMPUTEROWA – PAŃSTWOWY INSTYTUT BADAWCZY

NASK jest jednostką nadzorowaną przez ministra cyfryzacji.

PODSUMOWANIE ROCZNE:

W 2025 r. działający w strukturze CSIRT NASK Zespół CERT Polska odnotował znaczący wzrost liczby incydentów. Od 1 stycznia do 31 grudnia 2025 r. zarejestrowano ich **260,8 tys.**, podczas gdy w 2024 r. **103,4 tys.**, co oznacza wzrost o **152%**. Zdecydowanie najczęściej występującą kategorią zagrożeń były oszustwa komputerowe, które stanowiły **97%** wszystkich incydentów obsłużonych w 2025 r. Kolejnym najczęściej występującym zagrożeniem było szkodliwe oprogramowanie. W 2025 r. tego typu incydentów zarej. **3,4 tys.** W tym zestawieniu trzecią pozycję zajmowały podatne usługi (**1,7 tys.**).

Najbardziej rozpowszechnionym rodzajem oszustw komputerowych były próby wyłudzania poufnych danych, np. loginu i hasła do poczty, strony banku, portalu społecznościowego czy innej usługi online (ang. *phishing*). Łącznie takich przypadków było **78,4 tys.** Dane te wskazują na to, że osoby fizyczne pozostawały grupą najbardziej narażoną na cyberzagrożenia. Wśród metod ataku oszuści często wykorzystywali reklamy w mediach społecznościowych. W reklamach podszywali się m.in. pod znane osoby, by nakłonić potencjalne ofiary do fałszywych inwestycji. Linki prowadziły do stron obiecujących szybkie zyski, choć prawdziwym celem oszustów było wyłudzenie pieniędzy. W kampaniach podszywali się oni także pod platformy sprzedażowe i ogłoszeniowe, duże serwisy informacyjne oraz sklepy internetowe.

W 2025 r. zauważalny był również wzrost liczby incydentów w podmiotach publicznych – **5111** w stosunku do **3450** w 2024 r. Jednocześnie odnotowano wyraźny spadek incydentów poważnych zgłaszanych przez operatorów usług kluczowych (**57** w 2024 r. wobec **27** w 2025 r.), co bezpośrednio wiąże się z wejściem w życie rozporządzenia DORA (Digital Operational Resilience Act), które wyłączyło podmioty sektora finansowego spod obowiązków wynikających z UKSC.

Jedną z najpoważniejszych kategorii zagrożeń pozostawały ataki ransomware, które – choć nie były tak liczne jak pozostałe incydenty (w 2025 r. odnotowano **179** ataków ransomware) – mają potencjalnie ogromny wpływ na bezpieczeństwo danych i usług. Narażają one na straty finansowe i wizerunkowe nie tylko instytucję będącą bezpośrednią ofiarą, lecz także jej klientów, których dane mogły zostać ujawnione. W 2025 r. CERT Polska/CSIRT NASK nadal obserwował wysoką aktywność grup APT, głównie tych powiązanych z Federacją Rosyjską oraz Republiką Białorusi.

CERT Polska/CSIRT NASK niezmiennie rozwija swoje kluczowe projekty służące poprawie cyberbezpieczeństwa, takie jak moje.cert.pl., Lista Ostrzeżeń, narzędzia do zwalczania smishingu w ramach ustawy o zwalczaniu nadużyć w komunikacji elektronicznej, a także rozwiązania umożliwiające szybkie wykrywanie podatności w urządzeniach IT/OT.

W 2025 r. CERT Polska/CSIRT NASK pozostawał bardzo aktywny zarówno na arenie krajowej, jak i międzynarodowej – uczestniczył w licznych projektach, ćwiczeniach i zawodach, a także prowadził wymianę informacji oraz współpracę operacyjną z instytucjami odpowiedzialnymi za bezpieczeństwo w kraju i za granicą.

Oddzielną grupę zagrożeń stanowią incydenty związane z publikacją potencjalnie nielegalnych treści w internecie, w szczególności materiały przedstawiające seksualne wykorzystywanie dzieci lub inne

szkodliwe treści skierowane przeciwko bezpieczeństwu małoletnich. Tego typu zagrożenia obsługiwane są przez przeznaczony do tego celu zespół – Dyżurnet.pl. W 2025 r. Dyżurnet.pl przeanalizował **17,7 tys.** incydentów dotyczących potencjalnie nielegalnych treści. Natomiast liczba zarejestrowanych incydentów związanych z treściami przedstawiającymi seksualne wykorzystywanie dzieci (CSAM – Child Sexual Abuse Materials) wyniosła **2,9 tys**.

STATYSTYKI INCYDENTÓW:

Tabela 24. STATYSTYKI INCYDENTÓW CSIRT NASK

Kategoria	Liczba (2024 r.)	Liczba (2025 r.)	Zmiana r/r (%)
Łączna liczba zarejestrowanych zgłoszeń	600 990	658 320	+10%
Łączna liczba obsłużonych incydentów	103 449	260 783	+152
- w tym: incydenty poważne (OUK)	57	27	-53%
- w tym: incydenty istotne (DUC)	0	0	0%
- w tym: incydenty w podmiotach publicznych	3450	5111	+48%
- w tym: incydenty krytyczne	0	0	0%

STATYSTYKI INCYDENTÓW W PODZIALE NA GŁÓWNE KATEGORIE TAKSONOMII REFERENCYJNEJ:

Tabela 25. STATYSTYKI INCYDENTÓW W PODZIALE NA GŁÓWNE KATEGORIE TAKSONOMII REFERENCYJNEJ

Lp.	Kategoria incydentu (wg taksonomii referencyjnej)	Liczba (2025 r.)	Liczba (2024 r.)	Zmiana r/r (%)
1.	**Oszustwa komputerowe** *(Fraud)*	253 238	97 995	+158%
2.	**Złośliwe oprogramowanie** *(Malicious Code)*	3438	1891	+82%
3.	**Incydenty związane z dostępnością usług** *(Availability)*	427	426	+0,2%
4.	**Próby włamań** *(Intrusion Attempts)*	139	179	-22%
5.	**Incydenty związane z bezpieczeństwem informacji** *(Information Content Security)*	76	62	+23%
6.	**Zbieranie informacji** *(Information Gathering)*	15	26	-42%
7.	**Szkodliwe treści** *(Abusive Content)*	950	775	+23%
8.	**Podatności** *(Vulnerable)*	1 732	1 634	+6%
9.	**Włamania** *(Intrusions)*	750	447	+68%
10.	**Inne** *(Other)*	18	14	+29%

Kategorie incydentów wg standardu klasyfikacji incydentów eCSIRT.net mkVI.

NAJWAŻNIEJSZE ZAGROŻENIA:

Trend 1: W 2025 r. CERT Polska odnotował wzrost liczby ataków wiązanych z obcymi państwami (grup APT, haktywistycznych).
W 2025 r. CERT Polska/CSIRT NASK w dalszym ciągu obserwował wysoki poziom aktywności grup wiązanych z obcymi państwami (grup APT oraz haktywistycznych). Grupy te prowadziły swoje działania zarówno w celach wywiadowczych, jak i propagandowych. Aktywność atakujących polegała przede wszystkim na wyłudzaniu danych uwierzytelniających do skrzynek pocztowych, dystrybucji szkodliwego oprogramowania, a także na atakach na systemy przemysłowe, takie jak systemy wodociągowe oraz oczyszczalnie ścieków. W ubiegłym roku atakujący chętnie sięgali po narracje osadzone w bieżących wydarzeniach społeczno-politycznych – wykorzystywali m.in. motywy związane z polską prezydencją w Radzie Unii Europejskiej, kampanią wyborczą oraz innymi aktualnymi tematami, aby zwiększyć wiarygodność i skuteczność prowadzonych działań. W 2025 r. zaobserwowano też skoordynowane ataki, mające cel wyłącznie destrukcyjny, na wybrane podmioty z sektora energii. Większość z tych ataków można łączyć z działalnością grup związanych z Federacją Rosyjską oraz Republiką Białorusi.

Trend 2: Jednym z nadal istotnych zagrożeń dla organizacji pozostawały ataki ransomware obserwowane przez CERT Polska w 2025 r.
Ataki ransomware pozostają jednym z najpoważniejszych zagrożeń, które mają wpływ nie tylko na podmioty, które padły ofiarą ataków, lecz także na ich klientów, których dane zostały wykradzione i niejednokrotnie upublicznione. W 2025 r. CERT Polska zarejestrował **179** incydentów związanych z szyfrowaniem danych. Znaczna część ataków wynikała z wykorzystania podatności w urządzeniach brzegowych, usługach wystawionych do internetu oraz luk w popularnym oprogramowaniu.

W 2025 r. CERT Polska uczestniczył również w procesie skoordynowanego ujawniania podatności, w ramach którego opublikował m.in. krytyczną podatność RCE w DocsGPT (CVE-2025-0868) umożliwiającą zdalne wykonanie kodu przez nieuwierzytelnionego użytkownika oraz dwie poważne luki w Sparkle (CVE-2025-10015 i CVE-2025-10016) pozwalające na dostęp do zasobów chronionych i eskalację uprawnień.

Podatności w usługach, oprogramowaniu i urządzeniach brzegowych pozostawały w 2025 r. jednymi z głównych wektorów ataków, a nowe luki w urządzeniach brzegowych były wykorzystywane bardzo szybko przez atakujących.

Trend 3: Oszustwa komputerowe – nadal najczęstsza kategoria incydentów
W 2025 r. zdecydowanie najczęściej występującą kategorią zagrożeń były oszustwa komputerowe. Wśród ogółu obsłużonych incydentów (**260,8 tys.**) stanowiły one **97%**. Najbardziej rozpowszechnionym rodzajem oszustw komputerowych były próby wyłudzania poufnych danych, np. loginu i hasła do poczty, strony banku, portalu społecznościowego czy innej usługi online (ang. *phishing*). W 2025 r. łącznie odnotowano **78,4 tys.** tego typu incydentów. W dalszym ciągu obserwowano wzmożone kampanie phishingowe, w których oszuści podszywali się pod różne koncerny paliwowo-energetyczne, firmy oraz instytucje i proponowali użytkownikom nieistniejące programy dla akcjonariuszy indywidualnych. Wiele z tych oszustw zaczynało się od reklam wykorzystujących wizerunki znanych osób – polityków, sportowców, aktorów, które zamieszczano w mediach społecznościowych. Linki przekierowywały na strony, na których potencjalnym ofiarom obiecywano wysokie zyski, ale prawdziwym celem oszustów było wyłudzenie pieniędzy. Wśród popularnych kampanii phishingowych były m.in. przypadki nieuprawnionego wykorzystywania wizerunku serwisów OLX, Allegro, Gazeta.pl, Onet.pl. Ponadto na liście oszustw komputerowych znalazły się też m.in. fałszywe sklepy internetowe.

OPIS JEDNEGO, NAJWAŻNIEJSZEGO INCYDENTU (CASE STUDY):

Analiza case study przeprowadzona przez CERT Polska dotycząca incydentu w sektorze energii z 29 grudnia 2025 roku

29 grudnia 2025 roku doszło w Polsce do skoordynowanych ataków w cyberprzestrzeni wymierzonych w co najmniej 30 farm wiatrowych i fotowoltaicznych, spółkę prywatną z sektora produkcyjnego oraz dużą elektrociepłownię dostarczającą ciepło dla prawie pół miliona odbiorców w Polsce. Ataki miały cel wyłącznie destrukcyjny. Warto zwrócić uwagę, że ataki na farmy odnawialnych źródeł energii, mimo że spowodowały zerwanie komunikacji pomiędzy tymi obiektami a operatorami sieci dystrybucyjnej, nie wpłynęły na bieżącą produkcję energii elektrycznej. Podobnie atak na elektrociepłownię nie wywołał przerw w dostawie ciepła do odbiorców końcowych

W obszarze OZE atakami zostały dotknięte stacje elektroenergetyczne – główne punkty odbioru (GPO), w których obiekt OZE jest połączony z siecią dystrybucyjną i jej operatorem. Atakujący, po uzyskaniu dostępu do sieci wewnętrznej GPO, przeprowadził rekonesans, a następnie 29 grudnia dokonał działań prowadzących do uszkodzenia urządzeń przemysłowych różnych producentów. W efekcie uszkodzenia sterowników RTU stacje utraciły możliwość komunikacji z systemami operatora sieci dystrybucyjnej i uniemożliwiły zdalne sterowanie. Nie wpłynęło to jednak na bieżącą produkcję energii.

Atak na elektrociepłownię miał doprowadzić do nieodwracalnego uszkodzenia danych znajdujących się na urządzeniach w sieci wewnętrznej podmiotu za pomocą złośliwego oprogramowania typu wiper. Atak był poprzedzony długotrwałą infiltracją infrastruktury i kradzieżą wrażliwych informacji. W wyniku tych działań atakujący uzyskał dostęp do kont uprzywilejowanych, co umożliwiło mu swobodne poruszanie się w systemach elektrociepłowni. W momencie próby uruchomienia złośliwego oprogramowania jego działanie zostało zablokowane przez używane w podmiocie oprogramowanie klasy EDR.

29 grudnia atakujący próbował również zakłócić funkcjonowanie przedsiębiorstwa z sektora produkcyjnego. Swoje działania przeprowadził w sposób skoordynowany z atakami na przedsiębiorstwa sektora energetycznego z użyciem oprogramowania typu wiper.

Na podstawie analizy infrastruktury wykorzystanej do ataku, w tym przejętych serwerów VPS, routerów, można stwierdzić, że w znacznym stopniu pokrywa się ona z infrastrukturą używaną przez klaster aktywności znany w przestrzeni publicznej jako „Static Tundra", „Berserk Bear", „Ghost Blizzard" oraz „Dragonfly".

Więcej informacji na temat ataków, w tym szczegółowa analiza techniczna przeprowadzona przez zespół CERT Polska, znajduje się w publikacji „Raport z incydentu w sektorze energii 29.12" dostępnej na stronie https://cert.pl/posts/2026/01/raport-incydent-sektor-energii-2025. Pod tym linkiem można także zapoznać się z rekomendacjami wynikającymi z analizy incydentu.

DZIAŁANIA STRATEGICZNE:

Projekt A: Rozwój moje.cert.pl

W lutym 2025 r. zespół CERT Polska udostępnił publicznie serwis **moje.cert.pl**, w którym każdy obywatel posiadający stronę internetową może zlecić bezpłatne skanowanie bezpieczeństwa wszystkich swoich domen za pomocą systemu Artemis, może też uzyskać informacje na temat wycieków haseł użytkowników w swojej domenie. Serwis jest też dostępny dla administratorów serwerów i sieci, którzy mogą otrzymywać informacje o infekcjach szkodliwym oprogramowaniem i innych zagrożeniach w swoich sieciach. Na stronie moje.cert.pl w zakładce „Komunikaty" publikowane są aktualne ostrzeżenia dotyczące polskiej cyberprzestrzeni oraz alerty o podatnościach – komunikaty są dostępne dla wszystkich użytkowników internetu, także tych niezarejestrowanych w serwisie. Od sierpnia 2025 r. komunikaty można otrzymywać także w wiadomości e-mail (z tej funkcjonalności skorzystało do końca 2025 r. ponad **5 tys.** osób). W 2025 r. w serwisie zarejestrowało się ponad **15 tys.** użytkowników,

a w ramach usług przeskanowano ponad **3,3 mln** domen, subdomen i adresów IP, w których **znaleziono ponad pół miliona podatności lub błędnych konfiguracji**, z czego **21,3 tys.** wiążących się z wysokim ryzykiem.

Projekt B: Rozwój procesów i narzędzi umożliwiających szybkie wykrywanie podatności w urządzeniach IT/OT

CERT Polska stale monitoruje dostępne z internetu urządzenia przemysłowe oraz pulpity zdalne. Celem tych działań jest identyfikacja urządzeń stwarzających ryzyko dla instalacji przemysłowych i powiadomienie ich właścicieli o zagrożeniu. Jednym z narzędzi wykorzystywanych w tym procesie jest system **Snitch**. W 2025 r. CSIRT NASK wysłał **22 tys.** powiadomień mailowych dotyczących systemów OT. Wiadomości były wysyłane w większości do operatorów sieci. Dotyczyły one m.in. urządzeń dostępnych z internetu, które były niewłaściwie skonfigurowane lub posiadały podatność w oprogramowaniu. Ponadto wysłano **21,7 tys.** powiadomień mailowych dotyczących usług IT. Powiadomienia odnosiły się do podatnych urządzeń lub takich, wobec których podejrzewano występowanie podatności, a nie można było tego jednoznacznie potwierdzić. Powiadomienia związane z urządzeniami OT dotyczyły **10,1 tys.** unikalnych usług urządzeń OT działających na **8,4 tys.** hostów. Natomiast wiadomości odnoszące się do urządzeń IT dotyczyły **47,1 tys.** unikalnych usług urządzeń IT działających na **42,9 tys.** hostów.

DZIAŁANIA I WSPÓŁPRACA:

DZIAŁANIA EDUKACYJNE I BUDOWANIE ŚWIADOMOŚCI:

Tabela 26. DZIAŁANIA EDUKACYJNE I BUDOWANIE ŚWIADOMOŚCI

LP.	Nazwa działania/kampanii	Grupa docelowa	Liczba odbiorców
1	**Komunikowanie o zagrożeniach w mediach społecznościowych**. Ostrzeżenia dotyczą największych kampanii prowadzonych przez oszustów i są publikowane równolegle na profilach CERT Polska na Facebooku, X oraz LinkedInie.	Komunikaty są kierowane do ogółu internautów.	Od początku stycznia do końca grudnia 2025 r. posty CERT Polska na portalu Facebook uzyskały blisko **6 mln** wyświetleń, na LinkedInie **569,2 tys.** wyświetleń oraz **749,1 tys.** wyświetleń na platformie X.
2	**Powiadomienia push w aplikacji mObywatel** informują użytkowników o bieżących cyberzagrożeniach i stanowią część usługi **Bezpiecznie w sieci**.	Powiadomienia są kierowane do wszystkich użytkowników mObywatela, aby ostrzegać ich przed aktualnymi cyberzagrożeniami i wspierać bezpieczne korzystanie z sieci.	Na koniec 2025 r. liczba odbiorców powiadomień push przekroczyła **380 tys.**
3	**„Podsumowanie Miesiąca CERT Polska / CSIRT NASK”** to nowa formuła komunikacji, wprowadzona w październiku 2025 r., w ramach której CERT Polska publikuje comiesięczne raporty podsumowujące najważniejsze incydenty i zagrożenia cyberbezpieczeństwa, a także informuje o bieżących działaniach zespołu CERT Polska.	Raporty są tworzone dla użytkowników internetu.	Liczba subskrybentów raportów na stronie https://moje.cert.pl/komunikaty/subskrybuj/ na koniec grudnia 2025 r. to **3,4 tys.*** *Rzeczywista liczba odbiorców przewyższa liczbę subskrybentów, ponieważ subskrypcje obejmują tylko część użytkowników – raporty są dalej udostępniane i trafiają również do osób niezapisanych.

WSPÓŁPRACA KRAJOWA:

CERT Polska brał udział w cyklicznych spotkaniach przedstawicieli CSIRT-ów poziomu krajowego (CSIRT NASK, CSIRT GOV, CSIRT MON), zespołów sektorowych (CSIRT CeZ, CSIRT KNF), a także nowo tworzonych zespołów CSIRT Cyfra i CSIRT Infrastruktura oraz CSIRT PSE, jak również z UKE. W ramach spotkań wymieniano informacje na temat działań operacyjnych, analizy konkretnych przypadków

incydentów oraz identyfikacji potencjalnych ryzyk, a także identyfikowano potrzeby oraz możliwości wsparcia działań operacyjnych. Dodatkowo CERT Polska organizował spotkania warsztatowe z udziałem m.in. przedstawicieli Najwyższej Izby Kontroli, CSIRT CeZ, Ministerstwa Sprawiedliwości, Głównego Inspektoratu Sanitarnego. Ponadto, w ramach działań uświadamiających, CERT Polska współpracował z wieloma podmiotami, w tym z jednostkami samorządu terytorialnego i ich związkami, izbami gospodarczymi oraz stowarzyszeniami branżowymi. Współpraca ta polegała m.in. na udziale w konferencjach, szkoleniach i spotkaniach, podczas których poruszane były kwestie cyberbezpieczeństwa. W ramach współpracy krajowej CERT Polska uczestniczył też w ćwiczeniach KSC-EXE 2025. Ich celem było sprawdzenie działania procedur oraz gotowości kluczowych podmiotów KSC do skutecznej współpracy w warunkach symulowanego kryzysu teleinformatycznego.

ĆWICZENIA I WSPÓŁPRACA MIĘDZYNARODOWA:

Udział w międzynarodowych ćwiczeniach z zakresu cyberbezpieczeństwa w 2025 r. umożliwił realizację zakładanych celów strategicznych w obszarze współpracy międzynarodowej. Ćwiczenia prowadzone w ramach inicjatyw UE, NATO oraz działań koordynowanych przez ENISA pozwoliły na pogłębienie współpracy operacyjnej, przetestowanie obowiązujących procedur oraz wymianę doświadczeń z partnerami zagranicznymi. W trakcie ćwiczeń skutecznie wzmocniono relacje z dotychczasowymi partnerami, a także nawiązano nowe kontakty robocze, które mogą stanowić podstawę dalszej współpracy operacyjnej. Wspólne działania, realizowane w warunkach symulowanych incydentów transgranicznych i zagrożeń dla IK, przyczyniły się do podniesienia poziomu gotowości reagowania oraz interoperacyjności zespołów. Osiągnięte rezultaty ćwiczeń potwierdzają zasadność dalszego zaangażowania w inicjatywy międzynarodowe i mają bezpośredni wpływ na wzmacnianie zdolności krajowych w obszarze cyberbezpieczeństwa, co w konsekwencji przyczynia się do podniesienia poziomu bezpieczeństwa RP.

Tabela 27. ĆWICZENIA I WSPÓŁPRACA MIĘDZYNARODOWA

	Nazwa ćwiczenia	Data	Rola CSIRT	Zasięg	Opis scenariusza / Cel współpracy
1	Udział w sieci CSIRTs Network (UE) oraz w inicjatywach ENISA, takich jak ćwiczenia Cyber Europe (organizowane przez ENISA co dwa lata. Ostatnia edycja odbyła się w VI 2024 r.)	2025	Uczestnik / członek	Międzynar.	Współpraca w ramach CSIRTs Network (UE) ma na celu zwiększenie odporności cyberbezpieczeństwa całej Unii Europejskiej poprzez szybką wymianę informacji o zagrożeniach, wspólne reagowanie na incydenty transgraniczne, tworzenie jednolitych standardów i procedur, a także wzajemne wsparcie techniczne i eksperckie między krajowymi zespołami CSIRT.
2	Udział w ćwiczeniach Locked Shields	05.2025	Uczestnik	Międzynar.	W 2025 r. scenariusz Locked Shields koncentrował się na złożonym kryzysie dotyczącym infrastruktury krytycznej państwa, obejmującym jednoczesne ataki na wiele sektorów.
3	Udział w ECSC (European Cybersecurity Challenge)	10.2025	Organizator	Międzynar.	ECSC to europejskie zawody typu CTF (Capture The Flag), obejmujące zadania z różnych dziedzin cyberbezpieczeństwa. Cel konkursu to rozwijanie umiejętności młodych specjalistów, promowanie cyberbezpieczeństwa w Europie, budowanie współpracy między krajami, wyłanianie najlepszych talentów do pracy w sektorze cyber.
4	Udział w ćwiczeniach Cyber SOPEx	10.2025	Uczestnik	Międzynar.	Ćwiczenia polegały na symulacji skoordynowanego cyberataku na wiele państw UE. Miały na celu przećwiczenie procesu i procedur zgodnych z nową wersją Cyber Blueprint. Scenariusz ćwiczeń został dostosowany do aktualnych zagrożeń dla branży transportowej z wykorzystaniem podatności w urządzeniach automatyki przemysłowej.

5	Cyber Fire Foundry	03–04.2025 10.2025	Uczestnik	Międzynar.	Szkolenia z cyberbezpieczeństwa, zorganizowane na przełomie III i IV oraz w X 2025 r. przez Departament Energii USA, były bezpośrednio powiązane z codziennymi zadaniami realizowanymi przez CERT Polska/CSIRT NASK. Program koncentrował się na praktycznych ćwiczeniach obejmujących m.in. analizę incydentów oraz badanie złośliwego oprogramowania.
6	Hackaton DevOps #15 INTERPOL INHOPE NASK-PIB	10.2025	Współorganizator	Międzynar	Celem wydarzenia była budowa narzędzi informatycznych służących do detekcji oraz zwalczania przestępstw związanych z tworzeniem i rozpowszechnianiem CSAM.

ANALIZA I OCENA FUNKCJONOWANIA KSC:

W 2025 r. CSIRT NASK – w ramach monitorowania zmian w obszarze *constituency* CSIRT NASK związanych z nowelizacją UKSC , a także z rozwojem krajowego i europejskiego prawa w obszarze cyberbezpieczeństwa – opracował analizy, dostępne na portalu https://cyberpolicy.nask.pl:

1. „Wdrożenie Aktu o sztucznej inteligencji w państwach UE, cz. 1”,
2. „Wdrożenie Aktu o sztucznej inteligencji w państwach UE, cz. 2”,
3. „Zalecenia Rady w sprawie Planu działania UE na rzecz zarządzania cyberkryzysami (Cyber Blueprint)”,
4. „UKSC”,
5. „Akt o cyberodporności – cele i zakres regulacji”,
6. „Nowa rola ENISA w programie CVE”,
7. „Sprawozdanie na temat stanu Cyfrowej Dekady w 2025 r.”,
8. „Europejska Tarcza Demokracji – komunikat Komisji Europejskiej”.

PROGNOZY I PRZEWIDYWANIA DLA KSC NA ROK 2026:

1. Wzrost liczby ataków powiązanych z obcymi państwami (grupy APT).
2. Coraz szersze wykorzystanie w atakach na firmy podatności w oprogramowaniu i urządzeniach brzegowych.
3. Wykorzystanie AI w atakach socjotechnicznych może zwiększyć ich skuteczność (dzięki np. generowaniu realistycznych obrazów, głosu czy nagrań wideo).
4. Wzrost roli sztucznej inteligencji w szybszym wykrywaniu i wykorzystywaniu podatności przez cyberprzestępców, ale z drugiej strony wykorzystanie narzędzi AI do wykrywania cyberzagrożeń i cyberprzestępstw przez zespoły CSIRT.
5. Zagrożenia dla usług chmurowych związane z błędami konfiguracyjnymi.
6. Wzrost liczby oraz dostępności treści szkodliwych dla dzieci.

PLANY NA ROK 2026:

1. Wspieranie rozwoju CSIRT-ów sektorowych.
2. Wspieranie projektów: Cyberbezpieczne Wodociągi, CROPT, ISAC-JST, Lokalne Centra Cyberbezpieczeństwa.
3. Dalszy rozwój projektów DNS4EU, FETTA, AIPITCH.
4. Dalszy rozwój narzędzi CERT Polska: Snitch, Artemis, moje.cert.pl, MWDB, n6, bezpiecznapoczta.cert.pl.
5. Promocja Listy Ostrzeżeń wśród mniejszych dostawców usług internetowych oraz wśród firm korzystających z własnych systemów DNS.
6. Wspieranie rozwoju serwisu bezpiecznedane.gov.pl.
7. Stworzenie bezpiecznego resolvera DNS.

8. Kontynuowanie działań informacyjnych i edukacyjnych związanych z budowaniem świadomości cyberzagrożeń wśród użytkowników internetu.
9. Prowadzenie szkoleń dla firm obsługujących czy wdrażających systemy automatyki przemysłowej w lokalnych oczyszczalniach ścieków czy stacjach uzdatniania wody, aby poprawić bezpieczeństwo tych systemów i zapobiec atakom.
10. Uruchomienie publicznego programu Bug Bounty.
11. Zmiana klasyfikacji CSAM i ujednolicenie jej ze standardami światowymi (SCHEMA).

REKOMENDACJE NA 2026 - REKOMENDACJE DLA PEŁNOMOCNIKA RZĄDU DS. CYBERBEZPIECZEŃSTWA:

CSIRT NASK obserwuje ciągły wzrost zagrożeń zarówno w obszarze przestępczości zorganizowanej (ransomware), jak i grup sponsorowanych przez obce państwa (grup APT, haktywistycznych). Żeby skutecznie walczyć z tymi zagrożeniami, niezbędna jest jeszcze bliższa współpraca w ramach KSC oraz ze służbami specjalnymi. Częste są przypadki, że atak widziany przez jeden z CSIRT-ów jest tylko małym wycinkiem obrazu i nie da się go przeanalizować w całości bez współpracy. CSIRT NASK rekomenduje łączenie już istniejących systemów klasy TIP (Threat Intelligence Platform) w różnych organizacjach, aby usprawnić i przyspieszyć analizę zagrożeń.

CSIRT NASK rekomenduje rozpoczęcie prac legislacyjnych mających na celu wypracowanie skuteczniejszych metod dotarcia do właścicieli adresacji IP w przypadku stwierdzenia występowania podatności lub konfiguracji pozwalającej na atak.

Ze względu na wzrost liczby obserwowanych trendów dotyczących nielegalnych i szkodliwych treści, CSIRT NASK rekomenduje wypracowanie szybszych mechanizmów reagowania na szkodliwe treści przez platformy i organy ścigania, budowę narzędzi umożliwiających sprawniejszą identyfikację treści CSAM oraz rozwój ścieżek dystrybucji ostrzeżeń, a także rozbudowanej profilaktyki.

CSIRT-Y POZIOMU SEKTOROWEGO

W ramach KSC na poziomie operacyjnym funkcjonują dwa zespoły CSIRT poziomu sektorowego:

1) CSIRT KNF – sektorowy zespół cyberbezpieczeństwa dla sektora finansowego (prowadzony przez Urząd Komisji Nadzoru Finansowego)
2) CeZ– sektorowy zespół cyberbezpieczeństwa dla sektora ochrony zdrowia (prowadzony przez Centrum e-Zdrowia);

Zadania CSIRT-ów sektorowych określa art. 44 UKSC. Zgodnie z tymi przepisami, zespoły te są odpowiedzialne w szczególności za przyjmowanie zgłoszeń o incydentach poważnych, operacyjne wspieranie podmiotów w ich sektorach, analizowanie incydentów i poszukiwanie powiązań między nimi, a także ścisłą współpracę z zespołami CSIRT poziomu krajowego (GOV, MON, NASK) w zakresie koordynowania obsługi incydentów. W ramach nowelizacji UKSC kompetencje te są poszerzane m.in. o proaktywne wyszukiwanie podatności i wsparcie podmiotów kluczowych i ważnych.

W odpowiedzi na rosnącą skalę zagrożeń oraz wdrażanie dyrektywy NIS2, w 2025 roku rozpoczęto intensywne czynności (wspierane m.in. ze środków Krajowego Planu Odbudowy) celem powołania kolejnych zespołów. W fazie budowy i przygotowania do osiągnięcia gotowości operacyjnej znajdują się:

- CSIRT Cyfra – budowany w Ministerstwie Cyfryzacji dla sektora infrastruktury cyfrowej;
- CSIRT Infrastruktura – tworzony w Ministerstwie Infrastruktury dla sektora transportu oraz zaopatrzenia w wodę;
- CSIRT dla sektora energii.

CSIRT KNF

PODSUMOWANIE ROCZNE:

W analizowanym okresie krajobraz zagrożeń cyberbezpieczeństwa charakteryzował się wysoką dynamiką oraz rosnącą liczbą zdarzeń wpływających na dostępność i ciągłość działania systemów. Najistotniejszym wyzwaniem pozostawały ataki typu DDoS, a także awarie infrastrukturalne, w tym awarie po stronie dostawców zewnętrznych, które okresowo prowadziły do ograniczeń dostępności usług i wymagały skoordynowanych działań naprawczych.

Jednocześnie obserwowany jest globalny wzrost zagrożeń związanych z ransomware, w szczególności w modelu Ransomware as a Service (RaaS). Model ten znacząco obniża barierę wejścia dla cyberprzestępców, co przekłada się na zwiększoną liczbę oraz rosnącą złożoność ataków na całym świecie. Ataki ransomware coraz częściej łączą szyfrowanie danych z ich kradzieżą oraz szantażem, co istotnie zwiększa potencjalne skutki biznesowe incydentów. W związku z powyższym zagrożenie to należy traktować jako systemowe i długoterminowe ryzyko, na które sektor powinien pozostawać w stałej gotowości organizacyjnej i technicznej.

STATYSTYKI INCYDENTÓW:

Tabela 28. STATYSTYKI INCYDENTÓW CSIRT KNF

Kategoria	Liczba (rok bieżący)	Liczba (rok poprzedni)	Zmiana r/r (%)
Łączna liczba zarejestrowanych zgłoszeń	662	685	-3,4%
Łączna liczba obsłużonych poważnych incydentów ICT DORA	302	44	+586,4%*

**Znaczący wzrost liczby poważnych incydentów DORA r/r wynika ze zwiększenia liczby podmiotów zobligowanych do zgłaszania poważnych incydentów ICT.*

STATYSTYKI INCYDENTÓW (DORA/UKSC) W PODZIALE NA GŁÓWNE KATEGORIE TAKSONOMII REFERENCYJNEJ:

Tabela 29. STATYSTYKI INCYDENTÓW (DORA/UKSC) W PODZIALE NA GŁÓWNE KATEGORIE TAKSONOMII REFERENCYJNEJ

Lp.	Kategoria incydentu (wg taksonomii referencyjnej)	Liczba (rok bieżący)	Liczba (rok poprzedni)	Zmiana r/r (%)
1.	**Oszustwa komputerowe** *(Fraud)*	3	0	
2.	**Złośliwe oprogramowanie** *(Malicious Code)*	1	0	
3.	**Dostępność usług** *(Availability)*	289	43	572%
4.	**Próby włamań** *(Intrusion Attempts)*	0	0	
5.	**Bezpieczeństwo informacji** *(Information Content Security)*	5	0	
*	*Inne*	4	1	300%

NAJWAŻNIEJSZE ZAGROŻENIA:

Trend 1: Ataki socjotechniczne z wykorzystaniem AI

Ataki na klientów bankowości elektronicznej ewoluują z roku na rok, a przestępcy coraz sprawniej adaptują nowe technologie. Obserwujemy wykorzystanie generatywnej AI do tworzenia przekonujących treści phishingowych w języku polskim, pozbawionych wcześniej charakterystycznych błędów językowych. Poważnym problemem są fałszywe reklamy w wyszukiwarkach i mediach społecznościowych promujące oszukańcze platformy inwestycyjne. Przestępcy wykorzystują wizerunki znanych osób i nazwy rozpoznawalnych instytucji finansowych, by uwiarygodnić oferty "gwarantowanych zysków". Ofiary są następnie prowadzone przez fałszywych "doradców" i nakłaniane do kolejnych wpłat. Straty pojedynczych osób sięgają setek tysięcy złotych. Platformy reklamowe reagują z opóźnieniem na publikowane reklamy lub dopiero po zgłoszeniu, co pozwala kampaniom działać przez wiele dni.

Trend 2: Ransomware i ataki na łańcuch dostaw

Grupy ransomware aktywnie atakują polskie podmioty, w tym firmy współpracujące z sektorem finansowym. Obserwujemy model podwójnego wymuszenia - szyfrowanie danych połączone z groźbą ich publikacji. Szczególne ryzyko stanowią ataki na dostawców usług IT obsługujących instytucje finansowe. Kompromitacja jednego dostawcy może skutkować naruszeniem bezpieczeństwa wielu podmiotów nadzorowanych. Na bieżąco monitorujemy wycieki danych publikowane przez grupy ransomware i w przypadku zidentyfikowania powiązań z sektorem finansowym powiadamiamy zainteresowane podmioty. Ataki często inicjowane są przez skradzione dane uwierzytelniające lub exploitację podatności w publicznie dostępnych usługach. Rośnie także liczba ataków wykorzystujących zaufane relacje z dostawcami do uzyskania dostępu do systemów klientów końcowych.

Trend 3: Ataki DDOS wymierzone w sektor finansowy.

Sektor finansowy pozostaje częstym celem ataków DDoS wymierzonych w dostępność usług online. Ataki przybierają różne formy - od prostych ataków wolumetrycznych po bardziej wyrafinowane ataki aplikacyjne celujące w konkretne funkcjonalności serwisów bankowych. Motywacje atakujących są zróżnicowane: od prób wymuszenia okupu, przez działania konkurencji, po hacktywizm. W tym ostatnim przypadku aktywne pozostają prorosyjskie grupy (m.in. NoName057(16)), które atakują polską infrastrukturę finansową w kontekście wsparcia dla Ukrainy. Choć większość ataków jest skutecznie mitygowana, generują one obciążenie zespołów bezpieczeństwa i wymagają ciągłego dostosowywania mechanizmów ochrony. Ataki często są skoordynowane czasowo z wydarzeniami politycznymi.

OPIS JEDNEGO, NAJWAŻNIEJSZEGO INCYDENTU (CASE STUDY) :

Przebieg: W dniach 17-19 maja, w okresie pierwszej tury wyborów prezydenckich, jeden z podmiotów sektora finansowego został poddany serii skoordynowanych ataków DDoS. Pierwszy atak nastąpił 17 maja w godzinach 21:42-22:31 i trwał około 48 minut. Główna fala ataków rozpoczęła się 18 maja i trwała do wczesnych godzin 19 maja. Ataki występowały w kilkunastominutowych odstępach, często nakładając się na siebie. Atakujący celowali w różne elementy infrastruktury: bramki płatności 3DS, serwisy WWW, DNS oraz VPN.

Charakterystyka techniczna (TTPs): Kampania łączyła ataki nękające (140-500 Mbps, pakiety TCP ACK/SYN wymierzone w tablice sesji) z potężnymi uderzeniami wolumetrycznymi. Szczytowy wolumen osiągnął 1.3 Tbps. Głównym wektorem był UDP Amplification - technika polegająca na wykorzystaniu publicznie dostępnych serwerów w internecie do zwielokrotnienia siły ataku kierowanego na ofiarę. Ruch pochodził z rozproszonych źródeł, w tym przejętych urządzeń w Polsce, USA, Chinach i Brazylii.

Reakcja: Atak został wykryty natychmiast przez systemy monitoringu. Mechanizmy ochrony anty-DDoS zadziałały automatycznie, co pozwoliło na odfiltrowanie wrogiego ruchu przy zachowaniu dostępności usług dla klientów.

Skutki i wnioski: Dzięki przygotowanej infrastrukturze ochronnej atak nie spowodował przestoju w działaniu usług. Incydent potwierdził skuteczność wdrożonych mechanizmów obrony oraz znaczenie współpracy z dostawcą usług anty-DDoS. Zbieżność czasowa z wyborami wskazuje na polityczną motywację atakujących, co wpisuje się w szerszy trend ataków hacktywistycznych na polską infrastrukturę.

DZIAŁANIA STRATEGICZNE:

Projekt A: Wdrożenie oraz uruchomienie Systemu Do Obsługi Incydentów DORA

Jednym z kluczowych działań strategicznych było uruchomienie produkcyjne systemu do obsługi incydentów ICT, wspierającego wymagania wynikające z rozporządzenia DORA, w szczególności w zakresie zgłaszania znaczących cyberzagrożeń oraz poważnych incydentów. System został wdrożony równolegle z wejściem w życie regulacji DORA, zapewniając narzędziowe wsparcie dla realizacji obowiązków związanych z rejestracją, obsługą oraz raportowaniem zdarzeń.

Uruchomione rozwiązanie umożliwiło praktyczną realizację wymogów DORA poprzez ujednolicenie sposobu obsługi i raportowania incydentów oraz poprawę jakości i terminowości przekazywanych informacji. Realizacja projektu umożliwiła spójne i zgodne z regulacją DORA wykonywanie obowiązków związanych z obsługą oraz raportowaniem incydentów ICT.

Projekt B: Kontynuacja rozwoju systemów do wymiany informacji

Istotnym działaniem strategicznym była kontynuacja rozwoju platform do wymiany informacji o zagrożeniach i incydentach cyberbezpieczeństwa, opartych na narzędziach MISP oraz Mattermost. W ramach projektu zrealizowano podłączenie nowych źródeł informacji, a także rozszerzenie i rozwój już funkcjonujących integracji, co pozwoliło na zwiększenie zakresu oraz aktualności dostępnych danych.

Realizacja projektu umożliwiła dalsze ujednolicanie procesów wymiany informacji w ramach KSC oraz zwiększenie zdolności do bieżącego pozyskiwania i dystrybucji informacji o zagrożeniach, podatnościach i obserwowanych kampaniach cybernetycznych. Projekt stanowił element wsparcia operacyjnego dla podmiotów systemu w zakresie budowy wspólnej świadomości sytuacyjnej.

Projekt C: Udział w KPO i pozyskanie środków na rozwój zespołu CSIRT KNF.

Istotnym działaniem strategicznym był udział w przedsięwzięciach realizowanych w ramach Krajowego Planu Odbudowy, którego efektem było pozyskanie środków finansowych na rozwój CSIRT KNF.

Projekt koncentrował się na wzmocnieniu potencjału organizacyjnego i kompetencyjnego zespołu odpowiedzialnego za obsługę incydentów cyberbezpieczeństwa w sektorze finansowym.

Pozyskane środki umożliwiły realizację działań ukierunkowanych na rozwój zasobów ludzkich oraz wzmocnienie zdolności operacyjnych CSIRT KNF, w tym w obszarze reagowania na incydenty, analizy zagrożeń oraz wsparcia podmiotów sektora. Realizacja projektu stanowiła element długofalowych działań na rzecz zwiększania odporności cyberbezpieczeństwa sektora finansowego.

DZIAŁANIA I WSPÓŁPRACA:

DZIAŁANIA EDUKACYJNE I BUDOWANIE ŚWIADOMOŚCI:

W roku 2025 CSIRT KNF prowadził aktywnie działania edukacyjne w zakresie edukacji oraz budowania świadomości, opracowując 177 ostrzeżeń dotyczących najnowszych sposobów oraz metod działania cyberprzestępców. Publikowane komunikaty trafiały następnie do obiegu medialnego i były wykorzystane przez liczne ogólnopolskie portale informacyjne oraz branżowe. W 2025 roku przełożyło się to na 1995 publikacji prasowych opartych na informacjach przekazywanych przez CSIRT KNF.

Szczególnie istotnym elementem działań edukacyjnych był projekt CEDUR, w ramach którego w 2025 roku przeprowadzono 13 webinariów. Tematyka szkoleń obejmowała krytyczne aspekty cyberbezpieczeństwa, sposoby służące poprawie swojego bezpieczeństwa w sieci oraz problematykę cyberbezpieczeństwa dla środków finansowych użytkowników urządzeń mobilnych. Dodatkowo, zorganizowano 22 webinaria poświęcone Rozporządzeniu DORA, podczas których szczegółowo omówiono nowe wymogi regulacyjne dla podmiotów finansowych i dostawców usług ICT.

Tabela 30. DZIAŁANIA EDUKACYJNE I BUDOWANIE ŚWIADOMOŚCI

LP	Nazwa działania/kampanii	Grupa docelowa
1	**13 edycja kampanii Global Money Week (GMW) – Światowy Tydzień Pieniądza**	Uczniowie szkół podstawowych i ponadpodstawowych i nauczyciele
2	**World Investor Week – Światowy Tydzień Inwestora**	Uczniowie szkół ponadpodstawowych i nauczycieli oraz indywidualni uczestnicy rynku finansowego
3	Projekt edukacyjny **Centrum Edukacji dla Uczestników Rynku – CEDUR**, którego celem jest popularyzowanie wiedzy o cyberzagrożniach oraz wzmacnianie poziomu cyberbezpieczeństwa.	Webinaria CEDUR skierowane były do różnych grup odbiorców m.in.: • uczniów szkół uczniów szkół podstawowych i ponadpodstawowych oraz nauczycieli • seniorów oraz ich opiekunów • przedstawicieli instytucji ochrony praw nieprofesjonalnych uczestników rynku finansowego, w tym miejskich i powiatowych rzeczników konsumentów • pracowników banków komercyjnych i banków spółdzielczych • pracowników instytucji finansowych obsługujących klientów bankowości internetowej oraz osób zainteresowane tematyką cyberbezpieczeństwa • indywidualnych uczestników rynku finansowego, w tym inwestorów • podmiotów rynku finansowego • dostawców usług ICT dla podmiotów rynku finansowego
4	**Europejski Miesiąc Cyberbezpieczeństwa –** w ramach kampanii edukacyjnej CSIRT KNF skupił się na ochronie finansów i na ochronie danych osobowych użytkowników w Internecie. Podczas całego miesiąca publikowane były w mediach społecznościowych praktyczne porady oraz infografiki, które miały na celu ostrzeżenie przed najczęstszymi zagrożeniami w cyberprzestrzeni.	Użytkownicy Internetu zainteresowani tematyką cyberbezpieczeństwa
5	**CyberDay,** w ramach którego CSIRT KNF uczestniczył w wydarzeniu poświęconym budowaniu świadomości w zakresie cyberbezpieczeństwa	Pracownicy BGK

WSPÓŁPRACA KRAJOWA:

CSIRT KNF na bieżąco analizuje pojawiające się zagrożenia w obszarze cyberbezpieczeństwa, w tym ukierunkowane na ataki na klientów rynku finansowego. Uzyskane w ten sposób informacje wykorzystywane są do działań zapobiegających incydentom w podmiotach rynku finansowego. Działania te obejmują szybką identyfikację oraz ograniczanie dostępu do fałszywych stron internetowych. Niebezpieczne strony wykrywane przez CSIRT KNF zgłaszane są do CSIRT NASK, gdzie dokonywana jest ich blokada za pośrednictwem wpisania na listę ostrzeżeń.

CSIRT KNF przekazuje także do działu analitycznego Meta materiały służące do przestępstw w celu ograniczania skutków fałszywych inwestycji.

W ramach współpracy CERT Polska i CSIRT KNF stworzony został projekt moje.cert.pl. Jest to wspólna inicjatywa zwiększająca bezpieczeństwo sektora finansowego i usprawniająca wymianę informacji o incydentach i podatnościach. Instytucje finansowe biorące udział w programie zyskują szybki dostęp do informacji o nowych zagrożeniach, alerty i komunikaty o aktualnych atakach oraz podatnościach, a także możliwość bieżącego monitorowania stanu bezpieczeństwa swojej infrastruktury.

Zespół CSIRT KNF współpracuje z podmiotami i organizacjami rozwijającymi kompetencje w dziedzinie cyberbezpieczeństwa oraz udziela im wsparcia w ramach programu Partnerstwo dla Cyberbezpieczeństwa (PdC).

Pracownicy zespołu CSIRT KNF prowadzą wybrane zajęcia dydaktyczne na studiach podyplomowych w ramach współpracy z Wyższą Szkołą Policji w Szczytnie, dzieląc się swoim doświadczeniem w obszarze ataków na środki finansowe klientów w cyberprzestrzeni oraz cyberryzyka i cyberbezpieczeństwa wewnętrznego organizacji.

CSIRT KNF uczestniczy w cotygodniowych spotkaniach PCOC, gdzie wymienia informacje o cyberagrożeniach z kluczowymi instytucjami dla bezpieczeństwa Państwa. Zespół CSIRT KNF bierze udział także w sektorowych spotkaniach statusowych dla zespołów CSIRT poziomu krajowego oraz zespołów CSIRT sektorowych, gdzie wymienia się wiedzą, obserwacjami czy doświadczeniami co pozwala na szybsze identyfikowanie zagrożeń.

ĆWICZENIA I WSPÓŁPRACA MIĘDZYNARODOWA:

Zespół CSIRT KNF podejmował aktywną działalność w zakresie uczestnictwa w ćwiczeniach cyberbezpieczeństwa w formułach Table Top oraz Attack-Defense na szczeblu krajowym. Zaangażowanie zespołu obejmowało także realizację zadań w obszarze międzynarodowych grup roboczych i społeczności, związanych z cyberzagrożeniami oraz wzmacnianiem odporności sektora. Realizacja czynności przyczyniała się poszerzania świadomości, wymiany informacji, kształtowania sieci współpracy międzyinstytucjonalnych oraz budowania kompetencji członków zespołu.

Tabela 31. ĆWICZENIA I WSPÓŁPRACA MIĘDZYNARODOWA

LP	Nazwa	Data	Rola CSIRT	Zasięg	Opis scenariusza
1	KSC – EXE 2025	11.2025	Uczestnik	Krajowy	Ćwiczenia Table Top / Sprawdzenie działania procedur oraz weryfikacja zdolności operacyjnych podmiotów KSC w sytuacji kryzysowej spowodowanej cyberatakiem.
2	CyberFIGHT Bank.02-2025	06.2025	Uczestnik	Krajowy	Aktywne uczestnictwo i rywalizacja w ramach zorganizowanych zawodów CTF w formule Attack-Defense.
3	FS-ISAC	Współpraca w ramach członkostwa	Uczestnik	Międzynarodowy	Zespół CSIRT KNF uczestniczy w członkostwie FS-ISAC, w ramach którego posiada możliwość pozyskiwania i wymiany informacji o zagrożeniach dotykających sektora finansowego.
4	Trusted Introducer	Współpraca w ramach członkostwa	Uczestnik	Międzynarodowy	Serwis Trusted Introducer zrzesza wiele zespołów CSIRT z całego świata. CSIRT KNF utrzymuje status zespołu akredytowanego, posiada dostęp do zamkniętego grona, otrzymuje także dostęp do repozytorium wymiany wiedzy na temat panujących zagrożeń i trendów.
5	EU-SCICF	01.2025, 03.2025, 05.2025, 09.2025, 11.2025, realizacja zadań bieżących	Uczestnik	Międzynarodowy	Ułatwienie operacjonalizacji skutecznej koordynacji na szczeblu UE (trybu kryzysowego) w przypadku transgranicznych poważnych incydentów, związanych z ICT lub związanych z nimi zagrożeń, które mogłyby mieć systemowy wpływ na sektor finansowy Unii Europejskiej.
6	TIBER-EU	01.2025, 02.2025, 03.2025, 06.2025, 09.2025, 12.2025, realizacja działań bieżących	Uczestnik	Międzynarodowy	Uczestnictwo w grupach roboczych w ramach TIBER-EU Knowledge Centre and community (TKC), podejmowanie aktywności związanej tematyką testów TIBER / TLPT.

ANALIZA I OCENA FUNKCJONOWANIA KSC:

UKSC stanowi istotny element krajowych ram prawnych w obszarze cyberbezpieczeństwa i stworzyła podstawy do uporządkowania ról, odpowiedzialności oraz zasad współpracy pomiędzy kluczowymi podmiotami systemu. Wprowadzenie jednolitych mechanizmów raportowania incydentów oraz funkcjonowanie zespołów CSIRT na poziomie krajowym przyczyniły się do zwiększenia przejrzystości działań oraz lepszego rozpoznania zagrożeń w skali kraju.

W praktyce funkcjonowanie UKSC wspiera budowę wspólnej świadomości zagrożeń oraz stopniowe podnoszenie poziomu dojrzałości organizacyjnej i technicznej podmiotów objętych regulacją. Widoczny jest również rozwój zdolności reagowania na incydenty oraz rosnące znaczenie współpracy i wymiany informacji pomiędzy uczestnikami systemu.

Jednocześnie, ze względu na złożoność systemu oraz różnorodność podmiotów, ocena efektywności funkcjonowania UKSC opiera się obecnie głównie na dostępnych raportach cząstkowych i sprawozdaniach operacyjnych. Dokumenty te dostarczają cennych informacji o trendach i aktywnościach, jednak nie pozwalają na pełne, przekrojowe spojrzenie na całościowe działanie systemu.

Podsumowując, UKSC stanowi stabilną podstawę dla rozwoju KSC. Dalsze działania mogą koncentrować się na pogłębianiu współpracy, doskonaleniu mechanizmów koordynacji oraz stopniowym rozwijaniu narzędzi umożliwiających bardziej kompleksowe spojrzenie na funkcjonowanie systemu w obliczu dynamicznie zmieniających się zagrożeń.

PROGNOZY I PRZEWIDYWANIA DLA KSC NA ROK 2026:

Planowane kierunki rozwoju UKSC, związane z jej nowelizacją, wskazują na rosnące znaczenie wymiany informacji oraz koordynacji działań pomiędzy podmiotami systemu. W warunkach coraz bardziej złożonych i dynamicznych zagrożeń cybernetycznych kluczowe staje się szybkie przekazywanie informacji o incydentach, podatnościach oraz obserwowanych kampaniach ataków.

Wzmocnienie mechanizmów współpracy pomiędzy podmiotami KSC, zespołami CSIRT oraz organami właściwymi może przyczynić się do wcześniejszej detekcji zagrożeń i skuteczniejszego reagowania na incydenty o charakterze sektorowym lub krajowym. Nowelizacja UKSC postrzegana jest w tym kontekście jako krok w kierunku bardziej zintegrowanego i proaktywnego systemu, w którym wymiana informacji wspiera budowę wspólnej świadomości sytuacyjnej oraz odporności całego systemu cyberbezpieczeństwa.

PLANY NA ROK 2026:

W 2026 r. planowane są działania w tym rozwój kompetencji zespołu CSIRT KNF, w szczególności w obszarach reagowania na incydenty, analizy zagrożeń oraz wsparcia podmiotów rynku finansowego.

Równolegle, z wykorzystaniem środków pozyskanych z KPO, przewidywana jest organizacja ćwiczeń cyberbezpieczeństwa dla rynku finansowego, których celem będzie wzmocnienie gotowości uczestników rynku do reagowania na incydenty oraz doskonalenie współpracy i wymiany informacji.

Istotnym elementem działań w 2026 roku będzie również zwiększanie udziału podmiotów sektora w funkcjonującym portalu moje.cert.pl. Aktywne korzystanie z platformy umożliwia szybszą identyfikację i reagowanie na zagrożenia, dostęp do komunikatów dedykowanych sektorowi finansowemu oraz zapewnia eksperckie wsparcie w zakresie podatności i rekomendowanych działań naprawczych.

REKOMENDACJE NA 2026 - REKOMENDACJE DLA PEŁNOMOCNIKA RZĄDU DS. CYBERBEZPIECZEŃSTWA:

1. Organizacja regularnych ćwiczeń krajowych i sektorowych

Rekomenduje się organizację regularnych ćwiczeń cyberbezpieczeństwa na poziomie krajowym i sektorowym, ukierunkowanych na doskonalenie wymiany informacji, koordynacji działań oraz reagowania na zagrożenia. Ćwiczenia powinny obejmować realistyczne scenariusze incydentów o charakterze wielopodmiotowym, umożliwiając praktyczną weryfikację procedur oraz kanałów komunikacji w ramach KSC.

2. Wzmacnianie mechanizmów wymiany informacji w ramach KSC

Zasadne jest dalsze rozwijanie i uwspólnianie mechanizmów wymiany informacji pomiędzy podmiotami KSC, zespołami CSIRT oraz właściwymi organami. Sprawna i terminowa wymiana informacji o incydentach i zagrożeniach wspiera budowę wspólnej świadomości sytuacyjnej oraz zwiększa zdolność systemu do reagowania na zdarzenia o charakterze sektorowym i krajowym.

3. Wspieranie inicjatyw podnoszących dojrzałość podmiotów KSC

Rekomenduje się wspieranie działań ukierunkowanych na stopniowe podnoszenie dojrzałości organizacyjnej i procesowej podmiotów KSC, w szczególności poprzez promowanie wymiany dobrych praktyk, rozwój kompetencji oraz dążenie do bardziej spójnego poziomu przygotowania w zakresie cyberbezpieczeństwa.

CENTRUM E-ZDROWIA – CSIRT CEZ

PODSUMOWANIE ROCZNE:

- Odnotowano wzrost dynamiki zagrożeń w sektorze ochrony zdrowia – liczba zarejestrowanych incydentów wzrosła o 40% rok do roku.
- Skala ataków oraz niska dojrzałość infrastrukturalna podmiotów sektora (brak zapasowych urządzeń, systemy EoL, braki kadrowe) generują ryzyko dla ciągłości udzielania świadczeń medycznych i bezpieczeństwa pacjentów.
- W odpowiedzi na powyższe wyzwania, celem zapewnienia realizacji wymogów KSC oraz dyrektywy NIS2, trwa proces zakupu w ramach KPO mobilnego zestawu do awaryjnego przywracania usług.
- Trwa proces zakupu pakietu szkoleń mających podnieść kompetencje zespołu CSIRT.
- Inicjatywy współpracy i budowa synergii.
- Udział w ćwiczeniach KSC EXE pozwolił na przetestowanie kanałów komunikacji kryzysowej.
- Aktywność w Work Stream 12 oraz Medical Device Cybersecurity Task Force zapewnia wpływ na tworzenie norm bezpieczeństwa dla urządzeń medycznych.

STATYSTYKI INCYDENTÓW:

Tabela 32. Statystyki Incydentów

Kategoria	Liczba (rok bieżący) (2025)	Liczba (rok poprzedni) (2024	Zmiana r/r (%)
Łączna liczba zarejestrowanych zgłoszeń	1441	1028	40%
Łączna liczba obsłużonych incydentów	1441	1028	40%

STATYSTYKI INCYDENTÓW W PODZIALE NA GŁÓWNE KATEGORIE TAKSONOMII REFERENCYJNEJ:

Tabela 33. STATYSTYKI INCYDENTÓW W PODZIALE NA GŁÓWNE KATEGORIE TAKSONOMII REFERENCYJNEJ

Lp.	Kategoria incydentu (wg taksonomii referencyjnej	Liczba (rok bieżący) (2025)	Liczba (rok poprzedni) (2024)	Liczba (rok poprzedni) (2024)
1	Oszustwa komputerowe (Fraud)	580	374	55%
2	Złośliwe oprogramowanie (Malicious Code	146	93	57%
3	Dostępność usług (Availability)	28	53	-47%
4	Próby włamań (Intrusion Attempts	15	1+	-6%
5	Bezpieczeństwo informacji (Information Content	14	24	-42%
6	Inne	6	2	200%

NAJWAŻNIEJSZE ZAGROŻENIA:

Trend 1: Oszustwa sieciowe (phishing i podszywanie się)

Opis: Atakujący coraz częściej wykorzystują phishing, podszywając się pod placówki medyczne lub NFZ w celu kradzieży danych pacjentów i kont personelu. Wiadomości e-mail i SMS z fałszywymi linkami prowadzą do wyłudzeń danych logowania lub instalacji złośliwego oprogramowania.

Trend 2: Błędna konfiguracja systemów i wykryte podatności

Opis: Incydenty wynikają głównie z błędnych konfiguracji serwerów i systemów medycznych, a także z nieaktualnych aplikacji przechowujących dane pacjentów. Wykorzystanie znanych podatności umożliwia nieuprawniony dostęp do zasobów wrażliwych.

Trend 3: Naruszenia poufności i integralności danych

Opis: Najczęstsze przyczyny to brak MFA, słabe hasła oraz lekceważenie zasad bezpieczeństwa przez użytkowników. Skutkiem są przejęcia kont i wycieki danych logowania prowadzące do utraty poufności informacji medycznych. Konieczne jest wzmocnienie monitorowania aktywności użytkowników oraz szybsze wykrywanie anomalii w zachowaniu kont.

OPIS JEDNEGO, NAJWAŻNIEJSZEGO INCYDENTU (CASE STUDY):

W 2025 roku zespół CSIRT CeZ koordynował proces reagowania, analizy oraz mitygacji szeregu incydentów bezpieczeństwa w podmiotach sektora ochrony zdrowia.

Najważniejszy odnotowany incydent był incydentem poważnym (atak typu ransomware), który doprowadził do zakłócenia działania infrastruktury teleinformatycznej w podmiocie medycznym MSWiA w Krakowie. Incydent w pierwszej kolejności został zgłoszony do CBZC. Zespół CBZC jako pierwszy podjął czynności na miejscu zdarzenia.

Równolegle zespół CSIRT CeZ oraz administrator infrastruktury CeZ rozpoczął przygotowanie sprzętu celem wsparcia podmiotu w odzyskiwaniu ciągłości świadczenia usług. W analizę materiału dowodowego został włączony również zespół CERT Polska. Ślady podejrzanych działań miały miejsce m.in. już 02.10.2023 oraz 20.07.2024. Wektorem ataku najprawdopodobniej było urządzenie sieciowe Fortigate:

- Konta używały niewystarczająco złożonych haseł i były proste do odgadnięcia. Konfiguracja urządzenia była niewystarczająca, ponieważ umożliwiała w 30 minutowych odstępach podejmować próbę logowania;
- urządzenie nie było aktualizowane - było podatne na CVE-2019-6693 co umożliwiało odszyfrowanie haseł z pliku konfiguracyjnego.

Ze względu na brak potwierdzenia dotyczącego wektora ataku oraz brakujące, usunięte przez atakującego logi, nie było możliwości przekazania wszystkich niezbędnych zaleceń. W związku z powyższym podmiot otrzymał wsparcie w trakcie przywracania usług w oparciu o najlepsze praktyki stosowane w bezpieczeństwie które można wdrożyć w podmiocie.

DZIAŁANIA STRATEGICZNE:

Projekt A: Projekt realizowany ze środków KPO pn. Poprawa poziomu cyberbezpieczeństwa w obszarze ochrony zdrowia poprzez rozwój Sektorowego Zespołu CSIRT

Celem projektu jest poprawa poziomu cyberbezpieczeństwa w obszarze ochrony zdrowia poprzez rozwój sektorowego CSIRT. Przedsięwzięcie zapewnia kompleksowe podejście do aspektów bezpieczeństwa cyberprzestrzeni, poprzez realizację działań uwzględniających zarówno zakup narzędzi informatycznych - sprzętu i oprogramowania, jak również wsparcie odpowiedniego zaplecza eksperckiego, usługi konsultingowe i audytorskie, szkolenia pracowników CSIRT oraz działania promocyjne i tworzenie

materiałów edukacyjnych, skierowanych do placówek medycznych i ich personelu. Budżet projektu to 13 125 924,00 zł, a okres realizacji to od 01.04.2025 r. do 30.06.2026 r. Wniosek o dofinansowanie został wysłany w kwietniu 2025 r. Porozumienie o dofinansowaniu zostało podpisane 1 sierpnia 2025 r. W ramach projektu były realizowane bieżące zadania projektowe na poziomie zarządczym oraz przygotowywane dokumenty do postępowań przetargowych (łącznie 13 w ramach kosztów bezpośrednich).

DZIAŁANIA I WSPÓŁPRACA:

DZIAŁANIA EDUKACYJNE I BUDOWANIE ŚWIADOMOŚCI:

Tabela 34. DZIAŁANIA EDUKACYJNE I BUDOWANIE ŚWIADOMOŚCI

LP	Nazwa działania/kampanii	Grupa docelowa	Liczba odbiorców
1	Szkolenie cykliczne (14 szkoleń), przeprowadzone w 2025 r., pn. Jak chronić sektor ochrony zdrowia przed atakami ransomware?	Pracownicy placówek medycznych, kadra zarządzająca, administracyjna, działy IT	680
2	Szkolenia o cyberhigienie dla Kierowników placówek sektora	Kadra zarządzająca placówkami medycznymi	711
3	Szkolenia o cyberhigienie w ramach CeZ oraz MZ	Pracownicy CeZ oraz MZ	464
4	Przeprowadzone szkolenia o cyberhigienie w ramach konferencji MCB	B/D	1800
5	Przeprowadzone szkolenia o cyberhigienie w ramach konferencji PIRB	B/D	240

WSPÓŁPRACA KRAJOWA:

Podczas realizacji codziennych zadań CSIRT CeZ ściśle współpracuje z krajowymi CSIRTami oraz z podmiotami zajmującymi się zwalczaniem cyberprzestępczości, takimi jak CBZC oraz - DKWOC. Współpraca z CSIRT NASK umożliwia szybką wymianę informacji o incydentach i nowych zagrożeniach, co pozwala na natychmiastową reakcję i ograniczenie ryzyka dalszych ataków. Dzięki bieżącej wymianie wiedzy o technikach cyberataków, podatnościach i skutecznych metodach obrony zespół stale rozwija swoje kompetencje i zwiększa skuteczność działań.

W ramach formalnych porozumień pomiędzy CBZC oraz DKWOC utrzymywana jest szybka ścieżka wymiany informacji o zagrożeniach, co sprzyja skoordynowanemu reagowaniu na incydenty oraz budowaniu spójnego systemu ochrony w kraju. CSIRT CeZ od początku swojej działalności korzysta z różnych narzędzi i źródeł informacji, w tym z systemu Artemis oraz platformy n6 opracowanej przez CSIRT NASK, które wspierają analizę i wykrywanie podatności oraz błędnych konfiguracji w infrastrukturze podmiotów sektora ochrony zdrowia. Po identyfikacji problemu zespół niezwłocznie informuje daną organizację, przekazując zalecenia i ostrzeżenia dotyczące zagrożeń.

Kluczowym elementem działalności CSIRT CeZ jest również wykorzystanie platformy s46, służącej do obsługi incydentów bezpieczeństwa i rozsyłania ostrzeżeń w ramach komunikacji międzysektorowej. Dzięki niej możliwa jest szybka, bezpieczna i ujednolicona wymiana informacji pomiędzy zespołami CSIRT oraz instytucjami odpowiedzialnymi za bezpieczeństwo różnych sektorów, co znacząco usprawnia proces reagowania i koordynacji działań.

Zespół aktywnie uczestniczy w inicjatywach branżowych, w tym w Programie Partnerstwo dla Cyberbezpieczeństwa (PdC), współtworząc działania zwiększające odporność kraju na zagrożenia w cyberprzestrzeni. Na poziomie międzynarodowym CSIRT CeZ jest częścią The Trusted Introducer

Service jako Listed Team, co potwierdza jej kompetencje oraz umożliwia wymianę informacji i doświadczeń z zespołami CSIRT z całej Europy.

Dzięki szerokiej współpracy, dostępowi do zaawansowanych systemów i aktywnemu udziałowi w krajowych i międzynarodowych inicjatywach, CSIRT CeZ skutecznie wspiera bezpieczeństwo informatyczne sektora ochrony zdrowia i wzmacnia odporność całego ekosystemu na zagrożenia.

ĆWICZENIA I WSPÓŁPRACA MIĘDZYNARODOWA:

Tabela 35. ĆWICZENIA I WSPÓŁPRACA MIĘDZYNARODOWA

Nazwa	Data	Rola CSIRT	Zasięg	Opis scenariusza / Cel współpracy
Udział w KSC EXE	Q4/25	uczestnik	Krajowy	Udział jako uczestnik w dniu 26.11.2025 r. KSC - Executive Exercises) to cykliczne, międzysektorowe symulacje cyberataków, organizowane w Polsce przez Ministerstwo Cyfryzacji oraz Fundację Bezpieczna Cyberprzestrzeń w celu weryfikacji gotowości podmiotów z kluczowych sektorów, w tym sektora zdrowia.
Udział w spotkaniach grupy Work Stream 12				26 listopada 2025 odbyło się 24. spotkanie Work Stream on Health w ramach Grupy współpracy NIS, z udziałem CSIRT CeZ. Uczestnicy omówili postępy we wdrażaniu dyrektywy NIS2 w sektorze zdrowia w poszczególnych krajach oraz działania nadzorcze wspierające podmioty w realizacji obowiązków. Wymieniono doświadczenia dotyczące poważnych incydentów i bieżących prac w państwach członkowskich. Przedstawiono informacje Komisji Europejskiej o finansowaniu działań z europejskiego planu cyberbezpieczeństwa szpitali, pracach dotyczących regulacji (Cybersecurity Act, Digital Omnibus, MDR/IVDR, EHDS) oraz opracowywaniu rekomendacji i nowych wymagań bezpieczeństwa oraz przedstawiono dostępne źródła finansowania inicjatyw.
MedicalDevic **Cybersecurity Task Force**				W 2025 r. odbył się szereg spotkań grupy roboczej, której działania zostały podsumowane w ramach raportu
Współpraca z komponente m ZDC cyber WOT	Q4/25	Współ-organiztor	Krajowy	8.12.2025 r. zostało zorganizowane I wspotkanie wprowadzające. Do końca 2025 r. trwał proces opiniowania prozumienia, które sformalizuje dalszą współpracę.

ANALIZA I OCENA FUNKCJONOWANIA KSC:

Zespół CSIRT-CEZ co roku publikuje ankietę roczną badającą poziom dojrzałości podmiotów w zakresie cyberbezpieczeństwa. Planowany termin zakończenia zbierania informacji został przedłużony do 13.02.2026. Z dotychczasowych posiadanych przez zespół CSIRT-CEZ sektor ochrony zdrowia boryka się z kilkoma problemami:

- Niski poziom dojrzałości: Podmioty mają trudności z wypełnieniem obecnych wymagań ustawowych;
- Problemy kadrowe: Brakuje specjalistów nie tylko od cyberbezpieczeństwa ale także informatyków czy administratorów. Powodem mogą być niewystarczające fundusze i brak regularnych szkoleń dla obecnej kadry;
- Aspekty finansowe: Szpitale i inne podmioty nie mają wystarczających funduszy na bezpieczeństwo, sprzęt IT oraz specjalistyczne oprogramowanie;
- Niska świadomość: Kadra kierownicza często nie rozumie, jak duże ryzyko niosą ze sobą ataki hakerskie i nie rozumieją potrzeb związanych z cyfryzacją oraz cyberbezpieczeństwem.

PROGNOZY I PRZEWIDYWANIA DLA KSC NA ROK 2026:

W związku z planowanym wejściem w życie nowelizacji UKSC, przewidujemy następujące wyzwania:

- Skokowy, kilkukrotny wzrost liczby podmiotów objętych systemem w sektorze ochrony zdrowia.
- Zdecydowana większość nowych podmiotów nie będzie gotowa na przyjęcie i realizację nowych obowiązków wynikających z ustawy.
- Większa liczba podmiotów przełoży się na proporcjonalnie większą liczbę zgłaszanych i obsługiwanych incydentów. W związku z faktem, że podmioty te będą wymagać dużego wsparcia w celu osiągnięcia minimalnych wymagań CSIRTy sektorowe staną przed koniecznością zwiększenia zatrudnienia, aby podołać wsparciu zarówno technicznemu jak i edukacyjnemu dla nowych jak i już obecnych w systemie podmiotów.

PLANY NA ROK 2026:

Plan na 2026r skupia się na wsparciu podmiotów w spełnieniu nowych wymagań oraz inwestycjach technologicznych.

Działania edukacyjne i szkoleniowe:

- Uruchomienie dedykowanej platformy e-learningowej;
- Dalszy rozwój szkoleń online skierowanych do kadr szpitalnych;
- Organizacja konferencji branżowej.

Wsparcie techniczne:

- Inwestycje w ramach KPO, w tym tzw. “Cyberkaretki” czyli zestawu do awaryjnego przywracania usług IT w podmiotach objętych incydentem;
- Wdrożenie narzędzi do cyklicznego skanowania podatności;
- Pozyskanie narzędzi do zautomatyzowanych pentestów na potrzeby wsparcia podmiotów w analizie stanu zabezpieczeń ich infrastruktury;
- Publikowanie bardziej szczegółowych, technicznych wytycznych dotyczących wdrożeń narzędzi bezpieczeństwa.

Pozostałe:

- Utworzenie ankiety samooceny dla podmiotów pomagająca w ocenie czy podmiot w świetle nowelizacji KSC jest podmiotem ważnym (PW) czy podmiotem kluczowym (PK)
- Zacieśnienie współpracy i wymiana informacji z podmiotami;
- Zwiększenie częstotliwości wizyt w podmiotach;
- Zwiększenie współpracy z innymi zespołami cyberbezpieczeństwa oraz CSIRTów sektora ochrony zdrowia w Europie.

REKOMENDACJE NA 2026 - REKOMENDACJE DLA PEŁNOMOCNIKA RZĄDU DS. CYBERBEZPIECZEŃSTWA:

Wsparcie w koordynacji działań zespołów cyberbezpieczeństwa w celu uniknięcia dublowania prac lub wsparcie w inicjowaniu współpracy międzyresortowych.

ORGANY WŁAŚCIWE DO SPRAW CYBERBEZPIECZEŃSTWA I SEKTOROWE ZESPOŁY CYBERBEZPIECZEŃSTWA

Organy właściwe i ich zadania zdefiniowane są w art. 41 UKSC. Przepisy te przewidują istnienie następujących sektorów i odpowiedzialnych za nich organów:

1) sektor energii – minister właściwy do spraw energii (Minister Energii Do celów statystycznych incydenty krytyczne uwzględniają jedynie incydenty, w ramach których CSIRT GOV [6]);
2) sektor transportu z wyłączeniem podsektora transportu wodnego – minister właściwy do spraw transportu (Minister Infrastruktury);
3) podsektor transportu wodnego – minister właściwy do spraw gospodarki morskiej i minister właściwy do spraw żeglugi śródlądowej (Minister Infrastruktury);
4) sektor bankowy i infrastruktury rynków finansowych – Komisja Nadzoru Finansowego;
5) sektor ochrony zdrowia (z wyłączeniem podmiotów podległych MON) – minister właściwy do spraw zdrowia (Minister Zdrowia);
6) sektor ochrony zdrowia obejmujący podmioty podległe MON - Minister Obrony Narodowej;
7) sektor zaopatrzenia w wodę pitną i jej dystrybucji – minister właściwy do spraw gospodarki wodnej (Minister Infrastruktury);
8) sektor infrastruktury cyfrowej (z wyłączeniem podmiotów podległych MON) – minister właściwy do spraw informatyzacji (Minister Cyfryzacji);
9) sektor infrastruktury cyfrowej obejmujący podmioty podległe MON - Minister Obrony Narodowej;
10) dostawcy usług cyfrowych (z wyłączeniem podmiotów podległych MON) - minister właściwy do spraw informatyzacji (Minister Cyfryzacji);
11) dostawcy usług cyfrowych obejmujący podmioty podległe MON - Minister Obrony Narodowej.

[6] Do sierpnia 2025 r. organem właściwym do spraw cyberbezpieczeństwa w sektorze energii był Minister Klimatu i Środowiska.

SEKTOR ENERGII - MINISTER ENERGII (ME)

PODSUMOWANIE ROCZNE:

W analizowanym roku działania organu właściwego ds. cyberbezpieczeństwa sektora energii koncentrowały się na identyfikacji operatorów usług kluczowych, prowadzeniu postępowań administracyjnych (o uznanie za OUK, o nałożenie kar) oraz sprawowaniu bieżącego nadzoru nad podmiotami KSC. Istotnym elementem tych działań była analiza sektora pod kątem zmian organizacyjnych po stronie operatorów usług kluczowych, w tym aktualizacja danych kontaktowych oraz weryfikacja statusu podmiotów w związku z przejęciami i fuzjami.

Szczególną uwagę poświęcono analizie sprawozdań z audytów bezpieczeństwa systemów informacyjnych przeprowadzanych przez operatorów usług kluczowych. W wielu przypadkach była to kolejna tura audytów realizowanych u tych samych podmiotów, co umożliwiło porównanie wyników w ujęciu ciągłym. Analiza ta wskazuje na stopniowy wzrost dojrzałości sektora w obszarze cyberbezpieczeństwa, poprawę poziomu odporności systemów oraz rosnącą świadomość operatorów usług kluczowych. Widoczny jest trend polegający na zmniejszaniu liczby zaleceń poaudytowych.

Działania nadzorcze obejmowały nie tylko ocenę formalną sprawozdań z audytów, lecz także merytoryczną, czego wynikiem było m.in. kierowanie do operatorów usług kluczowych pism dotyczących stopnia wdrożenia zaleceń poaudytowych oraz planowanych terminów ich realizacji. Pozwoliło to na bieżące monitorowanie postępów w usuwaniu stwierdzonych nieprawidłowości oraz wzmocnienie funkcji nadzorczej organu właściwego.

Równolegle realizowane były prace w ramach projektu KPO C3.1.1, którego celem jest utworzenie sektorowego zespołu CSIRT. W ramach projektu prowadzono analizy przygotowawcze, w tym weryfikację potrzeb operatorów usług kluczowych w zakresie przyszłych usług CSIRTowych oraz oczekiwań sektora energii w obszarze wsparcia reagowania na incydenty i wymiany informacji. Decyzją kierownictwa ME, CSIRT powstanie poza strukturami ME, jednakże dokonane analizy zostaną wykorzystane w innych procesach.

Dodatkowym czynnikiem wpływającym na realizację zadań w ciągu roku była trwająca przez znaczną jego część kontrola Najwyższej Izby Kontroli, która stanowiła istotne obciążenie zadaniami względem organu właściwego.

Z perspektywy organu właściwego ds. cyberbezpieczeństwa, całokształt podjętych działań oraz wnioski płynące z kolejnych cykli audytowych pozwalają ocenić ogólną sytuację w cyberprzestrzeni sektora energii jako stabilną, z widoczną tendencją wzrostową w zakresie dojrzałości, odporności oraz skuteczności zarządzania cyberbezpieczeństwem przez operatorów usług kluczowych.

DZIAŁANIA STRATEGICZNE:

Projekt A: Projekt KPO C3.1.1 - utworzenie sektorowego zespołu CSIRT dla sektora energii

W 2025 r. organ właściwy ds. cyberbezpieczeństwa w sektorze energii realizował działania przygotowawcze w ramach projektu KPO C3.1.1, którego celem było utworzenie sektorowego CSIRT dedykowanego sektorowi energii. Projekt zakładał wzmocnienie zdolności sektora do reagowania na incydenty cyberbezpieczeństwa, poprawę wymiany informacji oraz wsparcie OUK.

W ramach projektu prowadzono prace koncepcyjne i analityczne, obejmujące przygotowanie koncepcji funkcjonowania CSIRT, opracowanie i złożenie wniosku o dofinansowanie oraz analizy sektorowe dotyczące potrzeb operatorów usług kluczowych i oczekiwanego zakresu usług CSIRT. Projekt uzyskał pozytywną ocenę wniosku oraz informację o wyborze do objęcia przedsięwzięcia wsparciem.

Decyzją kierownictwa Ministerstwa Energii odstąpiono od zawarcia umowy na dofinansowanie projektu i jego realizacji, jednak prace przygotowawcze prowadzone przez okres około czterech miesięcy stanowiły istotny element działań strategicznych w 2025 r., a ich wyniki mogą zostać wykorzystane w przyszłych inicjatywach.

Projekt B: Przygotowanie podstaw prawnych oraz udział w pracach nad implementacją Network Code on Cybersecurity for Electricity (NC CS)

W 2025 r. realizowano działania strategiczne związane z wdrażaniem Network Code on Cybersecurity for Electricity (NC CS) w krajowym porządku prawnym oraz udziałem w pracach na poziomie UE. W ramach projektu opracowano propozycje przepisów prawnych umożliwiających stosowanie NCCS w Polsce, w tym rozwiązania przewidujące wyznaczenie Ministra Energii jako organu właściwego ds. cyberbezpieczeństwa w sektorze energii, przygotowane w związku z nowelizacją UKSC (UC32).

Równolegle, organ brał udział w opiniowaniu dokumentów opracowywanych na poziomie europejskim, w szczególności tymczasowej listy norm i środków bezpieczeństwa wymaganych przez krajowe przepisy prawa w kontekście cyberbezpieczeństwa transgranicznych przepływów energii elektrycznej. Uzupełniająco przedstawiciele organu uczestniczyli w pracach ACER, obejmujących dyskusję nad metodologiami oceny ryzyka przygotowanymi przez ENTSO-E oraz EU DSO Entity.

Projekt C: Utworzenie podstaw organizacyjnych i prawnych funkcjonowania organu właściwego ds. cyberbezpieczeństwa w sektorze energii

W 2025 r., w związku z utworzeniem Ministerstwa Energii w sierpniu 2025 r., realizowano działania o charakterze strategicznym polegające na stworzeniu podstaw organizacyjnych i prawnych funkcjonowania organu właściwego ds. cyberbezpieczeństwa w sektorze energii. Projekt obejmował prace nad ukształtowaniem struktury organizacyjnej, określeniem zakresu kompetencji oraz przypisaniem zadań związanych z wykonywaniem funkcji organu właściwego wynikających z UKSC. Równolegle prowadzono działania mające na celu zapewnienie ciągłości realizacji zadań nadzorczych, w tym identyfikacji podmiotów objętych właściwością organu. Projekt miał znaczenie strategiczne, gdyż umożliwił rozpoczęcie wykonywania zadań organu właściwego w nowej strukturze organizacyjnej.

DZIAŁANIA I WSPÓŁPRACA:

DZIAŁANIA EDUKACYJNE I BUDOWANIE ŚWIADOMOŚCI:

Tabela 36. DZIAŁANIA EDUKACYJNE I BUDOWANIE ŚWIADOMOŚCI

Nazwa działania/kampanii	Grupa docelowa	Liczba odbiorców
Przekazywanie do OUK sektora energii Zanonimizowanych raportów sytuacyjnych	OUK sektora energii	71
Budowanie świadomości dot. Obowiązków sektora energii w NIS 2 – prelekcja podczas X Konferencja Warsztatowej - Niezawodność i Cyberbezpieczeństwo Infrastruktury Krytycznej i Przemysłowej - IT/OT	OUK sektora energii	50
Wsparcie powstania i działalności Centrum Szkoleniowego Instytutu Energetyki-PIB w obszarze cyberbezpieczeństwa i odporności cyfrowej	OUK sektora energii, kadra zarządzająca i zespoły techniczne	Brak danych – szkolenia prowadzone przez IEN-PIB

ĆWICZENIA I WSPÓŁPRACA MIĘDZYNARODOWA:

Tabela 37. ĆWICZENIA I WSPÓŁPRACA MIĘDZYNARODOWA

Nazwa ćwiczenia / Inicjatywy współpracy	Data	Rola CSIRT Organizator / Uczestnik	Zasięg	scenariusz / Cel współpracy
Udział w spotkaniu Workshop on Procurement Recommendation on Substation Automation	06.2025	OW jako Uczestnik	Międzynarodowy	Celem inicjatywy było wsparcie procesu konsultacji i opiniowania dokumentów dotyczących rekomendacji zakupowych w zakresie systemów automatyzacji stacji elektroenergetycznych w ramach Network Code on Cybersecurity (NCCS). Działania te miały na celu umożliwienie właściwym organom i interesariuszom zapoznania się z proponowanymi wymaganiami, w tym profilem cyberbezpieczeństwa dla urządzeń wykorzystywanych w stacjach elektroenergetycznych, oraz zgłoszenie uwag przed upływem przedłużonego terminu. Inicjatywa służyła wzmocnieniu spójnego podejścia do cyberbezpieczeństwa w procesach zakupowych infrastruktury elektroenergetycznej.
Udział w spotkaniu Third ad-hoc workshop for Competent Authorities	11.2025	OW jako Uczestnik	Międzynarodowy	Celem spotkania było omówienie pytań i uwag zgłoszonych przez właściwe organy do metodologii oceny ryzyka przedłożonych przez ENTSO-E oraz EU DSO Entity zgodnie z art. 8 ust. 5 Network Code on Cybersecurity. Spotkanie miało na celu wyjaśnienie wątpliwości, dążenie do ich rozstrzygnięcia oraz zbliżenie stanowisk w celu umożliwienia podjęcia decyzji przez właściwe organy.
Udział w posiedzeniu NIS COOPERATION GROUP - WORK STREAM ON ENERGY	10.2025	OW jako Uczestnik	Międzynarodowy	Celem spotkania było omówienie stanu wdrażania dyrektywy NIS2 w sektorze energii oraz wymiana doświadczeń pomiędzy państwami członkowskimi w zakresie nadzoru i reagowania na cyber zagrożenia Istotnym elementem dyskusji były również postępy we wdrażaniu Network Code on Cybersecurity (NCCS) oraz identyfikacja aktualnych i przyszłych wyzwań cyberbezpieczeństwa w sektorze energii. Spotkanie służyło wzmocnieniu koordynacji działań i spójnego podejścia regulacyjnego na poziomie UE.
8. Forum Cyberbezpieczeństwa sektora Energii (8th E.DSO/EE-ISAC/ENCS/ENISA Cybersecurity Forum -"Securing the Grid: Cyber Threats,	10.2025	OW jako uczestnik	Międzynarodowy	Celem wydarzenia było stworzenie platformy do współpracy i wymiany wiedzy pomiędzy ekspertami z sektorów energetyki, cyberbezpieczeństwa i technologii w celu przyspieszenia wdrażania nowych regulacji dotyczących cyberbezpieczeństwa w Europie. Miało ono również na celu wzmocnienie współpracy między podmiotami publicznymi i prywatnymi oraz wypracowanie wspólnych działań

Challenges and Actions in a Connected World")				zwiększających odporność europejskiej sieci energetycznej.
Ćwiczenia KSC-EXE 2025	11.2025	OW jako uczestnik	Krajowy	Ćwiczenia KSC-EXE 2025 miały na celu praktyczne sprawdzenie funkcjonowania KSC w warunkach symulowanego kryzysu cyberbezpieczeństwa, ze szczególnym uwzględnieniem współpracy i koordynacji działań pomiędzy podmiotami systemu. Scenariusze ćwiczeń pozwoliły na weryfikację obowiązujących procedur, kanałów komunikacji oraz zdolności decyzyjnych organów właściwych i zespołów CSIRT. Ćwiczenia stanowiły istotny element oceny gotowości KSC oraz przygotowania systemu do nowych wyzwań i wymagań regulacyjnych, w tym wynikających z dyrektywy NIS2.

ANALIZA I OCENA FUNKCJONOWANIA KSC:

W 2025 r. KSC funkcjonował jako ugruntowany mechanizm współpracy pomiędzy podmiotami odpowiedzialnymi za bezpieczeństwo cyberprzestrzeni, umożliwiający koordynację działań oraz reagowanie na zagrożenia i incydenty. System zapewniał podstawowe ramy organizacyjne pozwalające na współdziałanie organów administracji, CSIRT poziomu krajowego oraz podmiotów objętych regulacjami (OUK).

Na przestrzeni kolejnych lat funkcjonowania KSC widoczny był wzrost jego dojrzałości organizacyjnej, przejawiający się lepszym zrozumieniem ról i odpowiedzialności uczestników systemu, usprawnieniem komunikacji oraz większą przewidywalnością procesów związanych z obsługą incydentów. Pozytywnie należy ocenić współpracę z zespołami CSIRT poziomu krajowego, która umożliwiała bieżące konsultowanie zdarzeń oraz zachowanie spójności reakcji na incydenty.

Istotną rolę w funkcjonowaniu KSC odgrywały działania koordynacyjne podejmowane przez Ministerstwo Cyfryzacji, w szczególności organizacja spotkań roboczych, forów dla organów właściwych oraz tworzenie przestrzeni do wymiany doświadczeń i zgłaszania potrzeb. Ministerstwo Cyfryzacji aktywnie wspierało również postulaty dotyczące zwiększenia finansowania zadań realizowanych w ramach KSC, w tym w zakresie zasobów kadrowych organów właściwych. Pomimo tych działań, ostateczne rozstrzygnięcia budżetowe nie pozwoliły na zapewnienie środków adekwatnych do skali i złożoności realizowanych zadań.

Z perspektywy organu właściwego kluczowym i krytycznym ograniczeniem funkcjonowania KSC pozostawał niedostateczny poziom finansowania zasobów osobowych. Zapewnione środki nie pozwalały na zatrudnienie liczby pracowników adekwatnej do zakresu obowiązków ustawowych ani na skuteczne konkurowanie o specjalistów z obszaru cyberbezpieczeństwa. W konsekwencji organy właściwe funkcjonowały przy trwałym przeciążeniu kadrowym, co ograniczało możliwość prowadzenia aktywnego, systematycznego nadzoru nad dużą liczbą podmiotów oraz realizacji działań analitycznych i rozwojowych. Nawet przy wysokim poziomie zaangażowania zespołów dostępne zasoby ludzkie nie pozwalały na pełne wykonywanie wszystkich zadań w wymaganym zakresie.

Podsumowując, KSC w 2025 r. spełniał swoją rolę w zakresie koordynacji i reagowania, jednak jego dalsza skuteczność i stabilność są w istotnym stopniu uzależnione od zapewnienia realnego wzmocnienia finansowania, w szczególności w obszarze zasobów kadrowych organów właściwych.

PROGNOZY I PRZEWIDYWANIA DLA KSC NA ROK 2026:

W 2026 r. należy spodziewać się dalszego wzrostu znaczenia KSC w związku z rozszerzeniem zakresu regulacyjnego, objęciem systemem nowych podmiotów oraz pojawieniem się nowych organów właściwych. Wyzwanie stanowić będzie wdrożenie nowego podejścia do identyfikacji podmiotów kluczowych i ważnych, w tym stosowanie tzw. size-cap rule, opartego na samoidentyfikacji

i samorejestracji podmiotów, co może generować trudności interpretacyjne i wymagać skoordynowanych działań informacyjnych prowadzonych przez Ministerstwo Cyfryzacji we współpracy z innymi organami właściwymi.

Przewidywany jest istotny wzrost liczby zapytań ze strony nowo objętych podmiotów dotyczących realizacji obowiązków wynikających z KSC, a także konieczność rozpoczęcia i rozwijania współpracy z nowo powstającymi sektorowymi zespołami CSIRT. Dodatkowym wyzwaniem będzie objęcie części podmiotów nadzorem więcej niż jednego organu właściwego, co wskazuje na potrzebę wypracowania wspólnych metodyk nadzoru i mechanizmów koordynacji.

Jednocześnie należy oczekiwać dalszego narastania liczby obowiązków po stronie organów właściwych. Przy utrzymujących się niedostatecznych zasobach osobowych oraz ograniczonych środkach finansowych na etaty konieczna będzie stała priorytetyzacja zadań, co może ograniczać możliwość prowadzenia aktywnego i systematycznego nadzoru w ramach KSC.

PLANY NA ROK 2026:

W 2026 r., przy założeniu wejścia w życie nowelizacji UKSC, organ właściwy ds. cyberbezpieczeństwa planuje skoncentrować działania na wdrażaniu nowych przepisów oraz realizacji rozszerzonych zadań ustawowych. Kluczowym zadaniem będzie identyfikacja podmiotów kluczowych i ważnych oraz realizacja dalszych zadań nadzorczych wobec podmiotów objętych regulacjami, w tym analiza wyników audytów bezpieczeństwa podmiotów, które wcześniej posiadały status operatorów usług kluczowych.

Planowane są również działania nadzorcze obejmujące kontrole oraz stosowanie środków przewidzianych w ustawie, w tym nakładanie administracyjnych kar pieniężnych na OUK w przypadku niewywiązywania się z obowiązków, do których te podmioty obliguje ustawa. Istotnym elementem działań będzie rozpoczęcie realizacji zadań organu właściwego w zakresie Network Code on Cybersecurity (NCCS), w związku z objęciem nowej roli w tym zakresie.

Równolegle zakłada się podjęcie działań związanych z powołaniem i współpracą z sektorowym zespołem CSIRT. Ze względu na krytycznie ograniczone zasoby osobowe oraz niewystarczające środki finansowe na etaty, realizacja wszystkich zadań ustawowych w 2026 r. nie będzie możliwa jednocześnie, co wymagać będzie ścisłej priorytetyzacji działań i koncentracji na obszarach o najwyższym znaczeniu z punktu widzenia bezpieczeństwa.

REKOMENDACJE NA 2026 - REKOMENDACJE DLA PEŁNOMOCNIKA RZĄDU DS. CYBERBEZPIECZEŃSTWA:

Zasadne wydaje się rozważenie w 2026 r. działań legislacyjnych dotyczących mechanizmów finansowania zadań organów właściwych ds. cyberbezpieczeństwa. Obowiązujące limity wydatków, określone w UKSC oraz jej nowelizacji, w perspektywie będą niewystarczające wobec systematycznie rosnącego zakresu zadań, obejmujących m.in. identyfikację i nadzór nad podmiotami kluczowymi i ważnymi, analizę sprawozdań z audytów, kontrole oraz działania egzekucyjne. Poziom finansowania bezpośrednio wpływa również na możliwości pozyskiwania i utrzymania wyspecjalizowanej kadry eksperckiej. Utrzymanie obecnych limitów może prowadzić do ograniczenia zdolności operacyjnych organów właściwych oraz ryzyka zakłóceń w funkcjonowaniu KSC, w szczególności w sektorze energii. Rekomenduje się dostosowanie limitów wydatków do rzeczywistych potrzeb wynikających z obowiązków ustawowych;

Analiza możliwości implementacji sztucznej inteligencji w systemie S46, który w sposób automatyczny analizowałby sprawozdania z audytów podmiotów ważnych i kluczowych i wskazywał na których spółkach należy skupić zadania nadzorcze. Ręczna weryfikacja tysięcy audytów cyberbezpieczeństwa, przy obecnych zasobach osobowych (oraz wielu innych zadaniach OW) wydaje się niemożliwa;

Zasadne jest wzmocnienie roli koordynacyjnej na poziomie krajowym w kontekście wdrażania nowelizacji UKSC oraz regulacji sektorowych. Rekomenduje się inicjowanie i utrzymywanie platform dialogu pomiędzy organami właściwymi, umożliwiających wymianę doświadczeń, identyfikację wspólnych problemów interpretacyjnych oraz zapewnienie spójności podejścia do realizacji zadań w ramach KSC. Działania te mogłyby przyczynić się do ograniczenia ryzyka rozbieżności w stosowaniu przepisów oraz zwiększenia efektywności funkcjonowania KSC.

MINISTER OBRONY NARODOWEJ JAKO ORGANU WŁAŚCIWEGO DO SPRAW CYBERBEZPIECZEŃSTWA (SEKTOR OCHRONY ZDROWIA OBEJMUJĄCY PODMIOTY PODLEGŁE MINISTROWI OBRONY NARODOWEJ LUB PRZEZ NIEGO NADZOROWANE).

Ministerstwo Obrony Narodowej

PODSUMOWANIE ROCZNE:

Kluczowa pozycja geopolityczna Polski jako państwa frontowego NATO na wschodniej flance oraz głównego węzła logistycznego wspierającego Ukrainę w wojnie z Rosją, uczyniło ją jednym z priorytetowych celów adwersarzy i zdeterminowało sytuację w cyberprzestrzeni resortu obrony narodowej (RON). W 2025 r., podobnie jak w latach ubiegłych, znaczący wpływ na stan bezpieczeństwa systemów IT RON miały zagrożenia związane z adwersarzami typu APT. Aktywność ta kojarzona jest głównie z działalnością sponsorowaną lub pozostającą w strukturach państwa. Są to zaawansowane, długotrwałe ataki, których celem jest zapewnienie atakującym skrytej oraz możliwie najdłuższej obecności w środowisku ofiary. Spektrum działań zagrożeń typu APT obejmuje różnorodne czynności – od systematycznie realizowanego rozpoznania infrastruktury teleinformatycznej, poprzez cyberszpiegostwo, zakłócanie działania, aż po działania destrukcyjne. Od momentu rozpoczęcia pełnoskalowej inwazji Rosji na Ukrainę obserwowany jest dynamiczny wzrost aktywności prorosyjskich grup haktywistycznych.

W odniesieniu do OUK - 6 szpitali wojskowych, w 2025 r. nie zarejestrowano incydentów poważnych. Mając jednak na uwadze ogólną sytuację w cyberprzestrzeni RON, przeprowadzono weryfikację realizacji przez OUK wymagań wynikających z przepisów UKSC i rozporządzeń wykonawczych do niej, na podstawie, której przygotowano rekomendacje działań korekcyjnych i naprawczych. Kontynuowano cykliczne skanowanie OUK w obszarze zarządzania zewnętrzną powierzchnią ataków (EASM), na podstawie których OUK dokonywały weryfikacji swoich zasobów wystawionych do Internetu. Na potrzeby kadr OUK oraz innych jednostek RON zorganizowano Zimową i Letnią Szkołę Cyberbezpieczeństwa, której głównym celem było podniesienie świadomości i wiedzy uczestników dot. aktualnych cyberzagrożeń, wymagań prawnych w obszarze cyberbezpieczeństwa oraz praktycznych aspektów zarządzania cyberbezpieczeństwem.

DZIAŁANIA STRATEGICZNE:

Projekt A: Koncepcja konsolidacji polskiej społeczności „cyber" wokół SZ RP oraz Wojsk Obrony Cyberprzestrzeni – Cyber LEGION

Celem projektu jest podniesienie potencjału obronnego państwa w domenie operacyjnej cyberprzestrzeni poprzez budowanie rezerw osobowych wykwalifikowanych specjalistów oraz umożliwienie rozwoju osobistego poprzez uczestnictwo w zaawansowanych technicznie inicjatywach.

Kluczowym elementem Programu jest utworzenie w WOC Kompanii Uzupełnienia Kadrowego celem uzupełnienia struktur etatowych WOC czasu „W". Zakłada się pozyskanie co najmniej 400 żołnierzy aktywnej lub pasywnej rezerwy o ugruntowanej wiedzy specjalistycznej lub znaczącym potencjale

rozwojowym w dziedzinie cyberbezpieczeństwa. W 2025 r. chęć przystąpienia do Programu zgłosiło niemal 2500 osób.

Projekt B: System certyfikacji osób w obszarze cyberbezpieczeństwa

W 2023 r. Eksperckie Centrum Szkolenia Cyberbezpieczeństwa (ECSC) uzyskano akredytację Polskiego Centrum Akredytacji i uruchomiło pierwszy programu certyfikacji pn. Specjalista ds. Cyberbezpieczeństwa. W 2024 r. rozszerzono zakres certyfikacji o drugi program pn. Analityk ds. Cyberbezpieczeństwa, a w 2025 utrzymano uzyskaną akredytację i rozszerzono zakres certyfikacji o kolejne 4 programy tj.: Audytor, Ekspert, Architekt i Menadżer ds. cyberbezpieczeństwa.
Model zarządzania kompetencjami kadr odpowiedzialnych za realizację zadań w obszarze cyberbezpieczeństwa został przygotowany w oparciu o Standard NIST 800-181 (NICE Framework). Certyfikacja przeznaczona jest dla osób, które w sposób bezpośredni lub pośredni realizują zadania na rzecz podnoszenia poziomu cyberbezpieczeństwa, w tym kadr podmiotów KSC.

Projekt C: Budowa zdolności do organizacji ćwiczeń i warsztatów w obszarze cyberbezpieczeństwa realizowanych w oparciu o nowoczesny cyberpoligon w formacie krajowym i międzynarodowym

Projekt obejmuje pozyskanie przez ECSC nowej platformy cyberpoligonu, która będzie wykorzystana do prowadzenia ćwiczeń, warsztatów i szkoleń w zakresie działań w cyberprzestrzeni na potrzeby SZ RP, jednostek RON oraz podmiotów KSC. Cyberpoligon jest platformą, która poprzez zamodelowanie i symulację wybranego fragmentu cyberprzestrzeni umożliwia realizację określonych scenariuszy obejmujących zaawansowane formy działań defensywnych i ofensywnych. Celem projektu jest poprawa efektywności procesów kształcenia i podnoszenia kwalifikacji oraz przygotowanie zasobów osobowych dla potrzeb realizacji zadań w obszarze cyberbezpieczeństwa.

Jednocześnie na terenie WAT jest budowane Centrum Innowacji i Cyberbezpieczeństwa, które ma zapewnić i infrastrukturę na potrzeby m.in. realizacji szkoleń z wykorzystaniem cyberpoligonu.

DZIAŁANIA I WSPÓŁPRACA:

DZIAŁANIA EDUKACYJNE I BUDOWANIE ŚWIADOMOŚCI:

Tabela 38. DZIAŁANIA EDUKACYJNE I BUDOWANIE ŚWIADOMOŚCI MON

LP	Nazwa działania/kampanii	Grupa docelowa	Liczba odbiorców
1	Projekt Akademia_CYBER.MIL edycja III (rok akademicki 2024/2025)	Studenci kierunków technicznych cywilnych szkół wyższych (politechnik i uczelni technicznych)	8115
2	Międzynarodowy Kongres Cyberbezpieczeństwa IN.SE.CON	Eksperci z zakresu cyberbezpieczeństwa w podmiotach administracji publicznej i służbach mundurowych, przedstawiciele nauki oraz sektora prywatnego, w tym kluczowych firm technologicznych	2000
3	Konkurs Ministra Obrony Narodowej im. Mariana Rejewskiego na najlepszą pracę inżynierską, licencjacką i rozprawę doktorską, poświęconą cyberbezpieczeństwu i kryptologii	Młodzi naukowcy, studenci i absolwenci uczelni wyższych, doktoranci	55
4	Konferencja Sharing Cyber w Berlinie	Przedstawicieli polskich oraz niemieckich sił zbrojnych, administracji publicznej, środowiska naukowego i sektora prywatnego	80
5	Szkolenia i warsztaty dot. cyberbepzieczeństwa, w tym z cyberhigieny	Żołnierze i pracownicy RON	ok. 11000
6	#wGotowości – cykl cyberhigiena	Obywatele RP	393
7	Konferencja CyberEXPERT	Żołnierze, personel RON, przedstawiciele świata nauki, przemysłu, wendorzy	246
8	Legia akademicka (w specjalności 29B)	Studenci/podoficerowie	12
9	Szkolenia dla Ministerstwa Cyfryzacji	Pracownicy administracji państwowej	20
10	Szkolenie z podstaw cyberbezpieczeństwa dla ZSZ	Zespół Szkół Zawodowych w Górze Kalwarii	64

11	Szkolenie “Zanim klikniesz - zagrożenia w cyberprzestrzeni i bezpieczeństwo przetwarzania danych”	Ogólnopolskie Forum Szkół „Edukacja Obronna Młodzieży”	112
12	CI Awareness Seminar for Defence Attaches “Cyber Security in Daily Use”	Counter Intelligence Centre of Excellence	45
13	Projekt CYBER.MIL z klasą	Uczniowie klas I-III szkół średnich	765

ĆWICZENIA I WSPÓŁPRACA MIĘDZYNARODOWA:

Tabela 39. DZIAŁANIA EDUKACYJNE I BUDOWANIE ŚWIADOMOŚCI MON

LP	Nazwa ćwiczenia	Data	Rola CSIRT	Zasięg	opis scenariusza / Cel współpracy
1	Ćwiczenia Cyber Fortress (Belval, Luksemburg)	03.2025	Uczestnikiem był CSIRT MON/DKWOC w ramach współpracy Permanent Structured Cooperation in Security and Defence Policy (PESCO) „Cyber Rapid Response Teams and Mutual Assistance in Cyber Security”	międzynar.	Ćwiczenie przygotowawcze do LockedShields, oparte na rywalizacji między zespołami.
2	Ćwiczenia CyberNet (Haga, Królestwo Niderlandów)	10.2025	Uczestnikiem był CSIRT MON/DKWOC w ramach współpracy Permanent Structured Cooperation in Security and Defence Policy (PESCO) „Cyber Rapid Response Teams and Mutual Assistance in Cyber Security”	międzynar.	Ćwiczenia oparte na rywalizacji między zespołami, testujące zespoły w zakresie zaawansowanej cyberobrony, reagowania na incydenty oraz ataków/obrony sieci w złożonych scenariuszach.
3	Ćwiczenia MICNET	10.2025	Uczestnikiem był CSIRT MON/DKWOC	międzynar.	Ćwiczenia oparte na rywalizacji między zespołami, mające na celu umożliwienie szybkiej i bezpiecznej wymiany informacji dotyczących cyberzagrożeń, incydentów oraz najlepszych praktyk pomiędzy wojskowymi centrami cyberobrony w krajach UE.
4	NATO LOCKED SHIELDS 2025	05.2025	Uczestnikiem był CSIRT MON/DKWOC	międzynar.	Ćwiczenia oparte na rywalizacji między zespołami, umożliwiające ekspertom ds. cyberbezpieczeństwa doskonalenie umiejętności w zakresie obrony krajowych systemów informatycznych i infrastruktury krytycznej przed atakami w czasie rzeczywistym.
5	APEX 25	09.2025	Uczestnikiem był CSIRT MON/DKWOC	międzynar.	Ćwiczenia oparte na rywalizacji między zespołami, podczas których realizowano scenariusz obejmujący symulację wielonarodowej wojny w cyberprzestrzeni. Ćwiczenie miało na celu rozwijać umiejętności utwardzania systemów, wykrywania, analizowania oraz skutecznego reagowania na szkodliwą aktywność adwersarza, a także ocenę zdolności do identyfikacji i zapobiegania zagrożeniom.
6	EU Cyber Commaders & Cyber Ambassadors Conference	24-26.03	Organizatorem był DKWOC	międzynar.	Omawiano istotne kwestie cyberbezpieczeństwa dla państw członkowskich oraz samej UE
7	NATO Cyber Defence Pledge Conference	20-21.05	Organizatorem był DKWOC	międzynar.	Celem konferencji była ocena i koordynacja wspólnych działań w obszarze obrony w cyberprzestrzeni, w tym w zakresie ochrony infrastruktury krytycznej.
8	Cyber Flag	07.2025	Uczestnikiem był CSIRT MON/DKWOC	międzynar.	Ćwiczenia organizowane przez USCYBERCOM, oparte na rywalizacji między zespołami, w zakresie cyberbezpieczeństwa. Ich celem jest wzmocnienie partnerstw i poprawa

					zdolności państw uczestniczących do wykrywania, reagowania i obrony przed szkodliwą aktywnością w cyberprzestrzeni.
9	Cyber Coalition	28.11-4.12.	Uczestnikiem był CSIRT MON/DKWOC	międzynar.	Scenariusz zakłada symulowane incydenty i ataki w cyberprzestrzeni, podczas których państwa sojusznicze ćwiczą wspólnie reagowanie, wymianę informacji i koordynację działań pod egidą NATO.
10	CWIX	2 – 20.06	Uczestnikiem był CSIRT MON/DKWOC	międzynar.	Celem było sprawdzenie i usprawnienie współdziałania systemów dowodzenia, łączności i IT państw sojuszniczych, poprzez realne testy techniczne prowadzone zgodnie ze standardami NATO.
11	Brave Beduin 2025	05.2025	Uczestnikiem był DKWOC	międzynar.	Celem ćwiczenia było doskonalenie funkcjonowania ogniw analitycznych oraz systemu alarmowania i ostrzegania o skażeniach na poszczególnych szczeblach dowodzenia połączonych sił NATO.
12	APOLLO PHOENIX	10.2025	Uczestnikiem był DKWOC	międzynar.	Symulowane działania operacyjne, w których międzynarodowe zespoły testowały planowanie, podejmowanie decyzji i współdziałanie sił sojuszniczych w środowisku kryzysowym zgodnie z procedurami NATO.
13	CSIRT Summit 2025 & CSIRT Workshop	5-6.03	Organizatorem był CSIRT MON/DKWOC	międzynar.	Konferencja poświęcona wymianie doświadczeń zespołów CSIRT związanych z analizą i reagowaniem na incydenty komputerowe.
14	Podpisane porozumienia o współpracy w zakresie cyberbezpieczeństwa z Czechami, Norwegią, Rumunią	03.2025 10.2025 12.2025	DKWOC	międzynar.	Umowa zakłada współprace w zakresie wymiany informacji o zagrożeniach, wspólnych szkoleń i ćwiczeń oraz wzmocnienia zdolności obronnych w cyberprzestrzeni
15	CrossedSwords	11.2025	Uczestnikiem był CSIRT MON/DKWOC	międzynar.	Ćwiczenia koordynujące zespoły Cyber z wojskami kinetycznymi, którego celem jest doskonalenie umiejętności z dowództw wojskowych szczebla operacyjnego w zakresie zarządzania ofensywnymi i defensywnymi zdolnościami w cyberprzestrzeni, jak i specjalistów do spraw cyberbezpieczeństwa szczebla taktycznego w zakresie realizacji defensywnych i ofensywnych operacji cybernetycznych w symulowanym środowisku kryzysowym i konfliktowym.
16	Udział w posiedzeniu dyrektorów ds. bezpieczeństwa informacji resortów obrony państwa Grupy Wyszehradzkiej (V4) w Słowacji	11.2025	Uczestnikiem był MON, bez udziału CSIRT	międzynar.	Celem było umacnianie współpracy w zakresie bezpieczeństwa informacji, koordynacji wspólnych stanowisk na forach UE I NATO oraz wymiana doświadczeń I dobrych praktyk.
17	Udział w strategicznym dialogu obronnym z Niemcami – koordynacja obszaru cyberbezpieczeń	09.2025	Uczestnikiem był MON, bez udziału CSIRT	międzynar.	Celem było umacnianie współpracy polsko-niemieckiej w zakresie polityki obronnej, w tym cyberbepzieczeństwa I technologii informacyjnych.

	stwa w ramach dialogu.				
18	Cyber Range – Cybersecurity in Practice oraz Pentester Tools	03.2025 10.2025	Organizatorem było ECSC, uczestnik – CSIRT MON/DKWOC	międzynar. (NATO, UE)	Szkolenia techniczne przygotowane na platformie CyberRange z zaawansowanym scenariuszem realizowanym indywidualnie przez każdego kursanta.
19	CyberEXPERT Game	10.2025	Organizatorem było ECSC, uczestnik – CSIRT MON/DKWOC	międzynar. (NATO)	Warsztaty cyberbezpieczeństwa w formie współzawodnictwa.
20	Szkolenia dla SZ Ukrainy	03.2025 11.2025 12.2025	Organizatorem było ECSC	Przedstawiciele Sił Zbrojnych Ukrainy	Szkolenia dedykowane SZ Ukrainy.
21	Ćwiczenia KSE-EXE	11.2025 r.	Uczestnikiem był MON i CSIRT MON.	Krajowy	Ocena gotowości podmiotów krajowego systemu cyberbezpieczeństwa do skutecznej współpracy i wymiany informacji oraz weryfikacja procedur reagowania na incydenty w warunkach symulowanego kryzysu spowodowanego cyberatakiem.
22	Ćwiczenia Cyber Shield, Cyber Baltic, Cyber Autumn	06.2025, 08.2025, 11.2025	Uczestnikiem był DWOT	międzynar.	Ćwiczenie o charakterze Blue/Red Team.

ANALIZA I OCENA FUNKCJONOWANIA KSC:

Pozytywny aspekt funkcjonowania KSC stanowią istniejące mechanizmy współpracy podmiotów KSC, w tym nieformalne jak PCOC i FOW. Umożliwiają one wymianę wiedzy i doświadczeń, wypracowywanie wspólnych rozwiązań oraz usprawniają przepływ informacji, co pozytywnie wpływa na efektywność i skuteczność działań w ramach KSC.

Potrzebne i warte kontynuacji są również inicjatywy dot. ćwiczeń, które pozwalają podmiotom KSC na weryfikację skuteczności istniejących procedur reagowania na incydenty i sytuacje kryzysowe w cyberprzestrzeni, umożliwiają usprawnienie koordynacji działań i wymiany informacji.

Cenne i warte kontynuacji są inicjatywy budujące świadomość, wiedzę i kompetencje w obszarze cyberbezpieczeństwa, zarówno kadr KSC jak i całego społeczeństwa.

Brakuje natomiast spójnych wymagań w zakresie kompetencji personelu odpowiedzialnego za realizację zadań w zakresie cyberbezpieczeństwa w sektorze publicznym (standaryzacji kompetencji zasobów ludzkich). Problem stanowi brak wyznaczenia podmiotu odpowiedzialnego za przygotowanie i realizację stosownych szkoleń dostosowanych do określonych ról w systemie cyberbezpieczeństwa (np. zarządczych, technicznych, operacyjnych, analitycznych, audytowych) jak i ograniczony dostęp do specjalistycznych szkoleń dla pracowników podmiotów publicznych (np. brak specjalistycznych szkoleń centralnych w ramach służby cywilnej, wysoki koszty szkoleń komercyjnych).

W obliczu rosnących zagrożeń w cyberprzestrzeni konieczne jest: opracowanie ram prawnych regulujących działania ofensywne w cyberprzestrzeni, które będą zgodne z międzynarodowymi standardami i konwencjami, określenie jasnych zasad i procedur działań o charakterze ofensywnym w cyberprzestrzeni w warunkach pokoju, kryzysu i wojny, a także określenie jakie podmioty/instytucje w jakich warunkach mogą takie działania prowadzić.

PROGNOZY I PRZEWIDYWANIA DLA KSC NA ROK 2026:

Aktywność adwersarzy w polskiej cyberprzestrzeni pozostanie na wysokim poziomie intensywności, co w znaczącym stopniu determinowane jest trwającą wojną w Ukrainie oraz aktywną postawą Polski w zakresie wsparcia i donacji na rzecz Ukrainy. Przewiduje się, że dalej będzie rosnąć liczba ataków na podmioty administracji publicznej i infrastrukturę krytyczną skalkulowanych na testowanie odporności cybernetycznej państwa. Celami ataków będą również podmioty w ramach łańcucha dostaw celem

uzyskania danych i dostępu do istotnych danych z punktu widzenia bezpieczeństwa Polski. Aktywność w cyberprzestrzeni może być również skierowana przeciwko mniejszym organizacjom, których poziom zabezpieczeń jest dużo niższy.

Wejście w życie nowelizacji UKSC może znacząco wpłynąć na wzmocnienie cyberbezpieczeństwa RP, przy czym istotne będzie zapewnienie podmiotom kluczowym i ważnym wsparcia we wdrażaniu nowych wymagań oraz wypracowanie odpowiednich mechanizmów współpracy pomiędzy poszczególnymi podmiotami KSC.

Znaczący wzrost liczby podmiotów KSC spowoduje wzrost popytu na specjalistów ds. cyberbezpieczeństwa, co może skutkować większą rotację pracowników i problemami z zapewnieniem zasobów kadrowych niezbędnych do realizacji zadań w obszarze cyberbezpieczeństwa. Ważne w związku z tym będzie wsparcie w uzupełnieniu kompetencji pracowników lub przekwalifikowaniu oraz dostęp do narzędzi wspierających realizację zadań, a w przypadku podmiotów administracji publicznej - także utrzymanie świadczeń teleinformatycznych.

PLANY NA ROK 2026:

- Dostosowanie systemu cyberbezpieczeństwa RON do wymagań nowelizacji UKSC;
- Kontynuacja działań w zakresie organizacji konferencji, szkoleń i warsztatów z zakresu cyberbezpieczeństwa dla jednostek RON, podmiotów współpracujących z RON i innych podmiotów KSC;
- Rozwój i zwiększenie zdolności szkoleniowych ECSC oraz kontynuacja prac związanych z certyfikacją osób w obszarze cyberbezpieczeństwa;
- Dalsza realizacja projektu Akademia CYBER.MIL i warsztatów CyberMil z klasą;
- Kontynuacja Programu Cyber LEGION;
- Wdrożenie polityki bezpieczeństwa RON dotyczącej przeciwdziałania cyberzagrożeniom w łańcuchu dostaw na rzecz SZ RP;
- Podniesienie poziomu cyberbezpieczeństwa OUK m.in. poprzez opracowanie wytycznych dot. wdrożenia wymagań wynikających z nowelizacji UKSC i organizację dedykowanych szkoleń dla kadr OUK;
- Implementacja rozwiązań sztucznej inteligencji do celów zapewniania cyberbezpieczeństwa (realizowane w ramach programu SAFE).

REKOMENDACJE NA 2026 - REKOMENDACJE DLA PEŁNOMOCNIKA RZĄDU DS. CYBERBEZPIECZEŃSTWA:

- Utworzenie na szczeblu krajowym instytucji właściwej w zakresie budowy kapitału eksperckiego i zarządzania kompetencjami cyfrowymi Państwa poprzez organizację specjalistycznych szkoleń w obszarze cyberbezpieczeństwa, kryptografii oraz IT adresowanych do odbiorców z sektora administracji rządowej i samorządowej, podmiotów kluczowych i ważnych, operatorów infrastruktury krytycznej;
- Wzmacnianie i sprawdzanie efektywności zespołów cyberbezpieczeństwa oraz zgrywanie ich działania poprzez organizację specjalistycznych ćwiczeń i warsztatów cyberbezpieczeństwa, w tym z wykorzystaniem nowoczesnych platform typu CyberRange i zaawansowanych scenariuszy adresujących współczesne wyzwania i zagrożenia w domenie cyberbezpieczeństwa;
- Wzmocnienie działań w obszarze współpracy międzynarodowej, zarówno cywilnej jak i wojskowej z docelowym zamiarem osiągnięcia przez Polskę roli lidera w dziedzinie cyberbezpieczeństwa w obszarze Europy środkowo-wschodniej;
- Szersze wsparcie podmiotów KSC w zakresie realizacji wymagań formalnych (wytyczne dot. sposobu realizacji zadań, centra kompetencyjne, platformy wymiany wiedzy i doświadczeń) oraz dostęp do narzędzi wspierających realizację zadań w obszarze cyberbezpieczeństwa.

KOMISJA NADZORU FINANSOWEGO - SEKTOR BANKOWY I INFRASTRUKTURY RYNKÓW FINANSOWYCH (KNF)

PODSUMOWANIE ROCZNE:

Środki techniczne i organizacyjne mające na celu ochronę cyberprzestrzeni przed zagrożeniami wyznaczone są w głównej mierze dla podmiotów finansowych nadzorowanych przez KNF (w tym wszystkich operatorów usług kluczowych, dla których KNF jest organem właściwym) przez przepisy rozporządzenia DORA, którego celem jest zwiększenie operacyjnej odporności cyfrowej podmiotów finansowych oraz uregulowanie świadczenia usług ICT na rzecz podmiotów finansowych. Rozporządzenie to jest stosowane od 17.01.2025 r., z czym związana jest istotna zmiana procesu sprawozdawczego oraz komunikacja, a także wymiana informacji pomiędzy podmiotami finansowymi, organami krajowymi i organami unijnymi. Zautomatyzowane pozyskiwanie, rejestrowanie, przetwarzanie i analizowanie nowego zakresu danych, które nie były dotychczas wymagane od podmiotów finansowych, uwzględniając znaczne zwiększenie skali pozyskiwanych danych i informacji w stosunku do stanu dotychczasowego, jest związane z wdrażaniem nowych systemów i narzędzi IT w Urzędzie KNF. Działania te stanowią bezpośrednią realizację zaplanowanych na ten rok nowych obowiązków wynikających z regulacji DORA oraz intensyfikacji działań na rzecz wzmacniania cyberodporności sektora finansowego. Dla osiągnięcia tym celów znaczenie ma też wyznaczenie w trybie decyzji administracyjnych pierwszych 10 podmiotów finansowych (będących OUK) obowiązanych do przeprowadzenia testów, o których mowa w art. 26 ust. 1 rozporządzenia DORA (TLPT).

Natomiast monitorowanie przepisów UKSC związane było w 2025 r. głównie z weryfikacją podmiotów będących OUK, monitorowaniem realizacji zaleceń pokontrolnych oraz wydaniem decyzji administracyjnych dotyczących nałożenia kar związanych ze stwierdzanymi naruszeniami UKSC.

DZIAŁANIA STRATEGICZNE:

SYSTEMATYCZNE CZYNNOŚCI ANALITYCZNE OBEJMUJĄCE BIEŻĄCĄ WERYFIKACJĘ PODMIOTÓW W SEKTORZE BANKOWYM I INFRASTRUKTURY RYNKÓW FINANSOWYCH.

Analiza ta była ukierunkowana na dwa kluczowe aspekty:

- ocenę spełnienia kryteriów kwalifikujących do uznania za operatora usługi kluczowej, weryfikację utrzymywania warunków kwalifikujących podmiot jako operatora usługi kluczowej (W tym zakresie nie wydano w 2025 żadnej decyzji administracyjnej, w sektorze jest identyfikowanych operatorów usługi kluczowej. U wszystkich z tych podmiotów odbyła się kontrola przestrzegania UKSC);
- Monitorowano realizację zaleceń pokontrolnych z zakresu ustawowych obowiązków operatorów usług kluczowych zgodnie z przekazanymi przez podmioty harmonogramami realizacji zaleceń:
- Wydano decyzje administracyjne dotyczące nałożenia kar przewidzianych przez UKSC.

BIEŻĄCA WSPÓŁPRACA I WYMIANA INFORMACJI Z CSIRT KNF

Zamknięto projekt przygotowujący wdrożenie rozporządzenia DORA i dzięki wprowadzonemu systemowi sprawozdawczemu rozpoczęto realizację działań związanych ze sprawowaniem przez KNF nadzoru w ramach rozporządzenia DORA, co obejmowało w szczególności:

PODEJMOWANIE CZYNNOŚCI W ZAKRESIE NADZORU BIEŻĄCEGO ORAZ ANALITYCZNEGO, W TYM ZWRACANIE SIĘ DO PODMIOTÓW FINANSOWYCH Z WEZWANIAMI DOTYCZĄCYMI UDOSTĘPNIENIA INFORMACJI ORAZ ANALIZOWANIE DANYCH SPRAWOZDAWCZYCH, W ODNIESIENIU DO OBSZARÓW:

- zarządzania ryzykiem związanym z wykorzystaniem technologii informacyjno-komunikacyjnych (ICT),
- zarządzania incydentami związanymi z ICT i ich zgłaszania oraz dobrowolnego informowania o znaczących cyberzagrożeniach,
- zarządzania poważnymi incydentami związanymi z ICT i poważnymi incydentami bezpieczeństwa związanymi z płatnościami i ich zgłaszania przez podmioty finansowe,
- testowania operacyjnej odporności cyfrowej,
- środków na rzecz zarządzania ryzykiem ze strony zewnętrznych dostawców usług ICT,
- wymiany informacji i analiz w związku z cyberzagrożeniami i podatnościami,
- współpracę międzynarodową, w tym z Europejskimi Urzędami Nadzoru poprzez uczestnictwo przedstawicieli UKNF w gremiach nadzorczych związanych z rozporządzeniem DORA, jak Forum Nadzoru (*DORA Oversight Forum*) oraz EBA IT Task Force,
- wykonywanie obowiązków nadzorczych związanych z cykliczną sprawozdawczością wynikającą z rozporządzenia DORA, w szczególności pozyskiwanie od podmiotów finansowych pełnych rejestrów informacji w odniesieniu do wszystkich ustaleń umownych dotyczących korzystania z usług ICT świadczonych przez zewnętrznych dostawców usług ICT,
- podejmowanie działań służących wsparciu podmiotów finansowych w dostosowaniu ich działalności do rozporządzenia DORA, m.in. poprzez udzielanie odpowiedzi w zakresie zagadnień dotyczących rozporządzenia DORA, formułowanych w ramach zapytań kierowanych przez podmioty finansowe na dedykowaną temu skrzynkę poczty e-mail UKNF,
- realizowanie ocen związanych z metodyką BION oraz ankietami „Kluczowych wskaźników ryzyka dla obszaru IT i bezpieczeństwa IT" w kontekście wymagań rozporządzenia DORA,
- prowadzenie działań służących określeniu podmiotów finansowych, od których wymaga się by przeprowadzały testy penetracyjne ukierunkowane przez analizę zagrożeń (TLPT),
- utrzymywanie systemów i narzędzi IT UKNF do komunikacji z podmiotami finansowymi oraz analityki danych, w tym Systemu Sprawozdawczości DORA oraz Systemu do Obsługi Incydentów DORA.

DZIAŁANIA I WSPÓŁPRACA:

DZIAŁANIA EDUKACYJNE I BUDOWANIE ŚWIADOMOŚCI:

Tabela 40. DZIAŁANIA EDUKACYJNE I BUDOWANIE ŚWIADOMOŚCI

Nazwa działania/kampanii	Grupa docelowa
Projekt edukacyjny Centrum Edukacji dla Uczestników Rynku – CEDUR	Rynek finansowy
Projekt edukacyjny Centrum Edukacji dla Uczestników Rynku – CEDUR	Podmioty finansowe objęte Rozporządzeniem DORA

ĆWICZENIA I WSPÓŁPRACA MIĘDZYNARODOWA:

Tabela 41. ĆWICZENIA I WSPÓŁPRACA MIĘDZYNARODOWA

Nazwa ćwiczenia	Data	Rola	Zasięg	opis scenariusza / Cel współpracy
KSC – EXE 2025	11.2025	Uczestnik	Krajowy	ćwiczenia Table Top / Sprawdzenie działania procedur oraz weryfikacja zdolności operacyjnych podmiotów krajowego systemu cyberbezpieczeństwa w sytuacji kryzysowej spowodowanej cyberatakiem.

ANALIZA I OCENA FUNKCJONOWANIA KSC:

Z perspektywy organu właściwego funkcjonowanie KSC należy ocenić jako coraz bardziej dojrzałe, choć znajdujące się w fazie intensywnej adaptacji do nowych, unijnych ram regulacyjnych, w szczególności wynikających z rozporządzenia DORA. Kluczowym wyzwaniem jest harmonizacja krajowych przepisów o KSC z regulacją sektorową DORA, które różnią się zakresem podmiotowym i poziomem szczegółowości ale w praktyce powinny tworzyć spójny ekosystem zarządzania ryzykiem ICT. DORA wzmacnia podejście oparte na odporności operacyjnej, testowaniu (w tym nowych testach TLPT), zarządzaniu dostawcami ICT oraz wymianie informacji o incydentach, co z punktu widzenia organu właściwego uzupełnia i pogłębia mechanizmy znane z KSC, zamiast je zastępować. Efektywne wdrożenie DORA wymaga jednak ścisłej koordynacji interpretacyjnej i operacyjnej pomiędzy reżimami prawnymi, tak aby nie prowadzić do dublowania obowiązków po stronie podmiotów nadzorowanych, lecz do realnego wzmocnienia odporności krajowego systemu finansowego jako elementu KSC.

PROGNOZY I PRZEWIDYWANIA DLA KSC NA ROK 2026:

- W perspektywie 2026 r. mamy nadzieje, że KSC będzie dalej rozwijał się w kierunku większej harmonizacji z reżimem DORA, co powinno przełożyć się na większą przejrzystość i spójność wymagań stawianych podmiotom sektora finansowego. Pożądanym kierunkiem jest takie zbliżanie obu regulacji, które pozwoli na ich praktyczne uzupełnianie się i ograniczenie ryzyka rozbieżnych interpretacji regulacyjnych.
- Jednocześnie mamy nadzieje, że KSC będzie konsekwentnie dostosowywany do zmieniającego się krajobrazu zagrożeń, w tym narastających ryzyk związanych z łańcuchami dostaw, koncentracją usług ICT oraz wykorzystaniem nowych technologii przez sprawców incydentów. Oczekiwanym kierunkiem rozwoju jest wzmocnienie roli systemu jako narzędzia realnej koordynacji operacyjnej pomiędzy organami publicznymi a także zespołami CSIRT krajowymi oraz sektorowymi. W takim ujęciu KSC, funkcjonując równolegle z DORA, powinien w coraz większym stopniu przyczyniać się do odporności cyfrowej państwa i sektora finansowego.

PLANY NA ROK 2026:

Mając na uwadze trwający proces legislacyjny, w UKNF planowane są działania związane w wdrożeniem nowelizacji UKSC, w tym zwłaszcza określenie obowiązków podmiotów finansowych w kontekście wzajemnych relacji regulacji rozporządzenia DORA oraz znowelizowanej UKSC.

REKOMENDACJE NA 2026 - REKOMENDACJE DLA PEŁNOMOCNIKA RZĄDU DS. CYBERBEZPIECZEŃSTWA:

1. Organizacja regularnych ćwiczeń krajowych i sektorowych

Rekomenduje się organizację regularnych ćwiczeń cyberbezpieczeństwa na poziomie krajowym i sektorowym, ukierunkowanych na doskonalenie wymiany informacji, koordynacji działań oraz reagowania na zagrożenia. Ćwiczenia powinny obejmować realistyczne scenariusze incydentów o charakterze wielopodmiotowym, umożliwiając praktyczną weryfikację procedur oraz kanałów komunikacji w ramach KSC.

2. Wzmacnianie mechanizmów wymiany informacji w ramach KSC

Zasadne jest dalsze rozwijanie i uspójnianie mechanizmów wymiany informacji pomiędzy podmiotami KSC, zespołami CSIRT oraz właściwymi organami. Sprawna i terminowa wymiana informacji o incydentach i zagrożeniach wspiera budowę wspólnej świadomości sytuacyjnej oraz zwiększa zdolność systemu do reagowania na zdarzenia o charakterze sektorowym i krajowym.

3. Wspieranie inicjatyw podnoszących dojrzałość podmiotów KSC

Rekomenduje się wspieranie działań ukierunkowanych na stopniowe podnoszenie dojrzałości organizacyjnej i procesowej podmiotów KSC, w szczególności poprzez promowanie wymiany dobrych praktyk, rozwój kompetencji oraz dążenie do bardziej spójnego poziomu przygotowania w zakresie cyberbezpieczeństwa.

MINISTER WŁAŚCIWY DO SPRAW ZDROWIA (SEKTOR OCHRONY ZDROWIA (Z WYŁĄCZENIEM PODMIOTÓW PODLEGŁYCH MON) (MZ)

Ministerstwo Zdrowia

PODSUMOWANIE ROCZNE:

Sektor ochrony zdrowia w Polsce mierzy się z narastającą skalą zagrożeń cybernetycznych, co stanowi jedno z kluczowych wyzwań systemowych dla stabilności operacyjnej i bezpieczeństwa danych pacjentów. Postępująca digitalizacja, w tym wdrażanie elektronicznej dokumentacji medycznej oraz rozwój rozwiązań IoMT, znacząco zwiększają powierzchnię i możliwości ataku.

Skala incydentów rośnie dynamicznie. W 2025 r. odnotowano 1441 incydentów, dla porównania w 2024 r. było ich 1028, co stanowi wzrost o ok. 40% r/r.

Dominującymi zagrożeniami pozostają oszustwa sieciowe, podatne usługi sieciowe oraz ataki złośliwym kodem wykorzystujące słabo zabezpieczone urządzenia i oprogramowanie medyczne. Incydenty skutkują naruszeniami danych medycznych, przestojami operacyjnymi oraz realnym ryzykiem dla ciągłości opieki nad pacjentem.

Istotnym wyzwaniem pozostaje niedostateczna dojrzałość organizacyjna – znaczna część placówek nie dysponuje wyspecjalizowaną kadrą ds. cyberbezpieczeństwa, a polityki i procedury bezpieczeństwa często mają charakter fragmentaryczny.

Rosnąca skala zagrożeń wymusza intensyfikację działań defensywnych. Powołany przez Ministerstwo Zdrowia CSIRT CeZ intensyfikuje działania ostrzegawcze i edukacyjne oraz wykrywa i pomaga w eliminowaniu podatności cybernetycznych. Rozwijane są również inicjatywy współpracy krajowej i unijnej, zgodne z wymogami NIS2, mające na celu budowę systemowej odporności sektora.

DZIAŁANIA STRATEGICZNE:

Projekt A: Projekt w zakresie poprawy poziomu cyberbezpieczeństwa w obszarze ochrony zdrowia poprzez rozwój CSIRT CeZ. Projekt realizowany ze środków KPO.

Celem projektu jest poprawa poziomu cyberbezpieczeństwa w obszarze ochrony zdrowia poprzez rozwój sektorowego CSIRT. Przedsięwzięcie zapewnia kompleksowe podejście do aspektów bezpieczeństwa cyberprzestrzeni, poprzez realizację działań uwzględniających zarówno zakup narzędzi informatycznych - sprzętu i oprogramowania, jak również wsparcie odpowiedniego zaplecza eksperckiego, usługi konsultingowe i audytorskie, szkolenia pracowników CSIRT oraz działania promocyjne i tworzenie materiałów edukacyjnych, skierowanych do placówek medycznych i ich personelu.

Projekt B: Inwestycja D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie Zdrowia" realizowana w ramach środków z KPO.

W listopadzie 2025 r. Ministerstwo Zdrowia rozstrzygnęło nabór wniosków w ramach Inwestycji D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia". Jednym z działań w ramach tej inwestycji jest wzmocnienie poziomu cyberbezpieczeństwa w wybranych szpitalach. Wsparcie przeznaczone jest na modernizację infrastruktury IT, wdrażanie systemów ochrony przed cyberatakami, audyty bezpieczeństwa, szkolenia personelu oraz podnoszenie standardów zarządzania bezpieczeństwem informacji. Celem programu jest

wzmocnienie odporności placówek medycznych na zagrożenia cyfrowe oraz zapewnienie ciągłości udzielania świadczeń zdrowotnych. W ramach naboru wsparcie otrzyma 371 najwyżej ocenionych przedsięwzięć. Do dnia dzisiejszego podpisano 364 umów o objęcie przedsięwzięcia wsparciem z podmiotami wyłonionymi podczas procesu naboru.

DZIAŁANIA I WSPÓŁPRACA:

DZIAŁANIA EDUKACYJNE I BUDOWANIE ŚWIADOMOŚCI:

Działania realizowane przez CSIRT CeZ – ujęte w formularzu sprawozdania tego Zespołu.

ĆWICZENIA I WSPÓŁPRACA MIĘDZYNARODOWA:

Tabela 42. ĆWICZENIA I WSPÓŁPRACA MIĘDZYNARODOWA MZ

Nazwa ćwiczenia	Data	Rola CSIRT	Zasięg	opis scenariusza / Cel współpracy
Udział w ćwiczeniach krajowego systemu cyberbezpieczeństwa (KSC-EXE 2025)	11.2025	uczestnik	Krajowy	Celem ćwiczeń było sprawdzenie działania procedur oraz weryfikacja zdolności operacyjnych podmiotów KSC w sytuacji kryzysowej spowodowanej cyberatakami. Ćwiczenia zorganizowane z inicjatywy Pełnomocnika Rządu ds. Cyberbezpieczeństwa, odbyły się w dniu 26 listopada 2025 r. KSC EXE to cykliczne, międzysektorowe ćwiczenia weryfikujące zdolności cyberobrony podmiotów z kluczowych sektorów, w tym sektora ochrony zdrowia.

ANALIZA I OCENA FUNKCJONOWANIA KSC:

Z perspektywy organu właściwego ds. cyberbezpieczeństwa w sektorze ochrony zdrowia funkcjonowanie KSC należy ocenić jako:

- spełniające swoją rolę, lecz w praktyce napotykające na istotne bariery wdrożeniowe. System tworzy jasne ramy prawne, definiuje role podmiotów KSC, w tym OUK, oraz wprowadza obowiązki w zakresie zarządzania ryzykiem i raportowania incydentów. W sektorze ochrony zdrowia, ze względu na wrażliwość danych medycznych i bezpośredni wpływ incydentów na życie i zdrowie pacjentów, znaczenie tych regulacji jest szczególnie wysokie.
- obserwowany jest niski poziom dojrzałości organizacyjnej wielu podmiotów leczniczych. Często działania mają charakter reaktywny, a nie systemowy.
- Kluczowym problemem są braki kadrowe. Niedobór specjalistów ds. cyberbezpieczeństwa, administratorów i informatyków znacząco ogranicza możliwości realizacji wymagań KSC. Przyczyną są m.in. niewystarczające środki finansowe oraz brak cyklicznych programów szkoleniowych i ścieżek rozwoju zawodowego w podmiotach sektora ochrony zdrowia, w szczególności w szpitalach. Konkurencja z sektorem prywatnym pogłębia ten problem.
- Aspekty finansowe stanowią jedną z głównych barier. Wiele podmiotów nie dysponuje środkami na modernizację infrastruktury IT, zakup specjalistycznych narzędzi czy wdrożenie rozwiązań zwiększających odporność na ataki cyfrowe. Cyberbezpieczeństwo bywa traktowane jako koszt, a nie inwestycja w bezpieczeństwo pacjentów i ciągłość świadczeń.
- Istotnym wyzwaniem pozostaje także niska świadomość kadry zarządzającej w zakresie zagrożeń cybernetycznych, ryzyk i skutków ich wystąpienia. Brak zrozumienia skali zagrożeń oraz potrzeb związanych z cyfryzacją utrudnia podejmowanie decyzji strategicznych i alokację zasobów.

Podsumowując, KSC stanowi solidną podstawę prawną, jednak jego skuteczność w sektorze ochrony zdrowia wymaga wzmocnienia, w szczególności poprzez wsparcie finansowe, wdrożenie systemowych programów szkoleniowych oraz działań podnoszących świadomość zarządczą. Bez tego realny poziom odporności sektora pozostanie niewystarczający wobec rosnących zagrożeń.

PROGNOZY I PRZEWIDYWANIA DLA KSC NA ROK 2026:

W 2026 roku, po wejściu w życie nowelizacji UKSC, KSC wejdzie w fazę intensywnej transformacji. Nowelizacja znacząco rozszerzy katalog podmiotów objętych regulacją – z obecnych kilkuset do co najmniej kilku tysięcy, tylko w sektorze ochrony zdrowia – co istotnie zwiększy skalę nadzoru, raportowania incydentów oraz wymagań chociażby w zakresie zarządzania ryzykiem. Zdecydowana większość tych podmiotów nie jest jeszcze gotowa na realizację obowiązków wynikających z ustawy, więc czeka je bardzo trudne zadanie, żeby dostosować się do tych wymagań.

Z perspektywy OW oznacza to konieczność wzmocnienia mechanizmów koordynacji, standaryzacji wymagań oraz wsparcia podmiotów leczniczych w budowaniu dojrzałości cyberbezpieczeństwa. Kluczowym problemem może okazać się niewystarczające finansowanie, przez co nie będzie możliwe pozyskanie specjalistów, którzy będą realizować ten trudny i wymagający obszar działania.

PLANY NA ROK 2026:

W 2026 roku Ministerstwo Zdrowia skoncentruje się na realizacji rozszerzonych zadań wynikających z nowelizacji UKSC, w tym na objęciu nadzorem nowych podmiotów oraz wzmocnieniu mechanizmów monitorowania zgodności z wymogami ustawy.

Kluczowym wyzwaniem będzie pozyskanie i utrzymanie wykwalifikowanych pracowników – planowane jest zwiększenie zatrudnienia w obszarach nadzoru i kontroli. OW przewiduje także rozwój kompetencji eksperckich, wdrożenie procedur kontrolnych oraz wzmocnienia współpracy z innymi instytucjami KSC Celem jest skuteczny nadzór regulacyjny i podniesienie poziomu dojrzałości cyberbezpieczeństwa w sektorze ochrony zdrowia.

REKOMENDACJE NA 2026 - REKOMENDACJE DLA PEŁNOMOCNIKA RZĄDU DS. CYBERBEZPIECZEŃSTWA:

Z uwagi na ilość podmiotów, które obejmie znowelizowana UKSC oraz ograniczone zasoby kadrowe po stronie OW, zasadne wydaje się opracowanie jednolitych standardów, które umożliwią większą sprawność i efektywność realizowanych zadań (np. ustandaryzowanie - w wymaganym zakresie - wzorów raportów z audytów bezpieczeństwa systemów informacyjnych przeprowadzanych w podmiotach czy też podejścia w zakresie wymagań dot. zasobów kadrowych i kompetencyjnych). Takie działania ujednolicą procedury oraz usprawnią realizację ustawowych zadań zarówno po stronie podmiotów, jak i OW. Proponuje się ponadto skierowanie (również cyklicznie) do kluczowych podmiotów KSC korespondencji podkreślającej strategiczną rolę cyberbezpieczeństwa.

DZIAŁANIA MINISTRA INFRASTRUKTURY JAKO ORGANU WŁAŚCIWEGO DO SPRAW CYBEBRZPIECZEŃSTWA (MI)

Ministerstwo Infrastruktury

- Minister właściwy do spraw transportu – Minister Infrastruktury (sektor transportu z wyłączeniem podsektora transportu wodnego);
- Minister właściwy do spraw gospodarki morskiej oraz minister właściwy do spraw żeglugi śródlądowej – Minister Infrastruktury (podsektor transportu wodnego);
- Minister właściwy do spraw gospodarki wodnej – Minister Infrastruktury (sektor zaopatrzenia w wodę pitną i jej dystrybucji).

PODSUMOWANIE ROCZNE:

W 2025 r. Ministerstwo Infrastruktury realizując obowiązki organu właściwego dla dwóch sektorów ujętych w KSC: transportu oraz zaopatrzenia w wodę pitną i jej dystrybucji, podejmowało szereg działań, spośród których do najistotniejszych można zaliczyć:

- czynności związane z utworzeniem CSIRTu sektorowego – Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego dla podmiotów z sektorów pozostających we właściwości Ministra Infrastruktury;
- zainicjowanie oraz koordynacja działań zmierzających do utworzenia Centrum Wymiany Informacji i Analiz (ISAC) dla podmiotów z sektora zaopatrzenia w wodę pitną i jej dystrybucji.

Ministerstwo Infrastruktury brało czynny udział w pracach nad projektem ustawy o zmianie UKSC oraz niektórych innych ustaw (UC32). Na każdym etapie legislacyjnym dokonywano analiz projektu ustawy, zgłaszając niejednokrotnie uwagi oraz konsultując w różnych formach (zgłoszone uwagi obejmowały m.in.: fakultatywne wyznaczanie decyzją administracyjną organu właściwego ds. cyberbezpieczeństwa podmiotów świadczących usługi w więcej niż jednym sektorze zamiast obligatoryjnego, uwzględnienie wszystkich podmiotów podległych lub nadzorowanych przez Ministra Infrastruktury w katalogu podmiotów uprawnionych do wypłaty dodatku do wynagrodzenia za pracę, tzw. “świadczenia teleinformatycznego” czy uwag porządkowych oraz do skutków finansowych projektu).

Stale podejmowano działania statutowe wynikające z UKSC: prowadzono kontrolę operatorów usług kluczowych w zakresie bezpieczeństwa systemów informacyjnych służących do świadczenia usługi kluczowej (w 2025 r. przeprowadzono dwie kontrole planowe) czy postępowania administracyjne wobec naruszających obowiązki operatorów usług kluczowych.

W 2025 r. koncentrowano się również na budowaniu relacji z podmiotami, które wraz z nowelizacją UKSC prawdopodobnie staną się podmiotami kluczowymi i ważnymi, a także udzielano licznych wyjaśnień i odpowiedzi na kwestie związane z implementacją Dyrektywy NIS2 oraz budową CSIRTu sektorowego.

W celu zapewnienia wsparcia podmiotom w nadzorowanych sektorach, także wśród wytypowanych podmiotów kluczowych i podmiotów ważnych, aktywnie promowano System S46. Ministerstwo Infrastruktury brało także udział w warsztatach dotyczących wykazu inicjalnego KSC (obejmującego podmioty po nowelizacji UKSC) pod kątem funkcjonalności oraz występowania ewentualnych błędów, budowanego w ramach systemu S46.

Z powyższych wymieniono jedynie niektóre z podejmowanych przez Ministerstwo Infrastruktury działań, natomiast wszystkie z nich wpłynęły pozytywnie na rozwój i wzmocnienie cyberbezpieczeństwa w sektorach transportu oraz zaopatrzenia w wodę pitną i jej dystrybucji, realizując tym samym cel główny Strategii Cyberbezpieczeństwa RP, tj.: *Podniesienie poziomu odporności krajowych podmiotów przez zwiększenie poziomu ochrony informacji oraz zwiększenie zdolności do wykrywania i reagowania na zagrożenia, promowanie wiedzy i dobrych praktyk oraz podnoszenie kompetencji w zakresie cyberbezpieczeństwa.*

DZIAŁANIA STRATEGICZNE:

Projekt A: Utworzenie CSIRT sektorowego w Ministerstwie Infrastruktury – CSIRT Infrastruktura

W projekcie realizowanym w Inwestycji C3.1.1. "*Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo*" w ramach Krajowego Planu Odbudowy, Ministerstwo Infrastruktury podjęło działania zmierzające do utworzenia Sektorowego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego, który będzie świadczyć usługi dla podmiotów w sektorach pozostających we właściwości Ministra Infrastruktury jako organu właściwego ds. cyberbezpieczeństwa. Partnerem projektu jest Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy. W 2025 r. podjęto szereg działań przygotowujących do uruchomienia CSIRTu. Projekt jest obecnie na etapie realizacji, z planowanym formalnym terminem ustanowienia na połowę 2026 r.

Projekt B: Utworzenie Centrum Wymiany i Analizy Informacji (ISAC) w sektorze zaopatrzenia w wodę pitną i jej dystrybucji

Ministerstwo Infrastruktury wsparło podmioty z sektora zaopatrzenia w wodę pitną i jej dystrybucji w ustanowieniu ISAC wod-kan. Wynikiem tych działań było podpisanie dnia 5 września 2025 r. porozumienia ws. utworzenia ISAC wod-kan, przez: MPWIK Wrocław S.A., Aquanet Poznań S.A., Wodociągi Miasta Krakowa S.A. oraz MPWIK Warszawa S.A. Już 21 listopada 2025 r. do ISAC wod-kan dołączyły 3 kolejne podmioty.

Celem utworzenia ISAC jest przede wszystkim zwiększenie poziomu cyberbezpieczeństwa poprzez szybsze reagowanie na zagrożenia i lepsze zabezpieczenie infrastruktury, zacieśnienie współpracy oraz umożliwienie dzielenia się najlepszymi praktykami. W rezultacie przyczynia się to do optymalizacji działań, a regularna wymiana informacji zwiększa dodatkowo świadomość zagrożeń i sprzyja budowaniu zaufania między podmiotami. Członkowie ISAC mogą korzystać z doświadczeń innych podmiotów, a przez to podnosić swoje kompetencje w obszarze cyberbezpieczeństwa.

DZIAŁANIA I WSPÓŁPRACA:

DZIAŁANIA EDUKACYJNE I BUDOWANIE ŚWIADOMOŚCI:

Tabela 43. DZIAŁANIA EDUKACYJNE I BUDOWANIE ŚWIADOMOŚCI MI

LP	Nazwa działania/kampanii	Grupa docelowa	Liczba odbiorców
1	Udział w warsztatach „CSIRT Fundamentals”	Menagerowie cyberbezpieczeństwa średniego i wyższego szczebla	2
2	Udział w szkoleniu kadr CSIRT sektorowych	Pracownicy sektorowych zespołów CSIRT	1
3	Organizacja spotkania dedykowanego obszarowi cyberbezpieczeństwa w podsektorze transportu lotniczego	Kadra zarządzająca wyższego szczebla podmiotów podsektora transportu lotniczego z całej Polski	ok. 60
4	Prelekcja oraz udział w debacie pn. „Głos sektorów objętych i oczekujących na objęcie ustawą KSC” podczas wydarzenia KSC Forum 2025	Kadra zarządzająca, liderzy, eksperci oraz praktycy cyberbezpieczeństwa	ok. 400
5	Działania promujące konkurs grantowy „Cyberbezpieczne wodociągi”	Operatorzy usług kluczowych oraz inne podmioty, które prawdopodobnie staną się podmiotami kluczowymi i ważnymi wraz z nowelizacją ustawy o KSC z sektora zaopatrzenia w wodę pitną i jej dystrybucji	82

ĆWICZENIA I WSPÓŁPRACA MIĘDZYNARODOWA:

Tabela 44. ĆWICZENIA I WSPÓŁPRACA MIĘDZYNARODOWA MI

LP	Nazwa ćwiczenia	Data	Rola CSIRT	Zasięg	opis scenariusza / Cel współpracy
1	Ćwiczenia KSC-EXE 2025	11.2025	Uczestnik	Krajowy	Przegląd obowiązujących procedur w skali kraju, weryfikacja zdolności operacyjnej podmiotów krajowego systemu cyberbezpieczeństwa do działania w sytuacji kryzysowej spowodowanej incydentami, budowa świadomości w zakresie postępowania w sytuacji kryzysowej wśród organów wchodzących w skład Zespołu ds. Incydentów Krytycznych lub Rządowego Zespołu Zarządzania Kryzysowego.
2	Warsztaty „CSIRT Fundamentals”	02.2025	Uczestnik	Międzynar.	Wymiana poglądów i najlepszych praktyk w zakresie cyberbezpieczeństwa, rozwój umiejętności i kompetencji uczestników w zakresie reagowania na incydenty bezpieczeństwa informacji i zagrożeń cyberbezpieczeństwa, omówienie najnowszych zagrożeń w cyberprzestrzeni oraz metody ich analizy, zarządzania ryzykiem oraz wymiana wiedzy w zakresie budowania zespołów takich jak Security Operation Center czy CSIRT.
3	Spotkanie z delegacją Kongresu USA	08.2025	Organizator	Międzynar.	Przedstawienie wyzwań w sferze cyberbezpieczeństwa ze szczególnym uwzględnieniem sektora transportu oraz wymiana doświadczeń oraz wiedzy odnośnie Centrów Wymiany i Analizy Informacji tzw. ISAC.

4	Spotkanie branży lotniczej	10.2025	Organizator	Krajowy	Przedstawienie aktualnego krajobrazu zagrożeń dla podsektora transportu lotniczego, a także zagadnień związanych z koordynacją i zarządzaniem komunikacji oraz działaniami w sytuacjach kryzysowych. Omówienie metod i środków zwiększających poziom bezpieczeństwa w ramach NIS2, KSC 2.0 oraz Part-IS Cyber dla Safety, a także certyfikacja osób i podmiotów. Prezentacja roli ISAC Lotniczego w obliczu zagrożeń oraz potrzeb sektora.

ANALIZA I OCENA FUNKCJONOWANIA KSC:

Podmioty wchodzące w skład KSC realizują zadania związane z reagowaniem na incydenty bezpieczeństwa teleinformatycznego, a efektywność całego systemu pozostaje bezpośrednio powiązana z poziomem dojrzałości organizacyjnej OUK oraz zapewnieniem odpowiednich zasobów kadrowych posiadających specjalistyczne kompetencje w obszarze cyberbezpieczeństwa. Niemniej jednak, występowanie coraz większej ilości cyberataków oraz zwiększenie podmiotów wchodzących w KSC zgodnie z nowelizacją UKSC powodują, że system potrzebuje dalszego rozwoju i adaptacji. Osiągnięcie wysokiego poziomu dojrzałości całego systemu KSC jest kluczowe dla bezpieczeństwa państwa i ciągłości usług kluczowych. Do głównych atutów systemu należy jasne określenie ram prawnych i organizacyjnych, centralizacja procesów reagowania, istnienie wielu mechanizmów służących do wymiany informacji i platform analitycznych, które umożliwiają szybką identyfikację i monitorowanie zagrożeń. Rosnąca świadomość cyberzagrożeń wśród OUK oraz administracji państwowej przyczyniają się do poprawy odporności systemu. Jednocześnie w funkcjonowaniu KSC identyfikuje się istotne wyzwania. Jednym z nim jest ograniczona dostępność specjalistów oraz kompetencji w obszarze cyberbezpieczeństwa, również w systemach OT i ICT. Warto zaznaczyć, że organy właściwe prowadzą kontrole u podmiotów wykorzystujących tego typu rozwiązania, dlatego podstawowa wiedza z zakresu OT jest niezbędna do prawidłowego przeprowadzania działań kontrolnych. Kolejnym wyzwaniem jest bardzo zróżnicowany poziom dojrzałości cyberbezpieczeństwa wśród OUK. Część OUK posiada zaawansowane systemy monitoringu i procedury bezpieczeństwa, natomiast inne dysponują jedynie minimalnymi zabezpieczeniami, co tworzy słabe ogniwa w systemie KSC.

Dotychczasowe wnioski z funkcjonowania systemu KSC wskazują na konieczność dalszego wzmacniania kadrowego i kompetencyjnego. Istotne jest również przygotowanie systemu na zagrożenia hybrydowe poprzez ćwiczenia obejmujące IT, OT, media i działania fizyczne. Regularne monitorowanie i ocena dojrzałości OUK, a także wsparcie dla mniej dojrzałych operatorów, są niezbędne dla zapewnienia spójności i bezpieczeństwa całego systemu KSC.

KSC w obliczu rosnących zagrożeń hybrydowych, różnic w dojrzałości OUK oraz niedoborów kadrowych wymaga dalszego rozwoju, standaryzacji i wzmocnienia procesów wymiany informacji.

PROGNOZY I PRZEWIDYWANIA DLA KSC NA ROK 2026:

W perspektywie nadchodzącego roku priorytetem dla Ministerstwa Infrastruktury będzie utworzenie CSIRTu sektorowego realizującego zadania w sektorach pozostających we właściwości Ministra Infrastruktury jako organu właściwego ds. cyberbezpieczeństwa.

Jako podmiot publiczny Ministerstwo w 2026 r. będzie podejmowało działania w zakresie realizacji obowiązków wynikających z przepisów znowelizowanej UKSC, poprzez dostosowanie istniejących rozwiązań organizacyjnych, technicznych i proceduralnych do nowych wymogów.

Kolejnym istotnym zadaniem na 2026 r. jest rozwój kompetencji pracowników oraz zwiększenie kadry realizującej zadania organu właściwego ds. cyberbezpieczeństwa. Nowelizacja UKSC wprowadza szereg nowych obowiązków oraz znacząco zwiększa liczbę podmiotów pozostających pod nadzorem organu właściwego. Przy obecnym stanie zatrudnienia realizacja nowych zadań nie będzie możliwa. Dodatkowo

Ministerstwo Infrastruktury planuje działania ukierunkowane na podnoszenie świadomości w zakresie cyberzagrożeń wśród operatorów usług kluczowych oraz skutków wejścia w życie nowelizacji UKSC.

W obszarze reagowania na sytuacje kryzysowe, w 2026 r. Ministerstwa Infrastruktury podejmie działania w celu dalszego usprawnienia procedur i mechanizmów. Priorytetem będzie testowanie zdolności operacyjnej w ramach ćwiczeń, angażujących zarówno OUK, jak i instytucje państwowe.

PLANY NA ROK 2026:

Jednym z najistotniejszych przedsięwzięć na 2026 r. jest utworzenie CSIRTu sektorowego w Ministerstwie Infrastruktury, który będzie odpowiadał potrzebom obu sektorów oraz zapewni spełnienie obowiązków ustawowych wynikających z nowelizacji UKSC. CSIRT INFRASTRUKTURA będzie istotnym elementem krajowego systemu obrony przed cyberatakami w strategicznych sektorach infrastruktury, poprawiając bezpieczeństwo w całym kraju.

Rosnąca liczba nadzorowanych podmiotów i rozszerzenie katalogu zadań przekładają się bezpośrednio na konieczność zapewnienia odpowiednich zasobów kadrowych oraz zdolności operacyjnych. Stąd, w związku z nowelizacją UKSC oraz możliwością rozszerzenia kadry osób realizujących zadania organu właściwego ds. cyberbezpieczeństwa, Ministerstwo Infrastruktury planuje w 2026 r. zwiększenie zasobów kadrowych oraz rozwój kompetencji w zakresie zadań wynikających z nowelizowanej UKSC.

REKOMENDACJE NA 2026 - REKOMENDACJE DLA PEŁNOMOCNIKA RZĄDU DS. CYBERBEZPIECZEŃSTWA:

Podejmowanie działań wspierających wymianę wiedzy i informacji pomiędzy organami właściwymi ds. cyberbezpieczeństwa w zakresie bieżących działań, w tym ich postępów i wyzwań wynikających z wejścia w życie nowelizacji UKSC.

DZIAŁANIA MINISTRA CYFRYZACJI JAKO ORGANU WŁAŚCIWEGO DO SPRAW CYBEBRZPIECZEŃSTWA (MC)

Ministerstwo Cyfryzacji

CENTRALNY OŚRODEK INFORMATYKI (COI)

COI Centralny Ośrodek Informatyki

Jednostka nadzorowana przez ministra cyfryzacji.

PODSUMOWANIE ROCZNE:

W 2025 r. COI utrzymał stabilność cyberprzestrzeni, priorytetyzując bezpieczeństwo ekosystemu mObywatel. Głównym sukcesem było wdrożenie nowych e-usług (m.in. mStłuczka, mObywatel Junior, e-podpis) oraz wzmocnienie ochrony danych poprzez obowiązkową aktualizację aplikacji. Skutecznie zabezpieczono proces wyborczy dzięki nowej, metodzie weryfikacji mDowodu. Stabilność cyberprzestrzeni zapewniono dzięki aktywnej wymianie informacji z CSIRTami poziomu krajowego. Sytuację instytucji ocenia się jako stabilną, z wysoką skutecznością mitygacji zagrożeń w obszarze usług publicznych.

KLUCZOWE PROJEKTY I INICJATYWY:

Projekt A: Rozbudowa ekosystemu aplikacji mObywatel (aplikacja mObywatel)

Celem projektu jest zapewnienie obywatelom cyfrowego portfela dokumentów i usług publicznych w telefonie, który umożliwia szybkie potwierdzanie tożsamości, weryfikację uprawnień oraz załatwianie spraw urzędowych bezpośrednio w aplikacji mObywatel. W 2025 roku użytkownicy zyskali szereg nowych funkcji, m.in. mStłuczkę, mObywatel Junior, możliwość składania podpisu osobistego i kwalifikowanego z poziomu aplikacji oraz usługę Twoje sprawy, pozwalającą na szybkie sprawdzenie statusu złożonych wniosków urzędowych.

Rozszerzono również katalog dokumentów i cyfrowych legitymacji, dodano możliwość zapisów na szkolenia obronne oraz udostępniono wirtualnego asystenta, który wspiera użytkowników w sprawach związanych z administracją publiczną i usługami dostępnymi w aplikacji.

Istotnym elementem projektu była także poprawa bezpieczeństwa i stabilności działania mObywatela poprzez wprowadzenie obowiązku aktualizacji aplikacji do wersji 4.71.1 lub nowszej. Zapewniło to wyższy poziom ochrony danych oraz usprawniło funkcjonowanie całej aplikacji.

Projekt B: Przygotowanie specjalnej metody weryfikacji mDowodu w trakcie wyborów prezydenckich w 2025 roku

Ministerstwo Cyfryzacji, we współpracy z COI oraz w porozumieniu z Krajowym Biurem Wyborczym, na potrzeby wyborów prezydenckich w 2025 r., przygotowało specjalną metodę potwierdzania tożsamości wyborców posługujących się mDowodem. Rozwiązanie to opierało się na dostępnej w aplikacji mObywatel metodzie kryptograficznej, czyli najbezpieczniejszym i najbardziej wiarygodnym sposobie weryfikacji autentyczności mDowodu.

Mechanizm weryfikacji tożsamości został odpowiednio zmodyfikowany i dostosowany do specyfiki procesu wyborczego i możliwości technicznych okręgowych komisji wyborczych, które nie dysponowały sprzętem umożliwiającym standardową weryfikację kryptograficzną (urządzenie–urządzenie lub aplikacja– aplikacja). Każda komisja otrzymała wraz z pakietem wyborczym specjalny kod QR.

Po jego zeskanowaniu przez wyborcę korzystającego z mDowodu, na jego telefonie wyświetlał się ekran prezentujący dane pobrane z Rejestru Dowodów Osobistych oraz dodatkowe, unikalne elementy pozwalające na skuteczną weryfikację autentyczności dokumentu. Co istotne, ekran ten mógł być uruchomiony wyłącznie w dniu wyborów, co znacząco ograniczyło możliwość jego podrobienia lub nieuprawnionego wcześniejszego użycia.

OBSERWOWANE TRENDY I WYZWANIA:

Wzrost zgłoszeń dotyczących wyłudzeń tożsamości - w ostatnich latach obserwujemy wyraźny wzrost przypadków kradzieży tożsamości w Internecie. Coraz więcej cyberprzestępców wykorzystuje powszechny dostęp do danych osobowych, które często trafiają do sieci w wyniku wycieków z różnych instytucji oraz komputerów domowych obywateli. Rozwój technologii ułatwia tworzenie fałszywych kont oraz dokumentów, co umożliwia dokonywanie przestępstw podszywając się pod niczego nieświadome ofiary. W łańcuchu procederu przestępczego wykorzystywane są instytucje bankowe, aplikacje i systemy rządowe oraz firmy z sektora handlowego.

ANALIZA I OCENA FUNKCJONOWANIA KSC

Centralny Ośrodek Informatyki utrzymuje stałe kontakty z CSIRTami poziomu krajowego wymieniając się dwustronnie informacjami dotyczącymi incydentów bezpieczeństwa, podatności i innych zidentyfikowanych zagrożeń.

REKOMENDACJE NA 2026 - REKOMENDACJE DLA PEŁNOMOCNIKA RZĄDU DS. CYBERBEZPIECZEŃSTWA:

W oparciu o doświadczenia operacyjne z 2025 roku oraz planowane wejście w życie kluczowych przepisów nowelizacji UKSC, COI rekomenduje podjęcie następujących działań:

- **Inicjatywy Legislacyjne w zakresie ochrony tożsamości** - Rekomenduje się uszczelnienie przepisów w celu całkowitej eliminacji z obrotu tzw. "dokumentów kolekcjonerskich" oraz penalizacji tworzenia i dystrybucji aplikacji mobilnych imitujących interfejs usług państwowych (np. mObywatel). Działania te są niezbędne dla ograniczenia fali oszustw typu identity theft oraz ochrony zaufania obywateli do cyfrowego państwa.
- **Wsparcie wdrożenia wymogów NIS2 i KSC -** Rekomenduje się wypracowanie jednolitych wytycznych dla podmiotów publicznych w zakresie zarządzania bezpieczeństwem w łańcuchu dostaw. Nowelizacja UKSC nakłada nowe obowiązki weryfikacji dostawców ICT – niezbędne jest wsparcie merytoryczne i narzędziowe dla instytucji realizujących te zadania, aby uniknąć fragmentacji standardów.
- **Centralizacja programów Security Awareness** - Proponuje się uruchomienie ogólnokrajowej kampanii edukacyjnej, koordynowanej przez Pełnomocnika, skupionej na bezpiecznym korzystaniu z tożsamości cyfrowej (Profil Zaufany, mObywatel) w celu przeciwdziałania socjotechnice, która pozostaje głównym wektorem ataków w 2025/2026 roku.

INSTYTUT ŁĄCZNOŚCI – PAŃSTWOWY INSTYTUT BADAWCZY

Jednostka nadzorowana przez ministra cyfryzacji.

PODSUMOWANIE ROCZNE:

Działające w strukturze organizacyjnej IŁ-PIB Laboratorium Oceny Bezpieczeństwa Produktów Teleinformatycznych osiągnęło w 2025 roku kolejny poziom kompetencji. Laboratorium przeszło z powodzeniem proces organizacyjny i techniczny, który zakończył się wydaniem pozytywnej decyzji Ministra Cyfryzacji o wydaniu zezwolenia na realizację ewaluacji bezpieczeństwa na poziomie uzasadnienia zaufania 'wysoki' w programie EUCC jako jednostka oceniająca zgodność (CAB-ITSEF).

Laboratorium Oceny Bezpieczeństwa w IŁ-PIB jest pierwszym CAB-ITSEF w regionie oraz jednym z nielicznych laboratoriów w Europie, które mogą wykazać się potwierdzonymi formalnie kompetencjami w programie EUCC na takim poziomie uzasadnienia zaufania.

W bazie podmiotów notyfikowanych Unii Europejskiej NANDO w kontekście regulacji 2024/482 (https://webgate.ec.europa.eu/single-market-compliance-space/notified-bodies) Instytut Łączności jest zarejestrowany jako ITSEF 3195.

Laboratorium Oceny Bezpieczeństwa w IŁ-PIB realizuje z powodzeniem oceny bezpieczeństwa oraz badania zgodności oprogramowania, urządzeń sprzętowych, modułów kryptograficznych, urządzeń sieci 5G, urządzeń radiowych.

W ramach działań związanych z wdrożeniem europejskiego portfela tożsamości cyfrowej IŁ-PIB rozpoczął w 2025 roku krajowy schemat certyfikacji europejskiego portfela tożsamości cyfrowej, w tym w części dotyczącej cyberbezpieczeństwa.

W 2026 r. Dział Informatyki, we współpracy z obszarem bezpieczeństwa, planuje zintensyfikować działania ukierunkowane na podniesienie dojrzałości cyberbezpieczeństwa, tak aby zwiększyć przewidywalność działania usług oraz ograniczyć ryzyka wynikające z incydentów i awarii. Prace będą realizowane w formie programu poprawy, obejmującego ujednolicenie zasad i sposobu nadzoru, doprecyzowanie kluczowych procedur oraz wdrożenie rozwiązań wspierających bieżącą ochronę i monitoring. Celem jest stopniowe podnoszenie standardów, lepsza kontrola nad dostępami i zasobami oraz wzmocnienie zdolności reagowania na zdarzenia, przy zachowaniu ciągłości działania Instytucji.

KLUCZOWE PROJEKTY I INICJATYWY:

Realizacja zadań w obszarach działań Ministra właściwego ds. informatyzacji związanych z:

- funkcjonowaniem w europejskim programie certyfikacji cyberbezpieczeństwa zgodnym z Common Criteria (EUCC);
- wdrażaniem i funkcjonowaniem ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa;
- opracowaniem projektu krajowego programu certyfikacji portfela tożsamości cyfrowej.

Celem umowy dotacji, którą Ministerstwo Cyfryzacji udzieliło IŁ-PIB w 2025 roku, było:

- Wsparcie Ministra w działaniach wskazanych w ustawie z 25 czerwca 2026 roku, które mogą zostać powierzone państwowym instytutom badawczym, znajdującym się pod nadzorem Ministra właściwego do spraw informatyzacji;
- Rozbudowa krajowych kompetencji w obszarze oceny zgodności produktów teleinformatycznych w ramach programu EUCC w obszarach wymagających zezwolenia krajowego organu ds. certyfikacji cyberbezpieczeństwa (Ministra Cyfryzacji);
- Rozpoczęcie procesu przygotowania krajowego schematu certyfikacji europejskiego portfela tożsamości cyfrowej, które obejmują zbudowanie struktur oceny zgodności rozwiązań portfela, przeprowadzenie działań ewaluacyjnych oraz wydanie certyfikatów w trzech programach certyfikacji: obszaru funkcjonalnego, cyberbezpieczeństwa oraz środków identyfikacji elektronicznej wdrożonych w portfelu.

Umowa została zrealizowana i wszystkie cele zostały osiągnięte.

OBSERWOWANE TRENDY I WYZWANIA:

Trend 1: rozwój rynku certyfikacji cyberbezpieczeństwa w Europie
Rok 2025 był czasem rozwoju i potwierdzania kompetencji jednostek oceniających zgodność, realizujących oceny zgodności i wydających certyfikaty (odpowiednio, CAB-ITSEF i CAB-CB) w celu spełnienia wymagań programu EUCC. Ten okres kończy się w lutym 2026 i program EUCC wchodzi w pełni operacyjną fazę. Dzięki pracom Laboratorium Oceny Bezpieczeństwa w IŁ-PIB, polskie zdolności realizacji ocen bezpieczeństwa są porównywalne z najbardziej zaawansowanymi członkowskimi UE.

Trend 2: Braki kadrowe
Niewystarczająca liczba pracowników IT nie pozwalała do tej pory na wykonywanie prac rozwojowych środowiska teleinformatycznego IŁ-PIB. Zmiany organizacyjne oraz inwestycje w zakresie rozbudowy zespołu IT pozwalają na stopniowe budowanie kompetencji zespołu i pokrywanie coraz to nowych obszarów niezbędnych do podnoszenia poziomu bezpieczeństwa środowiska teleinformatycznego Instytutu.

Trend 3: Braki technologiczne
Niewystarczająca liczba pracowników IT nie pozwalała do tej pory na wykonywanie prac rozwojowych środowiska teleinformatycznego IŁ-PIB. Zmiany organizacyjne oraz inwestycje w zakresie rozbudowy i hardeningu obecnego środowiska pozwalają na stopniowe zabezpieczanie coraz to nowych obszarów, co w przyszłości pozwoli na podniesienie ogólnego poziomu bezpieczeństwa środowiska teleinformatycznego Instytutu.

ANALIZA I OCENA FUNKCJONOWANIA KSC:

- Z uwagi na brak ustawy wdrażającej postanowienia Dyrektywy NIS2 do KSC trudno ocenić jej wpływ na skuteczność tego systemu. Największym wyzwaniem nowej ustawy będzie włączenie wielu tysięcy nowych podmiotów tego systemu (klasyfikowanych jako podmioty kluczowe i ważne) i uzyskanie w zdefiniowanej perspektywie mierzalnego i utrzymywanego poziomu cyberbezpieczeństwa świadczonych usług, jednakże:
- KSC stanowi potrzebny i funkcjonujący mechanizm koordynacji państwowej (zwłaszcza w obszarze współpracy z CSIRT-ami i ćwiczeń), ale skuteczność „na styku" zależy od dojrzałości procesów i narzędzi po stronie instytucji;
- Największą wartość KSC osiąga w scenariuszach, gdzie instytucja ma przygotowane minimum operacyjne (procedury, role, kanały, rejestry). Nie każda instytucja jest na to gotowa, brakuje wsparcia merytorycznego w tym zakresie.
- Ostatnie zmiany legislacyjne (KSC/NIS2) wzmacniają presję na uporządkowanie cyberbezpieczeństwa i formalną rozliczalność.

REKOMENDACJE NA 2026 REKOMENDACJE DLA PEŁNOMOCNIKA RZĄDU DS. CYBERBEZPIECZEŃSTWA:

1. Wzorem kilku krajów członkowskich UE należy wdrażać programy upowszechniające certyfikację cyberbezpieczeństwa, w tym programy o charakterze pomocowym, tak aby zainteresować certyfikacją małe i średnie przedsiębiorstwa.

2. W 2026 roku należy zapewnić możliwość certyfikacji europejskiego portfela tożsamości cyfrowej w krajowym schemacie certyfikacji. W dłuższej perspektywie, krajowy system certyfikacji cybezpieczeństwa należy rozszerzyć na inne podmioty, które pełnią ważną rolę w ekosystemie portfela (np. na kwalifikowanych dostawców usług zaufania lub kwalifikowanych poświadczeń atrybutów).

3. Warto, aby KSC rozwijał jednolite formaty i kanały dystrybucji ostrzeżeń/IOC oraz rekomendował minimalne use-case'y detekcyjne (np. dla AD, poczty, VPN). Ułatwi to szybkie wdrażanie działań ochronnych i ujednolica poziom bezpieczeństwa.

4. Warto wprowadzić jednolity zakres minimalny danych incydentu oraz możliwość automatyzacji lub eksportu incydentu z systemów ITSM/SIEM. Formularze powinny wspierać triage (kategorie, priorytety, minimalny zestaw danych), umożliwiać szybkie uzupełnienia i korekty, oraz jasno rozróżniać „zgłoszenie wstępne" i „raport końcowy".

5. Wytworzenie więcej gotowych materiałów wdrożeniowych do wykorzystania w instytucjach (ustandaryzowane, aktualizowane pakiety do wdrożenia), np.: wzory playbooków IR (phishing, ransomware, utrata konta), wzór planu ćwiczeń i raportu z wnioskami, minimalny szablon RACI/organizacji SOC-triage.

URZĄD KOMUNIKACJI ELEKTRONICZNEJ (UKE)

Organ nadzorowany przez ministra cyfryzacji.

PODSUMOWANIE ROCZNE:

Sytuacja w cyberprzestrzeni w obszarze zainteresowania Prezesa Urzędu Komunikacji Elektronicznej przedstawia się następująco:

- Sektor komunikacji elektronicznej:
  Przedsiębiorcy telekomunikacyjni nie zgłosili incydentów poważnych w obszarze cyberbezpieczeństwa. Realizując obowiązki wynikające z Rozdziału VIIa ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U z 2024 poz. 34, 731,834,1222) przedsiębiorcy telekomunikacyjni zaraportowali w 2025 roku 28 naruszeń w zakresie dostępności sieci i usług telekomunikacyjnych, w szczególności spowodowanych awariami sprzętu i oprogramowania. Odnotowano wzrost liczby oraz wolumenu ataków typu DDoS, pośród których rekordowy przekroczył 1,5 Tbps.
- Bezpieczeństwo wewnętrzne UKE:
  W 2025 r. nie odnotowano skutecznych prób naruszenia bezpieczeństwa systemów informatycznych UKE.
- Współpraca międzynarodowa:
  Kontynuowano współpracę z ENISA[7] (m.in. w ramach wspólnego europejskiego systemu CIRAS[8] zaraportowano 4 istotne naruszenia bezpieczeństwa oraz integralności sieci i usług komunikacji elektronicznej), z BEREC[9] oraz w ramach grup roboczych: ECASEC[10], C&R WG[11] i Grupy ds. certyfikacji cyberbezpieczeństwa sieci 5G przy ENISA[12].
- Współpraca krajowa:
  W ramach zwiększania zaangażowania w KSC uczestniczono w ćwiczeniu KSC-EXE 2025, w spotkaniach Forum Organów Właściwych funkcjonującego pod auspicjami Ministerstwa Cyfryzacji oraz przystąpiono do programu Partnerstwo dla Cyberbezpieczeństwa realizowanego przez NASK PIB. Ponadto, prowadzone były cykliczne spotkania koordynacyjne z przedsiębiorcami telekomunikacyjnymi (formuła ISAC), dotyczące bezpieczeństwa sektora telekomunikacyjnego.

KLUCZOWE PROJEKTY I INICJATYWY:

Projekt A: „Cyberbezpieczny UKE”

Cel: Projekt Cyberbezpieczny UKE stanowi integralną część inicjatywy Cyberbezpieczny Rząd, a realizacja zadań w obszarach:

- System Zarządzania Bezpieczeństwem Informacji,
- system szkoleń,
- modernizacja techniczna,

[7] European Union Agency for Cybersecurity (ENISA)
[8] Cybersecurity Incident Reporting and Analysis System (CIRAS)
[9] Body of European Regulators for Electronic Communications (BEREC)
[10] European Competent Authorities for Secure Electronic Communications (ECASEC)
[11] Cybersecurity and Resilience Working Group (C&R WG)
[12] Ad hoc Working Group on the candidate EU 5G Cybersecurity Certification Scheme

znacząco poprawi efektywność działania, optymalizację kosztów, skróci czas reakcji na cyberzagrożenia oraz przygotuje Urząd do realizacji przedsięwzięć wynikających m.in. z implementacji wymagań Dyrektywy NIS2.

Status: w trakcie realizacji.

Efekty: Efektem realizacji projektu będzie szeroko rozumiana poprawa poziomu cyberbezpieczeństwa UKE, co w bezpośredni sposób przełoży się na:

- jakość i bezpieczeństwo usług (np. PLI CBD [13], PIT [14]) dostarczanych interesariuszom zewnętrznym,
- bezpieczeństwo danych wrażliwych otrzymywanych z nadzorowanych sektorów,
- budowę zaufania do podmiotu centralnej administracji rządowej,
- przygotowanie do wypełniania obowiązków organu właściwego ds. cyberbezpieczeństwa, podmiotu kluczowego i CSIRT sektorowego, wynikających z nowelizacji UKSC.

Projekt B: „Projekt 5G Trusted And seCure network servICes – 5G Tactic"

Cel: Projekt jest realizowany w ramach programu Digital Europe przez międzynarodowe konsorcjum, w skład którego wchodzą polskie podmioty i instytucje: PCSS[15], NASK PIB[16] oraz UKE. Jego celem jest wzmocnienie cyberbezpieczeństwa sieci 5G poprzez rozwój współpracy między organami krajowymi, operatorami sieci i dostawcami specjalistycznych technologii.

Status: w trakcie realizacji.

Efekty: W trakcie realizacji projektu prowadzone są m. in. działania obejmujące testowanie i integrację rozwiązań 5G z uwzględnieniem najnowszych standardów normalizacyjnych.

Wynikami realizacji projektu będą:

- zdefiniowane elementy architektury bezpieczeństwa oraz procedury działania sieci 5G,
- opracowany i przyjęty zestaw narzędzi oraz rekomendacji w zakresie bezpieczeństwa sieci 5G.

Projekt C: „Rozwój kompetencji cyfrowych użytkowników usług komunikacji elektronicznej"

Cel: Podniesienie poziomu kompetencji cyfrowych polskich użytkowników usług komunikacji elektronicznej, ze szczególnym uwzględnieniem uczniów i seniorów. Szerzenie wiedzy o bezpieczeństwie w Internecie jest jednym z zadań państw członkowskich UE wymienionym w Europejskiej Agendzie Cyfrowej. Działania edukacyjne prowadzone przez UKE zostały zgłoszone do Programu Rozwoju Kompetencji Cyfrowych.

Status: projekt realizowany w roku 2025, planowana kontynuacja w roku 2026

Efekty: Ponad 165 tys. uczniów szkół podstawowych wzięło udział w cyklu webinarów obejmujących wybraną tematykę bezpieczeństwa w Internecie („Loguj się bezpiecznie", „Chroń swoje dane w sieci", „Manipulacja w mediach społecznościowych").

Ponad 8 tys. młodych użytkowników sieci i seniorów uczestniczyło w wykładach, szkoleniach i webinarach dotyczących cyberbezpieczeństwa (ochrona danych, ochrona urządzeń, profilaktyka phishingu i spoofingu).

Ponad 1 700 uczestników wzięło udział w zajęciach z kodowania, podczas których dodatkowo rozwijane były umiejętności współpracy w grupie, rozwiązywania problemów, logicznego i twórczego myślenia.

[13] Platforma Lokalizacyjno-Informacyjna z Centralną Bazą Danych (PLI CBD)
[14] Punkt Informacyjny ds. Telekomunikacji (PIT)
[15] Poznańskie Centrum Superkomputerowo-Sieciowe (PCSS)
[16] Naukowa i Akademicka Sieć Komputerowa Państwowy Instytut Badawczy (NASK PIB)

Ostrzeżenia i materiały edukacyjne udostępniane przez UKE w Internecie były wyświetlane prawie 372 tys. razy.

OBSERWOWANE TRENDY I WYZWANIA:

Trend 1: Zmiana wektora nadużyć w komunikacji elektronicznej

Uchwalenie i wdrożenie ustawy o zwalczaniu nadużyć w komunikacji elektronicznej ograniczyło ilość przestępstw dokonywanych za pomocą usług komunikacji interpersonalnej wykorzystujących numery. Odnotowano jednocześnie zwiększoną aktywność przestępców z wykorzystaniem usług komunikacji interpersonalnej niewykorzystujących numerów (np. komunikatory), forów dyskusyjnych, mediów społecznościowych lub komunikacji e-mail, co wymaga szczególnej uwagi w przyszłych pracach związanych mi.in. z kształtowaniem przepisów prawa w tym zakresie.

Trend 2: Rosnąca świadomość użytkowników usług komunikacji elektronicznej

W porównaniu do lat poprzednich, w roku 2025 zaobserwowano wzrost liczby zgłoszeń przesyłanych do UKE przez użytkowników, co należy wiązać nie tylko ze wzrostem ilości nadużyć z wykorzystaniem środków komunikacji elektronicznej oraz wciąż ewoluujących zagrożeń związanych z użyciem usług cyfrowych, ale przede wszystkim z rosnącą świadomością użytkowników końcowych w zakresie cyberbezpieczeństwa i przysługujących im praw.

Trend 3: Rosnący deficyt specjalistów cyberbezpieczeństwa

Na podstawie prowadzonych w UKE procesów rekrutacji, zauważono rosnące trudności w pozyskiwaniu doświadczonych i kompetentnych pracowników, w szczególności z obszaru informatyki i cyberbezpieczeństwa. Sytuacja ta może być spowodowana m.in. niewielką pod względem finansowym atrakcyjnością podmiotów sfery budżetowej, w porównaniu z firmami komercyjnymi oraz aktualnie dużym zapotrzebowaniem występującym na rynku pracy w zakresie specjalistów z tych dziedzin.

REKOMENDACJE NA 2026 - REKOMENDACJE DLA PEŁNOMOCNIKA RZĄDU DS. CYBERBEZPIECZEŃSTWA:

1. Dynamiczna ewolucja technologii informatycznych oraz podążające za nimi zmiany standardów technicznych i aktualizacje przepisów Unii Europejskiej (np. nowelizacja Aktu o sieciach cyfrowych – Digital Networks Act), wskazują na potrzebę regularnego przeglądu i (w miarę potrzeb) aktualizacji prawa krajowego, w tym dotyczącego komunikacji elektronicznej.
2. Wobec rosnącego deficytu doświadczonych i kompetentnych pracowników na rynku pracy, zasadnym wydaje się intensyfikacja różnorodnych działań wprowadzanych na poziomie centralnym, promujących i podnoszących atrakcyjność pracy w sferze budżetowej, z równoległą maksymalizacją konkurencyjności finansowej.

CENTRUM PROJEKTÓW POLSKA CYFROWA (CPPC)

Jednostka podległa ministrowi cyfryzacji.

PODSUMOWANIE ROCZNE:

W 2025 nie odnotowaliśmy żadnych istotnych incydentów związanych z cyberbezpieczeństwem. Usługi DDoS realizowane w ramach umowy z NASK również nie potwierdziły ataków na infrastrukturę.

KLUCZOWE PROJEKTY I INICJATYWY:

Projekt FERC.02.02-IP.01-0001/23 pn. „Cyberbezpieczny Samorząd" Beneficjent: Centrum Projektów Polska Cyfrowa:

Opis projektu: Celem projektu Cyberbezpieczny Samorząd (akronim CS) jest zwiększenie poziomu bezpieczeństwa informacji JST poprzez wzmocnienie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych. Projekt zakłada uruchomienie konkursu grantowego, w którym wnioski o przyznanie grantu mogą złożyć JST na poziomie gminy, powiatu, samorządu województwa. W ramach konkursu przyznane zostaną granty na zakup usług i środków technicznych służących zwiększeniu poziomu cyberbezpieczeństwa JST w obszarach: organizacji, kompetencji i technologii. Projekt identyfikuje podstawowy problem, jakim jest stosowanie w administracji niewystarczających i przestarzałych rozwiązań cyfrowych, w szczególności w obszarze cyberbezpieczeństwa. Realizacja projektu wpłynie na poprawę jakości i efektywności świadczonych usług publicznych. JST usprawnią oraz zwiększą bezpieczeństwo cyfrowych procesów obsługi mieszkańców. W długofalowej perspektywie wpłynie pozytywnie na otwartość i brak wykluczenia mieszkańców, spadek emisji CO2 (zmniejszenie liczby bezpośrednich wizyt w urzędzie) oraz zwiększenie możliwości reagowania w sytuacjach kryzysowych. Projekt zapewni wzrost wiedzy w zakresie cyberbezpieczeństwa i z zakresu wdrażanych w ramach projektu rozwiązań przez kadrę kierowniczą JST i pracowników samorządowych oraz osoby wykonujące zadania w obszarze cyberbezpieczeństwa na rzecz samorządu terytorialnego, zatrudnione w jednostkach organizacyjnych JST, w szczególności osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami KSC.

Projekt KPOD.05.10-IW.06-0001/25 pn. „Cyberbezpieczny Rząd" Beneficjent: Centrum Projektów Polska CyfrowaOpis projektu:

Celem przedsięwzięcia jest poprawa cyberbezpieczeństwa podmiotów KSC, o których mowa w art. 4 pkt 7 UKSC (Dz.U. z 2023 r. poz. 913 z późn. zm.), poprzez udzielenie im wsparcia w formie grantów. Urzędy obsługujące te organy będą uprawnione do otrzymania wsparcia na poprawę odporności na cyberzagrożenia, w tym modernizację i rozbudowę infrastruktury cyberbezpieczeństwa. Wsparcie może również zostać przeznaczone na poprawę odporności na cyberzagrożenia w jednostkach podległych ww. podmiotom i wdrażane będzie z uwzględnieniem 3 obszarów: organizacji, technologii i kompetencji. Docelowo zakłada się, że realizacja przedsięwzięcia, poprzez udzielenie wsparcia w formie grantu, przyczyni się do: wdrożenia lub aktualizacji w podmiotach KSC systemów zarządzania bezpieczeństwem informacji (SZBI), wdrożenia w podmiotach KSC środków zarządzania ryzykiem w cyberbezpieczeństwie, wdrożenia w podmiotach KSC mechanizmów i środków zwiększających odporność na ataki

z cyberprzestrzeni poprzez wzmocnienie zasobów sprzętowych i zakup usług z zakresu cyberbezpieczeństwa, podniesienia poziomu wiedzy i kompetencji personelu podmiotów KSC kluczowego z punktu widzenia wdrożonego SZBI, przeprowadzenia w podmiotach KSC audytów SZBI potwierdzających uzyskanie wyższego poziomu odporności na cyberzagrożenia.

Projekt KPOD.05.10-IW.06-0008/25 pn. Cyberbezpieczne Wodociągi. Beneficjent: Centrum Projektów Polska CyfrowaOpis projektu:

Celem projektu jest poprawa cyberbezpieczeństwa podmiotów KSC, o których mowa w art. 4 pkt 1,7,15 UKSC (Dz.U. z 2024 r. poz. 1077 z późn. zm.), poprzez udzielenie im środków finansowych w formie grantów (pomoc de minimis). Zgodnie z zakresem programu pomocowego oraz zgodnie z Rozporządzeniem Ministra Cyfryzacji z dnia 29.05.2025 r. w sprawie udzielania pomocy de minimis na wsparcie podmiotów prowadzących działalność w zakresie zbiorowego zaopatrzenia w wodę objętych KSC, w ramach Krajowego Planu Odbudowy i Zwiększania Odporności pomoc de minimis może zostać udzielona podmiotowi prowadzącemu działalność w zakresie zbiorowego zaopatrzenia w wodę objętemu KSC, wykorzystującemu technologie operacyjne w przemysłowych systemach sterowania. Realizacja projektu przyczyni się do zwiększenia poziomu bezpieczeństwa informacji poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w podmiotach KSC.

SŁUŻBY SPECJALNE

AGENCJA WYWIADU (AW)

Szczegóły podejmowanych przedsięwzięć zamieszczono w części niejawnej Sprawozdania.

AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO (ABW)

Jawne informacje dot. działalności ABW w cyberprzestrzeni zawarte zostały w rozdziale CSIRT GOV. Natomiast **szczegóły podejmowanych przedsięwzięć zamieszczono w części niejawnej niniejszego Sprawozdania.**

SŁUŻBA WYWIADU WOJSKOWEGO (SWW)

Szczegóły podejmowanych przedsięwzięć zamieszczono w części niejawnej Sprawozdania.

CENTRALNE BIURO ANTYKORUPCYJNE (CBA)

Informacje dot. działalności CBA w cyberprzestrzeni zawarte zostały w rozdziale CENTRALNE BIURO ANTYKORUPCYJNE

SŁUŻBA KONTRWYWIADU WOJSKOWEGO (SKW)

PODSUMOWANIE ROCZNE:

Służba Kontrwywiadu Wojskowego, w zakresie swojej ustawowej właściwości, prowadzi szereg działań na rzecz bezpieczeństwa resortu obrony narodowej (RON), państwa oraz krajów sojuszniczych. Działania w cyberprzestrzeni są częścią szerszej działalności Służby i realizowane są, w zależności od ich charakteru, przez właściwe jednostki organizacyjne SKW.

W 2025 roku SKW, samodzielnie lub też współdziałając z podmiotami krajowymi oraz partnerskimi służbami specjalnymi, podejmowała szereg działań mających na celu eliminowanie zagrożeń o charakterze szpiegostwa i cyberszpiegostwa dla podmiotów krajowych oraz sojuszniczych.

NAJWAŻNIEJSZE ZAGROŻENIA:

Do najpoważniejszych zagrożeń należy zaliczyć działania w cyberprzestrzeni prowadzone przez rosyjskie służby specjalne oraz grupy z nimi powiązane i nadzorowane. Na szczególną uwagę zasługuje 85. Główne Centrum Zadań Specjalnych (85th GTsSS) Głównego Zarządu Wywiadowczego (JW. 26165), które jest zaangażowane w prowadzenie wielopoziomowych, skomplikowanych operacji w zakresie cyberszpiegostwa.

Trend 1: Socjotechnika (inżynieria społeczna)

W bieżącym okresie sprawozdawczym odnotowywano utrzymującą się wysoką ilość prób ataków phishingowych (w tym wykorzystujących wysoko wyspecjalizowane techniki i metody).
Najliczniejszą grupę ataków socjotechnicznych stanowiły ataki wymierzone w użytkowników komunikatorów SIGNAL oraz WhatsApp, stanowiące próbę kompromitacji kont personelu resortu obrony narodowej. Z wysokim prawdopodobieństwem ocenia się, że aktywność w obszarze ataków na szyfrowane komunikatory będzie nadal obserwowana.
Równolegle obserwowane były kampanie phishingowe o charakterze szpiegowskim z wykorzystaniem technik impersonacji oficerów SZ RP. Celem tych działań było pozyskanie informacji od personelu NATO dotyczących organizowanych ćwiczeń wojskowych w ramach Sojuszu. Z wysokim prawdopodobieństwem można założyć kontynuację tej kampanii w najbliższym okresie.

Trend 2: Wykorzystywanie infrastruktury anonimizacyjnej opierającej się na urządzeniach sieciowych typu SOHO w atakach cybernetycznych realizowanych przez aktorów państwowych.

Grupy APT wykorzystują rozproszoną infrastrukturę anonimizacyjną opartą na skompromitowanych domowych oraz biurowych urządzeniach sieciowych jako warstwę pośrednią do prowadzenia operacji cybernetycznych. Urządzenia tej klasy często działają latami bez nadzoru, z przestarzałym oprogramowaniem, domyślną konfiguracją lub znanymi podatnościami w usługach zdalnego zarządzania. W praktyce wiele z nich nie jest w terminie aktualizowane, a część producentów kończy wsparcie szybciej niż cykl życia sprzętu, co sprzyja trwałej kompromitacji i utrzymywaniu dostępu. Wykorzystanie takiej infrastruktury utrudnia identyfikację sprawców oraz jednoznaczną atrybucję incydentów. Ruch sieciowy jest maskowany poprzez wielowarstwowe pośrednictwo, a źródłowe adresy IP odpowiadają legalnym węzłom zlokalizowanym w wielu państwach. Dodatkowo możliwość rotacji węzłów i dynamicznej zmiany tras routingu ogranicza skuteczność korelacji zdarzeń i analiz śledczych.

Trend 3: Nieprzestrzeganie przepisów, procedur

W 2025 roku obserwowano stale utrzymującą się dużą ilość incydentów dotyczących naruszenia przepisów prawa i procedur. Świadczyć to może o braku świadomości wśród pracowników odnośnie postępowania z informacjami podczas przenoszenia ich pomiędzy systemami o różnych klauzulach, braku świadomości o zagrożeniach dla systemów w przypadku wykorzystywania oprogramowania innego niż dopuszczane do pracy w danym systemie.

REKOMENDACJE NA 2026 REKOMENDACJE DLA PEŁNOMOCNIKA RZĄDU DS. CYBERBEZPIECZEŃSTWA:

Podjęcie prac legislacyjnych w zakresie umożliwienia ustaleń telekomunikacyjnych połączeń zagranicznych adresów IP wykorzystywanych wyłącznie przez grupy APT do puli adresów IP polskich operatorów telekomunikacyjnych.

Szczegóły podejmowanych przedsięwzięć zamieszczono w części niejawnej Sprawozdania.

ZWALCZANIE CYBERPRZESTĘPCZOŚCI

PROKURATURA KRAJOWA (PK)

PODSUMOWANIE ROCZNE:

Rozwój nowoczesnych technologii informacyjno-komunikacyjnych, dostępność środków komunikowania się na odległość i związany z tym rozwój elektronicznych usług wpłynął na sposoby działania sprawców przestępstw skierowanych przeciwko różnym dobrom prawnie chronionym. Z technologii teleinformatycznych korzystają zarówno sprawcy popełniający przestępstwa tradycyjne znajdujące się pod ochroną prawa karanego, jak również ci, którzy przeprowadzają zamachy skierowane na systemy, przetwarzane i utrzymywane w nich dane. Ponieważ większość z obserwowanych w Polsce cyberprzestępstw to przestępstwa nakierowane na monetyzację, skuteczna walka z cyberprzestępcami wymaga analizy przepływów finansowych (*follow the money*). Dlatego też, szybkie uzyskanie przez organy procesowe dowodów: w tym dowodów cyfrowych i informacji objętych tajemnicą bankową, znacząco wpłynie na skuteczność postępowań karnych, umożliwiając sprawne działania wykrywcze, ograniczając bezkarność sprawców przestępstw i eskalację zjawiska.

KLUCZOWE PROJEKTY I INICJATYWY:

Projekt A: Organizacja szkoleń

Organizacja powszechnych szkoleń online w zakresie tematyki zwalczania cyberprzestępczości prowadzonych przez prokuratorów Departamentu do Spraw Cyberprzestępczości i Informatyzacji oraz podmioty współdziałające - w 2025 r. zorganizowano szkolenia, w których udział wzięło łącznie ponad 10 tysięcy osób (prokuratorów oraz funkcjonariuszy Policji)

Projekt B: Nadzór i koordynacja postępowań karnych

- nadzorowanie przez prokuratorów Departamentu do Spraw Cyberprzestępczości i Informatyzacji najpoważniejszych śledztw dotyczących cyberprzestępczości, łącznie nadzorowano w 2025 r. 155 postępowań w kraju dotyczących cyberprzestępczości (rejestr Dsn);
- koordynacja postępowań w zakresie cyberprzestępczości w celu zmniejszenia ilości prowadzonych spraw o ten sam czyn, poprzez ich łączenie w postępowania zbiorcze, w zakresie fałszywych platform internetowych (art. 286 § 1 k.k., art. 178 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi) czy kaskadowych alarmów bombowych (art. 224a k.k.)

Projekt C: Rozwój narzędzi informatycznych

Rozwój narzędzi informatycznych i budowa nowych funkcjonalności mających na celu ułatwienie i przyspieszenie pozyskiwania informacji niezbędnych w postępowaniach karnych czy lepsze zarządzanie zasobem informacyjnym, w szczególności prowadzone prace wspólnie z Policją nad budową modułu do wymiany danych pomiędzy systemami PROK-SYS a ERCDŚ, podłączenie do systemu prokuratury PROK-SYS rejestru zewnętrznego - Systemu Informacji Finansowej (SInF).

OBSERWOWANE TRENDY I WYZWANIA:

Wyzwanie 1: Informatyzacja postępowania karnego

Opis: Jednym z najważniejszych działań jakie należy podjąć to zmiany legislacyjne umożliwiających wprowadzenie do kodeksu postępowania karnego **elektronicznej formy czynności procesowych**, w tym prawnie skutecznego podpisywania decyzji procesowych **podpisem elektronicznym**. Niezbędne jest zatem wprowadzenie przepisów odnoszących się do elektronicznej formy decyzji procesowych, dokumentowania czynności procesowych, komunikowania się uczestników postępowania z organami procesowymi, jak również komunikowania się organów procesowych z innymi uczestnikami postępowania karnego. Konsekwencją wprowadzenia elektronicznej formy czynności procesowych winno być także, wprowadzenie równoważności pomiędzy aktami tradycyjnymi/papierowymi, a aktami elektronicznymi w tym również hybrydowymi (zwierającymi zarówno dokumenty w formie papierowej jak i elektronicznej). Z punktu widzenia procesowego miałoby to istotne znaczenie dla dynamiki i sprawności prowadzonych postępowań karnych, w szczególności w sprawach z zakresu cyberprzestępczości. Rozwiązania legislacyjne, jakie należy przyjąć, dotyczące elektronicznej formy czynności procesowej, powinny uwzględniać także uregulowania zawarte na poziomie Unii Europejskiej, w tym w art. 3 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/2844 z dnia 13 grudnia 2023 r. w sprawie cyfryzacji współpracy sądowej i dostępu do wymiaru sprawiedliwości w sprawach cywilnych i handlowych o charakterze transgranicznym oraz współpracy wymiarów sprawiedliwości i dostępu do wymiaru sprawiedliwości w sprawach karnych o charakterze transgranicznym oraz zmieniające niektóre akty w tych dziedzinach (Dz. U. UE. L. z 2023 r. poz. 2844), dotyczące obligatoryjnej komunikacji przy przekazywaniu odezw i dokumentów między organami z poszczególnych krajów członkowskich UE poprzez zdecentralizowany system informatyczny, przy wykorzystaniu środków identyfikacji elektronicznej i elektronicznych usług zaufania, do których odwołuje się to rozporządzenie.

Wyzwanie 2: Wzmocnienie wyspecjalizowanych struktur zwalczania cyberprzestępczości w prokuraturze

W zakresie zwalczania cyberprzestępczości, zwrócić należy szczególną uwagę na potrzebę stworzenia wyspecjalizowanego zasobu kadrowego, który będzie zajmować się zwalczeniem tego rodzaju przestępczości oraz wyposażenie pionu zwalczania cyberprzestępczości w niezbędne narzędzia służące do zbierania i analizowania dowodów, w tym elektronicznych, w toku prowadzonych postępowań karnych. Aktualnie postępowania dotyczące cyberprzestępczości pozostają w szczególnym zainteresowaniu Departamentu do Spraw Cyberprzestępczości i Informatyzacji Prokuratury Krajowej i są monitorowane lub nadzorowane przez prokuratorów tego departamentu. Z uwagi na rozwój nowoczesnych technologii i związane z nim pojawianie się nowych podatności, wektorów ataków, usług elektronicznych wykorzystywanych w przestępczym procederze, czy w końcu, nowych sposobów działania sprawców, niezbędne jest ustawiczne kształcenie zarówno kadr sądownictwa, prokuratury oraz policji oraz tworzenie wyspecjalizowanych komórek organizacyjnych do spraw cyberprzestępczości.

DANE LICZBOWE (STATYSTYKI) DOT. PROWADZONEJ DZIAŁALNOŚCI

Tabela 45. DANE LICZBOWE (STATYSTYKI) DOT. PROWADZONEJ DZIAŁALNOŚCI PK

Przepis	Zar. spraw	Odm. wszczęcia	Umorzenia NN (niewykrycie sprawcy przestępstwa)	Umorzenia pozostałe (art. 17 § 1 pkt 1 do 11 k.p.k., warunkowe umorzenie postępowania, wniosek o umorzenie - art. 324 k.p.k.)	Akt oskarżenia (oraz wnioski o wyrok skazujący art. 335 § 1 k.p.k.)
art. 287 kk (oszustwo komputerowe)	10879	1793	7515	979	584
art. 267 kk (bezprawne uzyskanie informacji)	17542	5764	8218	2633	677
art. 268 kk (utrudnianie zapoznania się z informacją)	536	162	215	119	37
art. 268a kk (niszczenie danych informatycznych)	1746	613	945	165	49
art. 269 kk (uszkodzenie danych informatycznych)	36	6	12	5	6
art. 269a kk (uszkodzenie systemu informatycznego)	121	24	53	16	9
art. 269b kk (wytwarzanie oprogramowania i narzędzi do popełniania przestępstw)	122	9	44	13	32
art. 200a kk (uwodzenie małoletniego w sieci)	899	90	178	250	261
art. 202 § 3 kk (rozpowszechnianie twardej pornografii)	581	46	71	99	235
art. 202 § 4 kk (utrwalanie pornografii z udziałem małoletniego)	170	17	15	58	79
art. 202 § 4a kk (posiadania pornografii dziecięcej)	758	27	71	217	380
art. 286 kk (oszustwo, na podstawie danych Policji, można szacować, iż 50% spraw z zakresu 286 kk dotyczy cyberprzestępczości, w zestawieniu są wszystkie sprawy z art. 286 kk)	163456	34307	65570	29288	18194
art. 190a § 2 kk (kradzież tożsamości)	9100	3204	2751	1268	831
art. 29, 30, 31, 32 ustawy z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (generowanie sztucznego ruchu, smishing, CLI Spoofing, niezgodną z prawem modyfikację informacji adresowej)	867	60	878	34	24

***dane wygenerowano wg stanu bazy danych PROK-SYS na dzień 2026-01-21**

****przy generowaniu danych zastosowano zasadę iż każda sprawa jest liczona tylko jeden raz (w przypadku ponownej rejestracji np: w wyniku podjęcia umorzenia nie jest ona uwzględniana, filtr Następna sprawa - pusty)**

ANALIZA I OCENA FUNKCJONOWANIA KSC:

Z punktu widzenia prokuratury Strategia KSC poprawia warunki reagowania na incydenty, jednak ich skuteczność w obszarze ścigania nadal jest ograniczona. W praktyce komunikacja w ramach KSC działa przede wszystkim na płaszczyźnie technicznej: szybkie zgłoszenie, analiza, ograniczenie skutków i przywrócenie działania systemów. Dla prokuratury kluczowe jest natomiast, aby równolegle

zapewnienie zabezpieczenia materiału dowodowego w sposób umożliwiający jego wykorzystanie w postępowaniu karnym.

W zakresie komunikacji największym problemem pozostaje brak jednolitego standardu przekazywania informacji pomiędzy CSIRT a organami ścigania. Dane o incydencie często są przekazywane w formie użytecznym operacyjnie, ale niepełnym procesowo – bez odpowiedniego kontekstu, dokumentacji działań czy zachowania łańcucha dowodowego. W efekcie nawet szybka reakcja CSIRT nie zawsze przekłada się na szybkie wszczęcie skutecznych czynności procesowych.

Z perspektywy czasu reakcji strategie realnie skracają czas podjęcia działań technicznych, natomiast nie rozwiązują problemu czasu zabezpieczenia dowodów. W cyberprzestępczości dowody są ulotne, a działania naprawcze podejmowane w trybie pilnym (np. reinstalacje, reset haseł, odtwarzanie systemów) mogą prowadzić do utraty kluczowych śladów/dowodów.

REKOMENDACJE NA 2026 - REKOMENDACJE DLA PEŁNOMOCNIKA RZĄDU DS. CYBERBEZPIECZEŃSTWA:

Zapewnienie kompleksowego ekosystemu regulacji odnoszących się do zwalczania cyberprzestępczości, zabezpieczenia elektronicznego materiału dowodowego - w zakresie proponowanych zmian legislacyjnych w pierwszej kolejności należy zwrócić uwagę na konieczność pilnej zmiany **przepisu art. 106a ustawy z dnia 29 sierpnia 1997 r. Prawo Bankowe**, **w zakresie trybu pozyskiwania przez prokuratora informacji stanowiących tajemnicę bankową** w toku prowadzonego postępowania przygotowawczego w fazie in rem. Celowe jest umożliwienie żądania danych objętych tajemnicą bankową **jedynie na podstawie postanowienia prokuratora**, bez udziału właściwego miejscowo sądu okręgowego. Proponowana zmiana w znaczący sposób wpłynęłaby na skuteczność prowadzonych postępowań, koncentrację materiału dowodowego, w szczególności we wstępnej fazie prowadzonego śledztwa czy dochodzenia, które co do zasady prowadzone jest w fazie in rem. Konieczne jest również określenie **obowiązków banków i innych instytucji finansowych** w zakresie retencjonowania oraz przekazywania informacji i danych dotyczących prowadzonych rachunków bankowych i innych usług oraz produktów za pośrednictwem zdalnych kanałów dostępowych (sieci Internet). W informacjach przekazywanych przez banki, niejednokrotnie brakuje informacji o porcie przypisanym do ustalonego adresu IP. Tak przekazana informacja, uniemożliwia organom ścigania ustalenie sprawcy czynu zabronionego, gdyż informacja o adresie IP bez portu, wskazuje nam na dane wielu osób, które korzystały z danego publicznego adresu IP w ustalonej jednostce czasu. Tym samym należałoby wprowadzić obowiązek dla instytucji finansowych (w tym banków) gromadzenia również informacji o portach przypisanych do ustalonego adresu IP, co znacząco wpłynęłoby na możliwości wykrywcze w toku prowadzonych postępowań przygotowanych. Celowe jest również podjęcie prac legislacyjnych mających na celu umożliwienie prokuratorom prowadzącym postępowania karne (w tym dotyczących oszustw na pozagiełdowym rynku forex) **blokowania stron internetowych**, za pośrednictwem których przestępcza działalność jest prowadzona. Obecnie w polskiej procedurze karnej brak jest przepisu mówiącego wprost o takiej możliwości. Niezbędne są również przepisy odnoszące się do egzekwowania **odpowiedzialności finansowej platform internetowych**, za których pośrednictwem rozpowszechniana są naruszające prawo reklamy. Konieczna jest też dalsza ewolucja przepisów przeciwdziałających kradzieży tożsamości w szczególności **w zakresie weryfikowania tożsamości klienta bez jego fizycznej obecności** przy zastosowaniu środków identyfikacji elektronicznej przy zawieraniu transakcji i korzystaniu z nowych produktów finansowych oraz rejestracji przedpłaconych kart SIM. Aktualne przepisy dotyczące rejestracji kart SIM, przy realnym braku weryfikacji tożsamości dysponenta czy zakazu dalszego obrotu zarejestrowanymi kartami sprawiają, że cel regulacji nie został osiągnięty.

CENTRALNE BIURO ZWALCZANIA CYBERPRZESTĘPCZOŚCI (CBZC)

PODSUMOWANIE ROCZNE:

Najpoważniejsze zagrożenia w cyberprzestrzeni jakie w 2025 roku odnotowano to ataki ransomware, ataki DDoS oraz oszustwa internetowe (nigeryjskie, inwestycyjne, "na pracownika banku"). W 2025 roku odnotowano wzrost wszczętych postępowań przygotowawczych dot. przestępstw z wykorzystaniem złośliwego oprogramowania typu ransomware (118), w stosunku do 103 postępowań wszczętych w 2024 roku. Zarejestrowano wzrost aktywności grup przestępczych motywowanych finansowo, często działających w ramach międzynarodowej przestępczości zorganizowanej takich jak Qilin, Akira czy BlackField. Odnotowano również wzrost internetowych oszustw stanowiących największą część wszystkich zarejestrowanych zdarzeń.

KLUCZOWE PROJEKTY I INICJATYWY:

Projekt „Cropt"

Utworzenie zespołów specjalistów cyberbezpieczeństwa działających lokalnie i wspierających podmioty krajowego systemu cyberbezpieczeństwa w obsłudze incydentów i odzyskiwaniu danych, oraz prowadzenie działań podnoszących świadomość o cyberbezpieczeństwie w ramach Krajowego Planu Odbudowy i Zwiększania Odporności (KPO). Liderem ww. projektu jest NASK, a jego realizacja zostanie przeprowadzona w latach 2024-2026.

Opis (cel, status, efekty): . Głównym celem projektu jest stworzenie zespołów tzw. szybkiego reagowania na incydenty, przy jednoczesnym poszerzeniu wiedzy i umiejętności policjantów CBZC, oraz ich wyposażenie w wysokiej jakości sprzęt.

OBSERWOWANE TRENDY I WYZWANIA:

Trend 1: Ransomware

Ransomware to jeden z najpoważniejszych i najszybciej rozwijających się rodzajów cyberprzestępczości. Ataki te dotyczą zarówno osób prywatnych, jak i firm, instytucji publicznych oraz infrastruktury krytycznej. Ataki te obecnie wykraczają poza samo szyfrowanie danych, a sprawcy w celu wywarcia dodatkowej presji na pokrzywdzonego, wykradają poufne dane i grożą publikacją tych danych, często na stronach w sieci TOR. W Europie, w tym w Polsce, ransomware należy do najczęściej zgłaszanych incydentów cyberbezpieczeństwa w sektorze prywatnym i publicznym. Szczególnie narażone są małe i średnie przedsiębiorstwa oraz szpitale i samorządy, które często nie dysponują wystarczającymi zasobami na zaawansowaną ochronę IT. Jednym z kluczowych trendów jest tzw. podwójne, a nawet potrójne wymuszenie. Oprócz szyfrowania danych przestępcy kradną je i grożą publikacją, a czasem także atakami DDoS lub informowaniem klientów i partnerów ofiary. Kolejnym trendem jest model „ransomware as a service" (RaaS), w którym twórcy złośliwego oprogramowania udostępniają je innym przestępcom w zamian za udział w zyskach. Znacznie obniża to próg wejścia do cyberprzestępczości i zwiększa liczbę ataków. Coraz częściej obserwuje się również precyzyjnie ukierunkowane ataki. Zamiast

masowych kampanii e-mailowych, przestępcy prowadzą rozpoznanie ofiary, wykorzystują luki w usługach zdalnego dostępu, phishing lub przejęte konta, aby maksymalizować presję i wysokość okupu.

Trend 2: Oszustwa inwestycyjne

Oszustwa inwestycyjne to jedna z najszybciej rosnących form przestępczości finansowej. Polegają na wyłudzaniu środków pod pozorem inwestycji obiecujących ponadprzeciętne, „pewne" zyski przy niskim lub zerowym ryzyku. Sprawcy wykorzystują niewiedzę, emocje oraz presję czasu, a rozwój technologii znacząco ułatwił im dotarcie do ofiar. W Polsce, liczba zgłoszeń rośnie z roku na rok, a realna skala problemu jest prawdopodobnie większa – część ofiar nie zgłasza spraw z powodu wstydu lub niskiej wiary w odzyskanie środków. Ofiarami padają zarówno osoby młode, kuszone nowymi technologiami i kryptowalutami, jak i seniorzy, którzy często tracą oszczędności życia. Po pierwsze, dynamiczny wzrost oszustw opartych na kryptowalutach i rzekomych platformach tradingowych. Fałszywe aplikacje i strony internetowe do złudzenia przypominają legalne serwisy, pokazując fikcyjne zyski, aby zachęcić do dalszych wpłat.

Po drugie, coraz powszechniejsze jest wykorzystanie mediów społecznościowych. Reklamy z udziałem spreparowanych wizerunków znanych osób, fałszywe rekomendacje „ekspertów" czy grupy inwestycyjne na komunikatorach budują pozory wiarygodności.

Po trzecie, oszuści stosują zaawansowane techniki socjotechniczne, takie jak indywidualny „opiekun inwestycyjny", codzienne telefony, presja natychmiastowej decyzji oraz stopniowe zwiększanie zaangażowania finansowego ofiary. Coraz częściej pojawia się też tzw. „recovery scam", czyli ponowne oszustwo polegające na obietnicy odzyskania utraconych środków za dodatkową opłatą.

ANALIZA I OCENA FUNKCJONOWANIA KSC:

CBZC jest w bieżącym kontakcie z krajowymi Zespołami Reagowania na Incydenty Krytyczne poziomu krajowego (NASK, GOV i MON) oraz z CSIRTAMI sektorowymi takimi jak UKNF. Informacje pozyskane z CSIRTÓW są na bieżąco przekazywane do właściwych komórek organizacyjnych CBZC. Współdziałanie w zakresie incydentów będących zarazem przestępstwami, zgłaszanie witryn scam, weryfikacja zgłoszeń.

Naczelnik WOC pełni funkcję oficera łącznikowego z Departamentem Cyberbezpieczeństwa Ministerstwa Cyfryzacji i bierze udział w cotygodniowych spotkaniach PCOC przy Pełnomocniku Rządu ds. cyberbezpieczeństwa.

Powyższe wpływa na skuteczne i efektywne podejmowanie czynności służbowych przez funkcjonariuszy CBZC i zmniejsza czas reakcji organów ścigania i podmiotów działających w trybie KSC do reagowania na incydenty w cyberprzestrzeni.

CENTRALNE BIURO ANTYKORUPCYJNE (CBA)

PODSUMOWANIE ROCZNE:

Centralne Biuro Antykorupcyjne w 2025 roku realizowało działania o szerokim spektrum, przeciwdziałające zagrożeniom cyberprzestępczości oraz zagrożeniom cyberbezpieczeństwa. Przedsięwzięcia te skupiały się na działaniach analityczno-informacyjnych, kontrolnych oraz teleinformatycznych.

CBA w zakresie cyberbezpieczeństwa zrealizowało w ostatnim roku następujące zadania:

- udział w posiedzeniach Zespołu ds. Koordynacji Cyberbezpieczeństwa, zarówno stacjonarnie, jak i za pośrednictwem PCOC;
- ścisła współpraca CSIRT CBA z CSIRT GOV, obejmująca m.in. zgłaszanie IoC (ang. Indicator of Compromise) dotyczących aktów teleinformatycznych skierowanych na CBA oraz wdrażanie zaleceń CSIRT GOV;
- wykonywanie audytów i testów bezpieczeństwa systemów teleinformatycznych funkcjonujących w CBA;
- realizacja szkoleń wewnętrznych podnoszących świadomość funkcjonariuszy i pracowników w zakresie profilaktyki bezpieczeństwa teleinformatycznego;
- zwiększenie kompetencji kadry realizującej zadania z zakresu bezpieczeństwa teleinformatycznego i utrzymania systemów teleinformatycznych poprzez udział w szkoleniach i konferencjach specjalistycznych;
- współpraca z sektorem prywatnym w celu zapewnienia bezpieczeństwa usług internetowych, takich jak hosting czy usługi pocztowe.
- Ponadto, podobnie jak w latach ubiegłych, CBA konsekwentnie dąży do uniezależnienia się od konieczności zlecania prac związanych z budową krytycznych systemów teleinformatycznych firmom zewnętrznym, poprzez osiągnięcie samodzielności w tym zakresie.

KLUCZOWE PROJEKTY I INICJATYWY:

Projekt A: Spotkania eksperckie

Organizacja spotkań eksperckich i konferencji pionów teleinformatycznych służb specjalnych. Celem tych wydarzeń jest transfer wiedzy i wymiana doświadczeń w zakresie wytwarzania narzędzi teleinformatycznych, wdrażania technologii sztucznej inteligencji oraz rozwiązań wspierających realizację ustawowych zadań służb specjalnych, ze szczególnym uwzględnieniem wyzwań cyberbezpieczeństwa.

Wynikiem spotkań ekspertów IT służb specjalnych jest usystematyzowanie wiedzy z zakresu IT i najnowszych trendów w wytwarzaniu oprogramowania, a także opracowanie mechanizmów implementacji i wdrożenia zasad działania AI w narzędziach wytwarzanych przez te instytucje. Konferencje przynoszą pozytywne efekty w zakresie wymiany doświadczeń oraz zacieśnienia współpracy w strategicznych obszarach podejmowanych działań.

Projekt B: Narzędzia teleinformatyczne

Wytwarzanie narzędzi teleinformatycznych, systemów, aplikacji i usług na potrzeby Jednostek Organizacyjnych CBA. Budowane i dostarczane narzędzia teleinformatyczne umożliwiają jednostkom CBA realizację ustawowych zadań Biura, dzięki czemu Służba może skutecznie przeciwdziałać przestępstwom godzącym w interes ekonomiczny Państwa, co ma bezpośredni wpływ na obronność i bezpieczeństwo kraju. Usługi dostarczane przez CBA są budowane zgodnie z najnowszymi trendami technologicznymi, posiadają wbudowane mechanizmy cyberbezpieczeństwa oraz zapewniają rozliczalność i audyt przetwarzanych danych. Narzędzia budowane w CBA są udostępniane również innym służbom specjalnym, co wzmacnia potencjał wiedzy oraz podnosi poziom bezpieczeństwa usług w sferze resortowej.

ANALIZA I OCENA KSC:

W ocenie CBA KSC w 2025 roku znajdował się w fazie intensywnego wzmacniania, zarówno legislacyjnego (wdrażanie NIS2, nowelizacja UKSC, przygotowanie systemu certyfikacji), jaki organizacyjnego (rozwój CSIRT krajowych i sektorowych). Skuteczność komunikacji koordynacji była systemowo wzmacniana, a czas reakcji na incydenty, dzięki cyklicznym posiedzeniom Zespołu ds. Koordynacji Cyberbezpieczeństwa, był w dużej mierze wystarczający do podjęcia odpowiednich działań.

INNE INSTYTUCJE WSPÓŁTWORZĄCE KSC

SŁUŻBA OCHRONY PAŃSTWA (SOP)

PODSUMOWANIE ROCZNE:

W Służbie Ochrony Państwa cyberbezpieczeństwo traktowane jest jako priorytet strategiczny. Systemy informatyczne SOP działają w głównej mierze w zamkniętym środowisku, co powoduje zmniejszenie ryzyka np. na ataki typu ransomware, phishing oraz prób nieautoryzowanego dostępu. W ostatnim roku nie odnotowano znacznego wzrostu prób naruszeń bezpieczeństwa. Dzięki wprowadzonym w SOP procedurom monitoring, informacjom z CSiRT GOV a także szybkiej reakcji na zaistniałe incydenty SOP miało możliwość na działania uniemożliwiające doprowadzenie do szkód operacyjnych i wizerunkowych firmy. Funkcjonariusze i pracownicy SOP są objęci programem szkoleń w zakresie świadomości cyberzagrożeń. Współpraca z zespołem reagowania na incydenty CSIRT GOV zapewnia szybkie reagowanie na nowe zagrożenia i aktualizacje zabezpieczeń.

KLUCZOWE PROJEKTY I INICJATYWY:

Służba Ochrony Państwa realizuje zadania/projekty z zakresu rozwoju własnych istotnych systemów informatycznych. Służba Ochrony Państwa nie realizuje zadań/projektów związanych z usługami dla obywatela będącymi elementem cyfryzacji administracji.

OBSERWOWANE TRENDY I WYZWANIA:

Trend 1: Braki kadrowe

Istotnym problemem w 2025 roku było pozyskanie do Służby Ochrony Państwa specjalistów z branży IT w szczególności w obszarze cyberbezpieczeństwa oraz programowania.

Trend 2: Spear Phishing

Służba Ochrony Państwa w 2025 r. otrzymała i przeanalizowała około 600 podejrzanych maili pod względem możliwości wyłudzenia danych mogących posłużyć do uzyskania dostępu do zasobów SOP. Służba Ochrony Państwa zauważa, że jest to zjawisko problematyczne i stanowi jedno z większych zagrożeń w cyberbezpieczeństwie dla systemów informatycznych SOP.

ANALIZA I OCENA FUNKCJONOWANIA KSC:

KSC należy ocenić pozytywnie, ponieważ system ten w znaczący sposób wzmacnia bezpieczeństwo państwa, instytucji publicznych oraz obywateli w przestrzeni cyfrowej. W dobie rosnącej liczby cyberataków jego rola ma charakter strategiczny. Dzięki informacjom przekazywanym przez CSiRT GOV jako wyspecjalizowany zespół możliwe jest szybkie i skuteczne reagowanie na ataki co zwiększa odporność wykorzystywanej przez Służbę Ochronny Państwa infrastruktury.

RADA DO SPRAW CYFRYZACJI (RDC)

O RADZIE

Zgodnie z art. 17 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne przy ministrze właściwym do spraw informatyzacji działa RDC, która jest organem opiniodawczo-doradczym.

RDC jest „think-tankiem", którego członkowie wspierają swoją wiedzą i doświadczeniem Ministra Cyfryzacji oraz Komitet do Spraw Cyfryzacji. Rada opiniuje dokumenty strategiczne (projekty i programy rozwoju) oraz inne dokumenty związane z działalnością resortu cyfryzacji. Rada składa się z minimum 15 członków, którzy reprezentują administrację publiczną, organizacje pozarządowe, sektor gospodarki cyfrowej oraz środowiska naukowe i eksperckie. Istotnym elementem w działaniach Rady jest praca zespołowa i dobre relacje z szerokim gronem interesariuszy, w tym m.in. współpraca z organizacjami pozarządowymi. W ramach działań Rady przedstawiciele organizacji pozarządowych mogą być zapraszani do przedstawienia swoich opinii na forum Rady.

Podczas posiedzeń Rady uczestnicy prezentują swoje poglądy niezależnie od stanowiska instytucji, w której pracują. Działalność Rady jest wartością dodaną do działań podejmowanych w zakresie cyfryzacji kraju zarówno w Ministerstwie Cyfryzacji, jak również w innych resortach. Głównym nurtem działań Rady jest generowanie nowych pomysłów, które mogą być realizowane przez Ministerstwo Cyfryzacji. Prowadzone przez Radę prace mają przede wszystkim wymiar projektowy. Wielosektorowy i wielopodmiotowy potencjał Rady, a także otwarta na współpracę z interesariuszami formuła pracy pozwala agregować wiedzę i trendy z różnych środowisk.

PODSUMOWANIE

W 2025 roku Rada V kadencji zebrała się na dziesięciu posiedzeniach. Podczas trzech posiedzeń Rady, których tematyka koncentrowała się na kwestiach z zakresu cyberbezpieczeństwa zostały omówione poniższe zagadnienia:

- Projekt Strategii Cyberbezpieczeństwa RP 2025-2029;
- Systemowe wsparcie w zakresie cyberbezpieczeństwa dla sektora naukowobadawczego:
    - Przedstawienie skali problemu na podstawie dostępnych danych z raportów firm analitycznych, wniosków z rozmów przeprowadzonych z przedstawicielami pionów IT/cyber uczelni (2024/2025) i debaty na temat bezpieczeństwa badań w kontekście nowego Programu Ramowego FP 10;
    - Wnioski z badań potrzeb dot. budowania kompetencji w zakresie cyberbezpieczeństwa pionów IT uczelni (2023);
    - Nowe obowiązki uczelni wynikające z NIS2/KSC 2.0 i problem zapewnienia finansowania na realizację tych obowiązków, działania KRASP;
    - Wsparcie działań na rzecz rozwoju rozwiązań dla bezpieczeństwa sieci i systemów ICT, w tym inwestycje w R&I dla cyberbezpieczeństwa i
    - kształcenie zaawansowanych kadr oraz badań podstawowych w obszarze
        - AI, cyberbezpieczeństwa i innych technologii ICT w kontekście dyskusji o FP 10;
    - Krajobraz cyberzagrożeń dla sektora naukowo-badawczego w Polsce.
- Dostęp do Informacji Publicznej – wyzwania w kontekście cyberbezpieczeństwa;
- Informacja w sprawie prac prowadzonych w Ministerstwie Finansów w kontekście cyberbezpieczeństwa.

RDC w 2025 r. wydała następujące stanowiska obejmujące tematykę cyberbezpieczeństwa, które przedstawiam jako rekomendację na rok 2026 dla Pełnomocnika Rządu ds. Cyberbezpieczeństwa:

- Stanowisko Rady do Spraw Cyfryzacji dotyczące konieczności systemowego wsparcia cyberbezpieczeństwa sektora naukowobadawczego w Polsce.
- Stanowisko Rady do Spraw Cyfryzacji w sprawie cyberbezpieczeństwa w sektorze medycznym.

KOMENDA GŁÓWNA STRAŻY GRANICZNEJ (KGSG)

PODSUMOWANIE ROCZNE:

Ogólny stan zagrożeń w zakresie cyberbezpieczeństwa w bieżącym roku nie uległ istotnym zmianom w stosunku do roku poprzedniego. Stale obserwowane są próby ingerencji i przełamania zabezpieczeń występujących w infrastrukturze teleinformatycznej Straży Granicznej.

Obszarami szczególnej ochrony są usługi wystawione na zewnątrz tj:

- Poczta elektroniczna;
- Portal SG.

Wśród takich prób możemy wyróżnić m.in.:

- ataki typu odmowa dostępu wykrytych i zablokowanych w systemach Straży Granicznej,
- skanowanie zasobów Straży Granicznej widocznych w sieci Internet - ataki poprzez pocztę elektroniczną,
- ataki na użytkowników przeglądających strony Web,
- wykorzystania podatności urządzeń i systemów Straży Granicznej - praktycznie codziennie obserwowane na urządzeniach brzegowych Straży Granicznej.

KLUCZOWE PROJEKTY I INICJATYWY:

Projekt A:

Zainicjowano w 2025 roku współpracę z NASK PIB w zakresie przeprowadzenia szkoleń dla funkcjonariuszy i pracowników Straży Granicznej z zakresu cyberbezpieczeństwa. Planuje się przeszkolenie personelu SG w formule stacjonarnej w dogodnych lokalizacjach. Aktualnie trwają szczegółowe ustalenia dot. projektu.

Projekt B:

24 lipca 2025 roku zostało podpisane porozumienie pomiędzy Ministerstwem Cyfryzacji a Komendą Główną Straży Granicznej o udostępnieniu Systemu rozpoznawania zagrożeń w cyberprzestrzeni (Cyber Threat Intelligence, CTI). Straż Graniczna znalazła się w gronie 9 kluczowych z punktu widzenia bezpieczeństwa państwa podmiotów KSC zapewniających bezpieczeństwo teleinformatyczne na poziomie krajowym.

Na podstawie porozumienia Zespół Security Operation Center Straży Granicznej pozyskał narzędzie do rozpoznawania zagrożeń w cyberprzestrzeni (CTI), o planowanych przez hackerów atakach na infrastrukturę teleinformatyczną oraz użytkowników systemów Straży Granicznej.

Możliwość identyfikacji zagrożeń, zanim dojdzie do ataku to jedna z wielu zalet tego narzędzia. Dzięki analizie aktywności grup cyberprzestępczych rozwiązanie odpowiednio wcześnie ostrzega o planowanych atakach, co daje czas na przygotowanie obrony.

Udział w tym projekcie zapewnia Straży Granicznej bezpłatny i nieograniczony dostęp do zaawansowanego narzędzia cyberbezpieczeństwa jakim jest system CTI co pozytywnie wpływa na jakość realizacji obowiązków wynikających z UKSC a co istotne, umożliwia pozyskanie przez SG nowych zdolności w zakresie rozpoznawania zagrożeń w cyberprzestrzeni.

Projekt C:

W dniach 24 i 27 października 2025 r. Straż Graniczna zawarła porozumienia o współpracy z dyrektorami następujących szkół średnich: Technikum Elektronicznego nr 1 w Zespole Szkół nr 36 im. Marcina Kasprzaka w Warszawie oraz Technikum Łączności w Zespole Szkół Łączności w Warszawie.

Na mocy tych porozumień KGSG uzyskała możliwość prowadzenia przedsięwzięć promocyjnych Straży Granicznej w dziedzinie technologii informacyjnych i komunikacyjnych, ukierunkowanych przede wszystkim na pozyskanie wysoko wykwalifikowanych kadr o solidnym przygotowaniu branżowym.

W ramach porozumień uczniowie ww. szkół będą mogli odbywać specjalistyczne praktyki zawodowe w Biurze Łączności i Informatyki KGSG. SG natomiast aktywnie przyczyni się do rozwoju kompetencji młodzieży poprzez: organizację dedykowanych, specjalistycznych zajęć dydaktycznych, przyjmowanie uczniów na praktyki oraz ich kształcenie w nowoczesnym, wyposażonym w najnowsze technologie laboratorium IT, a także aranżowanie wizyt studyjnych i lekcji tematycznych

Straż Graniczna, we współpracy ze szkołami średnimi, zainicjowała strategiczny proces wspólnego kształtowania nowej generacji kadr w pionie łączności i informatyki, inwestując w edukację i profesjonalny rozwój przyszłych funkcjonariuszy już na etapie szkolnym.

REKOMENDACJE NA 2026 - REKOMENDACJE DLA PEŁNOMOCNIKA RZĄDU DS. CYBERBEZPIECZEŃSTWA:

Proponuje się wprowadzenie zmiany w przepisach ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1662 z późn. zm.) polegającej na jednoznacznym zakazie obniżania uposażeń lub stosowania niższych wskaźników wynagrodzeń wobec osób realizujących zadania z zakresu cyberbezpieczeństwa w instytucjach publicznych.

W szczególności proponowana zmiana ma na celu wyeliminowanie praktyk polegających na różnicowaniu poziomu uposażenia tych osób w porównaniu do innych pracowników lub funkcjonariuszy zatrudnionych na tych samych lub równorzędnych stanowiskach, wykonujących porównywalne obowiązki.

Celem projektowanej nowelizacji jest zapewnienie równego traktowania w zakresie wynagradzania, stabilności zatrudnienia oraz utrzymania wysokich kompetencji w obszarze cyberbezpieczeństwa, który ma kluczowe znaczenie dla bezpieczeństwa państwa.

KOMENDA GŁÓWNA PAŃSTWOWEJ STRAŻY POŻARNEJ (KGPSP)

PODSUMOWANIE ROCZNE:

W 2025 r. cyberprzestrzeń wokół Państwowej Straży Pożarnej (PSP) pozostała stabilna mimo wzrostu aktywności cyberzagrożeń wobec sektora publicznego. Nie odnotowano incydentów DDoS ani przerw w kluczowych systemach, takich jak Systemy Wspomagania Decyzji PSP. Pojedynczy incydent dotyczył potencjalnego wycieku danych z urządzeń FortiGate w KP PSP Wysokie Mazowieckie – szybko zaizolowany i zanalizowany bez skutków operacyjnych.
Ciągła współpraca z CSIRT ABW zapewniała monitorowanie zagrożeń w czasie rzeczywistym, m.in. z Internetu z użyciem narzędzi ARAKIS.GOV. Prowadzone były kampanie informacyjne oraz stałe monitorowane zabezpieczenia systemów i sieci w jednostkach organizacyjnych PSP.

KLUCZOWE PROJEKTY I INICJATYWY:

Projekt A: „Dostawa urządzeń infrastruktury sieci sd-wan dla platformy chmurowej integracji danych KG PSP"

Celem tego zadania jest stworzenie spójnego i zintegrowanego systemu komunikacyjnego, który umożliwi efektywny, szybki i bezpieczny przepływ krytycznych informacji w ramach działań Państwowej Straży Pożarnej i innych służb odpowiedzialnych za bezpieczeństwo publiczne. W tym celu, kontynuowano proces zamówienia publicznego zakupu i wdrożenia zaawansowanych urządzeń bezpieczeństwa sieciowego oraz budowę rozległej zarządzanej sieci teleinformatycznej SD-WAN (Software-Defined Wide Area Network) na obszarze kraju w skali całej PSP, stanowiącej pierwszą linię obrony przed cyberatakami. Przedmiotowe zadanie objęło dostawę i wyposażenie lokalizacji PSP w urządzenia sieci SD-WAN, w celu stworzenia zaawansowanego i zintegrowanego systemu komunikacyjnego. Zadanie to jest częścią projektu rozbudowy Platformy Chmurowej Integracji Danych Komendy Głównej PSP (PCID-KGPSP), który realizowany jest w ramach projektu SOIA (System Ostrzegania i Alarmowania Ludności).
Główne cele to:

- Interoperacyjność.
- Ciągłość działania.
- Szybkość przekazu informacji.
- Zabezpieczenie danych.
- Skalowalność.
- Zgodność z przepisami.

Projekt ten zapewni zwiększenie efektywności operacyjnej i bezpieczeństwa w działaniach Państwowej Straży Pożarnej.

Projekt B: Zabezpieczenie infrastruktury KG PSP przed zawansowanymi cyberzagrożeniami.

Zakup i wdrożenie systemu EDR, który umożliwia wykrywanie i neutralizację zagrożeń na różnych poziomach, oraz zapewnia ciągły monitoring bezpieczeństwa. System zapewnia ochronę przed malware, ransomware, atakami behawioralnymi oraz zaawansowane narzędzia analityczne.

Projekt C: Zintegrowany System Zarządzania Bezpieczeństwem Informacji (SZBI)

Komenda Głowna PSP wdrożyła Zintegrowany System Zarządzania Bezpieczeństwem Informacji (SZBI). W ramach systemu powstał szereg dokumentów, regulujących obszar zarządzania bezpieczeństwem. W skład systemu wchodzi szereg dokumentów (Polityki, Regulaminy, Instrukcje). Wyznaczono również Pełnomocnika ds. SZBI. Wdrożenie SZBI pozwoli na lepsze zabezpieczenie wrażliwych informacji przed ich utratą lub zniszczeniem. Stanowi również wypełnienie wymogów prawnych związanych z wejściem dyrektywy NIS2, przepisów KRI oraz RODO.

OBSERWOWANE TRENDY I WYZWANIA:

Trend 1: Ataki na infrastrukturę krytyczną.

Pomimo wyraźnego trendu wzrostowego dotyczącego zagrożeń infrastruktury krytycznej państwa, system Stanowisk Kierowania PSP działał bez większych zakłóceń. W minionym roku nie zaobserwowano poważnych awarii oraz ataków na infrastrukturę PSP. Wdrożono dodatkowe firewalle i segmentację sieci.

Trend 2: Spam i malware.

W minionym roku obserwowano wzmożoną aktywność akcji spamowych oraz malware. Na bieżąco wprowadzane były blokady na urządzeniach i systemach (zgodnie z informacjami z CSIRT GOV).

Trend 3: Braki kadrowe oraz urządzenia IoT.

Niedobór specjalistów w zakresie cyberbezpieczeństwa oraz rosnące ryzyka związane z urządzeniami IoT.

ANALIZA I OCENA FUNKCJONOWANIA KSC:

KSC działa efektywnie z perspektywy PSP, zapewniając szybką reakcję i interoperacyjność. Skuteczność komunikacji jest na wysokim poziomie dzięki dedykowanym kanałom wymiany informacji, takim jak platforma ARAKIS.GOV oraz zintegrowane interfejsy z CSIRT GOV (ABW).

PSP regularnie otrzymuje alerty o zagrożeniach w czasie rzeczywistym, co umożliwia szybkie i prewencyjne blokady zagrożeń (m.in. próby phishingu i malware) dzięki współdzieleniu danych z CSIRT GOV. Czas reakcji na incydenty oraz analiza incydentów jest szybka i satysfakcjonująca.

MINISTERSTWO KLIMATU I ŚRODOWISKA (MKIŚ)

Ministerstwo Klimatu i Środowiska

PODSUMOWANIE ROCZNE:

Do 21 sierpnia 2025 r. MKiŚ pełniło funkcję OW ds. cyberbezpieczeństwa dla sektora energii. Mimo to Raport jest składany na formularzu podmiotu publicznego - gdyż na dzień jego złożenia MKiŚ ma taki status, jednak informacje w raporcie zawierają działania z całego 2025 r. - obejmują zarówno działania OW jak i podmiotu publicznego.

W 2025 r. Ministerstwo Klimatu i Środowiska realizowało zestaw inicjatyw o charakterze strategicznym w obszarze cyberbezpieczeństwa, wynikających z pełnienia zadań organu właściwego oraz roli resortu w kształtowaniu ram systemowych dla sektorów objętych jego właściwością. Działania te obejmowały zarówno inicjatywy planistyczne i koncepcyjne, a także przedsięwzięcia ukierunkowane na wzmacnianie zdolności operacyjnych oraz kompetencyjnych sektora. Jednym z kluczowych kierunków było przygotowanie rozwiązań systemowych wspierających reagowanie na incydenty cyberbezpieczeństwa na poziomie sektorowym. W tym obszarze realizowane były prace analityczne i koncepcyjne, których celem było określenie docelowego modelu wsparcia podmiotów KSC oraz identyfikacja potrzeb interesariuszy w zakresie wymiany informacji i obsługi incydentów.

Równolegle prowadzone były działania związane z przygotowaniem dokumentów wyznaczających kierunki polityki państwa w obszarze energii i klimatu. W pracach tych zagadnienia cyberbezpieczeństwa traktowane były jako element horyzontalny, warunkujący bezpieczeństwo energetyczne, ciągłość procesów opartych na danych oraz odporność sektorów na zagrożenia, w tym o cyberzagrożenia. Uzupełnieniem działań systemowych były inicjatywy ukierunkowane na rozwój kompetencji i świadomości w obszarze cyberbezpieczeństwa. Obejmowały one wsparcie przedsięwzięć szkoleniowych adresowanych do kadry zarządzającej i specjalistów technicznych, koncentrujących się na zagrożeniach dla infrastruktury krytycznej, nowych wyzwaniach technologicznych, w tym związanych z automatyzacją i sztuczną inteligencją, oraz na przygotowaniu sektora do nowych obowiązków regulacyjnych.

Łącznie podejmowane inicjatywy tworzyły spójny zestaw działań ukierunkowanych na wzmacnianie odporności na cyberzagrożenia sektorów oraz przygotowanie ram dla dalszego rozwoju KSC.

KLUCZOWE PROJEKTY I INICJATYWY:

Projekt A: Projekt KPO C3.1.1 – przygotowanie koncepcji sektorowego zespołu CSIRT

W roku 2025 Ministerstwo Klimatu i Środowiska realizowało działania przygotowawcze w ramach projektu KPO C3.1.1, prowadzone w okresie do 21 sierpnia 2025 r., kiedy zadania związane z obszarem energii pozostawały w zakresie właściwości resortu. Projekt dotyczył przygotowania koncepcji utworzenia sektorowego zespołu CSIRT, ukierunkowanego na wzmocnienie zdolności reagowania na cyberzagrożenia, usprawnienie wymiany informacji oraz zapewnienie wsparcia podmiotom objętym KSC. Zakres prac obejmował działania koncepcyjne i analityczne, w tym opracowanie założeń funkcjonowania CSIRT, przygotowanie i złożenie wniosku o dofinansowanie w ramach KPO oraz analizy sektorowe dotyczące potrzeb interesariuszy i oczekiwanego katalogu usług CSIRT. Złożony wniosek uzyskał

pozytywną ocenę oraz informację o przyznaniu środków finansowych. Dalsze działania były prowadzone w Ministerstwie Energii.

Projekt B: Przygotowanie aKPEiK z uwzględnieniem aspektów cyberbezpieczeństwa

W 2025 r. Ministerstwo Klimatu i Środowiska prowadziło prace nad przygotowaniem projektu aktualizacji Krajowego Planu w dziedzinie Energii i Klimatu do 2030 r. z perspektywą do 2040 r. (aKPEiK), stanowiącego strategiczny dokument planistyczny wymagany przepisami Unii Europejskiej. W toku opracowywania dokumentu uwzględniono aspekty cyberbezpieczeństwa i odporności sektorowej jako elementy warunkujące bezpieczeństwo energetyczne oraz prawidłowe funkcjonowanie systemów i procesów opartych na danych. aKPEiK identyfikuje cyberzagrożenia jako istotny czynnik ryzyka dla sektora energii oraz sektora gospodarowania odpadami, wskazując na potrzebę wzmacniania podejścia sektorowego do zarządzania ryzykiem cyberzagrożeń, w tym w kontekście wdrażania dyrektywy NIS2 oraz spójności z regulacjami sektorowymi UE, takimi jak Network Code on Cybersecurity for Electricity (NC CS). Prace te były prowadzone w okresie, gdy sektor energii pozostawał w zakresie właściwości MKiŚ, tj. do 21 sierpnia 2025 r., i stanowiły istotny wkład w przygotowanie ram dla dalszych działań w obszarze KSC

Projekt C: Wsparcie powstania i działalności Centrum Szkoleniowego w obszarze cyberbezpieczeństwa i odporności cyfrowej sektorów energetycznego i środowiskowego

W 2025 r. Ministerstwo Klimatu i Środowiska wspierało powstanie oraz działalność sektorowego Centrum Szkoleniowego prowadzonego przez Instytut Energetyki-PIB którego celem jest podnoszenie kompetencji w obszarze cyberbezpieczeństwa, odporności cyfrowej i zarządzania ryzykiem w środowisku transformacji energetycznej i cyfrowej. Centrum Szkoleniowe oferuje szkolenia otwarte i dedykowane dla kadry zarządzającej oraz zespołów technicznych sektora energetycznego, ze szczególnym uwzględnieniem zagadnień cyberbezpieczeństwa infrastruktury krytycznej, strategicznych wymagań wynikających z NIS2 i KSC. W 2025 r. w ramach działalności centrum odbyły się m.in.: szkolenia na temat strategii i wdrożenia cyberbezpieczeństwa w infrastrukturze krytycznej oraz programy poświęcone cyberbezpieczeństwu w pracy zdalnej i hybrydowej, szkolenia z zakresu zagrożeń związanych z AI. W szkoleniu uczestniczyli operatorzy usług kluczowych sektora energii.

OBSERWOWANE TRENDY I WYZWANIA:

Wyzwanie 1: Braki kadrowe i finansowe

W ostatnich latach wyraźnie rośnie presja operacyjna: liczba incydentów, regulacji i systemów do utrzymania zwiększa się szybciej niż możliwości zespołu bezpieczeństwa i administratorów. Jednocześnie powszechnym trendem są braki kadrowe i przeciążenie kluczowych osób. Redukcja budżetów operacyjnych na poziomie jednostki dodatkowo ogranicza możliwość rozwoju kompetencji, automatyzacji i utrzymania narzędzi oraz pracowników na właściwym poziomie. W efekcie działy bezpieczeństwa są zmuszane do przechodzenia z podejścia proaktywnego na reaktywne, skupiając się na minimum zgodności i neutralizowaniu najpilniejszych zagrożeń zamiast realnego podnoszenia poziomu bezpieczeństwa organizacji.

Wyzwanie 2: Brak wysokospecjalizowanych szkoleń technicznych dla kluczowych osób

Brak regularnego podnoszenia kwalifikacji osób z obszaru cyberbezpieczeństwa, administratorów kluczowych systemów bezpieczeństwa powoduje, że decyzje techniczne mogą opierać się na nieaktualnej wiedzy, co zwiększa ryzyko błędów i podatności. W praktyce oznacza to wolniejsze reagowanie na nowe techniki ataków, co długofalowo generuje koszty i ryzyka znacznie wyższe niż oszczędności wynikające z rezygnacji ze szkoleń.

Wyzwanie 3: Ograniczenia finansowe i kadrowe w realizacji zadań organu właściwego ds. cyberbezpieczeństwa

W 2025 r. istotnym wyzwaniem w obszarze cyberbezpieczeństwa były ograniczenia wynikające z obowiązujących ram prawnych i finansowych. Przepisy UKSC zapewniały środki niewystarczające do pełnej i kompleksowej realizacji zadań organu właściwego ds. cyberbezpieczeństwa. W konsekwencji konieczne było podejmowanie decyzji priorytetyzujących działania oraz koncentracja dostępnych zasobów na obszarach o najwyższym znaczeniu z punktu widzenia bezpieczeństwa.

Ograniczenia finansowe przekładały się bezpośrednio na wyzwania organizacyjne I kadrowe. Skutkowało to znacznym obciążeniem istniejącego zespołu oraz koniecznością reagowania na bieżące zdarzenia w trybie doraźnym, często kosztem działań planowych i rozwojowych. Pomimo wysokiego poziomu zaangażowania pracowników i dużej dyspozycyjności zespołu, Zakres powierzonych obowiązków istotnie przekraczał dostępne możliwości organizacyjne. W dłuższej perspektywie utrzymanie takiego modelu finansowania może stanowić istotne ryzyko dla skuteczności wykonywania zadań ustawowych oraz stabilności funkcjonowania KSC.

OBSERWOWANE TRENDY I WYZWANIA - SPECYFICZNE OSZUSTWA

W 2025 r. jednym z najbardziej istotnych zjawisk w cyberprzestrzeni były działania o charakterze oszukańczym polegające na wykorzystywaniu wizerunku podmiotów sektora energii oraz instytucji publicznych do wyłudzania danych lub środków finansowych. Odnotowano przypadki podszywania się pod znane marki energetyczne oraz organy administracji, w których wykorzystywano elementy identyfikacji wizualnej, nazwy podmiotów oraz treści nawiązujące do bieżących tematów, takich jak rozliczenia, taryfy, programy wsparcia czy zmiany regulacyjne.

ANALIZA I OCENA FUNKCJONOWANIA KSC:

W 2025 r. KSC funkcjonował w sposób efektywny. Jakości komunikacji oraz koordynacji działań podejmowanych z punktu widzenia Ministerstwa Cyfryzacji była dobra. Z perspektywy MKiŚ widoczny był wzrost dojrzałości organizacyjnej KSC oraz coraz lepsze ukształtowanie ról i mechanizmów współdziałania.

Współpraca Ministerstwa Klimatu i Środowiska (jako podmiotu publicznego) z CSIRT GOV układała się w sposób konstruktywny i efektywny, co umożliwiało bieżące konsultowanie zdarzeń oraz koordynację działań w sytuacjach wymagających wsparcia eksperckiego.

Pozytywnie oceniane były również działania podejmowane przez Ministerstwo Cyfryzacji w zakresie koordynacji funkcjonowania KSC. W szczególności istotne znaczenie miało uwzględnianie potrzeb zgłaszanych przez organy właściwe oraz tworzenie przestrzeni do wymiany doświadczeń i opinii, m.in. w ramach spotkań roboczych i forów, które umożliwiały zgłaszanie propozycji usprawnień oraz dyskusję nad kierunkami rozwoju systemu.

Jednocześnie istotnym wyzwaniem dla dalszego rozwoju i skuteczności KSC pozostawał brak wystarczającego finansowania zadań realizowanych przez organy właściwe ds. cyberbezpieczeństwa. Ograniczenia te wpływały na zdolność do równoległego prowadzenia działań operacyjnych, nadzorczych i rozwojowych oraz przekładały się na zwiększone obciążenie kadrowe.

Dodatkowym wyzwaniem była ograniczona dostępność informacji o incydentach po stronie organów właściwych. Organy te nie uczestniczą bezpośrednio w pełnym obiegu informacji operacyjnych dotyczących incydentów, mimo że ponoszą odpowiedzialność polityczną za funkcjonowanie sektorów objętych właściwością. Utrudnia to pełną ocenę sytuacji oraz podejmowanie działań o charakterze strategicznym i systemowym.

REKOMENDACJE NA 2026 R. REKOMENDACJE DLA PEŁNOMOCNIKA RZĄDU DS. CYBERBEZPIECZEŃSTWA:

Zasadne wydaje się rozważenie w 2026 r. działań legislacyjnych dotyczących mechanizmów finansowania zadań organów właściwych ds. cyberbezpieczeństwa. Obowiązujące limity wydatków, określone w UKSC oraz jej nowelizacji w dłuższej perspektywie będą niewystarczające wobec rosnącego zakresu zadań, obejmujących m.in. nadzór nad operatorami usług kluczowych, analizę audytów, kontrole. Poziom finansowania wpływa również na możliwości pozyskiwania i utrzymania wyspecjalizowanej kadry eksperckiej. Nowelizacja UKSC oferuje zbyt małą ilość etatów dla specjalistów z zakresu cyberbezpieczeństwa, a tym które są przewidziane proponuje zbyt niskie mnożniki. Utrzymanie takich limitów może prowadzić do ograniczenia zdolności operacyjnych organu właściwego oraz zakłóceń w funkcjonowaniu KSC w każdym sektorze, dlatego rekomenduje się rozważenie dostosowania limitów wydatków do rzeczywistych potrzeb każdego sektora KSC w perspektywie średnio i długoterminowej. Wyszkolenie pracownika do połowa sukcesu, jego utrzymanie wymaga także nakładu na budowanie dalszego doświadczenia oraz konkurowanie z sektorem prywatnym o skończoną liczbę ekspertów.

Ponadto niezbędne jest kontynuowanie intensywnych kampanii informacyjnych dla obywateli, podnoszenie świadomości w zakresie zagrożeń bezpieczeństwa teleinformatycznego oraz eliminacja wykluczenia z wiedzy o obchodzeniu się z elektroniką. Wskazana jest silna promocja serwisu cyber.gov.pl, dalszy rozwój moje.cert.pl oraz zwrócenie uwagi na konieczność podnoszenia kompetencji cyfrowych pracowników sektora publicznego.

KANCELARIA PREZESA RADY MINISTRÓW (KPRM)

PODSUMOWANIE ROCZNE:

W minionym roku sytuacja w obszarze cyberbezpieczeństwa KPRM utrzymywała się na stabilnym, kontrolowanym poziomie. Nie odnotowano żadnych poważnych incydentów, które mogłyby wpłynąć na ciągłość działania, dostępność usług lub bezpieczeństwo informacji. Skuteczny nadzór operacyjny, sprawna współpraca BI i CSiRT w ramach KSC oraz dojrzałe procedury reagowania pozwoliły na szybkie wykrywanie i neutralizowanie potencjalnych zagrożeń jeszcze na wczesnym etapie.

KPRM konsekwentnie wzmacniała swoje zdolności obronne w ramach Bravo CRP, prowadząc stały monitoring środowiska teleinformatycznego, 24 godzinne dyżury IT i wdrażając narzędzia podnoszące poziom automatyzacji oraz precyzję detekcji. Rozwijano mechanizmy analityczne, usprawniano procesy raportowania, a także podnoszono kompetencje pracowników w obszarze cyberbezpieczeństwa, co realnie zwiększyło odporność na zagrożenia oraz umożliwiło szybsze podejmowanie decyzji operacyjnych. Regularnie aktualizowane standardy bezpieczeństwa i prace modernizacyjne pozwoliły utrzymać wysoki poziom ochrony infrastruktury oraz zagwarantować zgodność z wymaganiami organizacyjnymi.

Ogólny obraz cyberprzestrzeni KPRM można ocenić jako stabilny, dobrze zarządzany i wzmacniany w sposób ciągły. Aktywne działania prewencyjne, rozwój narzędzi bezpieczeństwa oraz odpowiedzialne podejście do zarządzania ryzykiem pozwoliły nie tylko utrzymać wysoki poziom bezpieczeństwa, lecz także zbudować solidne podstawy do dalszej poprawy odporności cybernetycznej.

OBSERWOWANE TRENDY I WYZWANIA:

Trend 1: Braki kadrowe

Opis: W 2025 roku KPRM mierzyła się z silnie narastającymi wyzwaniami kadrowo-personalnymi w obszarze cyberbezpieczeństwa. Ogólny niedobór specjalistów, a także znaczące różnice wynagrodzeń w administracji i w biznesie, bezpośrednio przekładały się na trudności w rekrutacji, zwiększone obciążenie pracowników i wydłużone czasy reakcji na incydenty. Dodatkowo, dynamiczny rozwój technologii AI wymuszał stałe podnoszenie kwalifikacji, ponieważ tradycyjne kompetencje specjalistów SOC czy analityków incydentów okazywały się niewystarczające wobec narzędzi i taktyk atakujących.

Trend 2: Celowanych kampanii mailowych

Opis: Równolegle zaobserwowaliśmy wzrost zagrożenia ze strony **celowanych kampanii mailowych**, które w 2025 r. stały się jednym z podstawowych wektorów prób destabilizacji pracy KPRM. Zjawisko phishingu i SPAMu – wzmocnione użyciem zaawansowanej generatywnej AI – osiągnęło bezprecedensową skalę. Te ukierunkowane działania wyraźnie zwiększyły presję operacyjną na instytucję, utrudniając utrzymanie ciągłości działania i wymuszając wzmacnianie środków ochronnych.

ANALIZA I OCENA FUNKCJONOWANIA KSC:

Jako instytucja będąca beneficjentem w KSC oceniamy jego funkcjonowanie jako bardzo efektywne i realnie wspierające nasze działania w zakresie ochrony przed cyberzagrożeniami. KSC zapewnia nam szybkie, jasne i dobrze zorganizowane kanały komunikacji, co pozwala na sprawne przekazywanie i odbieranie kluczowych informacji operacyjnych.

Wymiana informacji jest prowadzona w sposób ustandaryzowany, bezpieczny i szybki, a otrzymywane komunikaty są precyzyjne i wartościowe z punktu widzenia analitycznego i operacyjnego. Znacząco skraca to czas potrzebny na wykrywanie i neutralizowanie zagrożeń.

Współpracę z CSiRT Gov oceniamy bardzo wysoko. Czas reakcji CSIRT jest krótki, a wsparcie podczas incydentów – profesjonalne i skuteczne. Ułatwia to podejmowanie właściwych działań naprawczych.

REKOMENDACJE NA 2026 R. - REKOMENDACJE DLA PEŁNOMOCNIKA RZĄDU DS. CYBERBEZPIECZEŃSTWA:

Dynamiczny rozwój technologii sztucznej inteligencji stwarza nowe możliwości dla administracji rządowej, umożliwiając usprawnienie procesów, odciążyć urzędników od zadań powtarzalnych i podnieść jakość usług publicznych. Aby jednak wprowadzać te rozwiązania w sposób odpowiedzialny i bezpieczny, konieczne jest utworzenie spójnych polityk bezpieczeństwa regulujących wykorzystanie AI w instytucjach publicznych.

Takie regulacje powinny zapewniać najwyższe standardy bezpieczeństwa danych, przejrzystość działania algorytmów oraz zachowanie pełnej odpowiedzialności człowieka za decyzje administracyjne. Jednocześnie muszą uwzględniać zasady etyki, niedyskryminacji oraz konieczność kontroli ryzyk związanych z automatyzacją procesów urzędowych.

Stworzenie jednolitych wytycznych i mechanizmów nadzoru — obejmujących m.in. ocenę ryzyka, certyfikację systemów AI oraz centralną koordynację wdrożeń — umożliwi bezpieczne i efektywne wykorzystanie technologii przy zachowaniu zaufania publicznego oraz ochronie interesu państwa i obywateli.

MINISTERSTWO SPRAW WEWNĘTRZNYCH I ADMINISTRACJI (MSWIA)

PODSUMOWANIE ROCZNE:

Ministerstwo Spraw Wewnętrznych i Administracji odpowiada za cyberbezpieczeństwo infrastruktury telekomunikacyjnej, zapewniającej niezawodną i bezpieczną transmisję danych (fizyczna separacja od Internetu) i wykorzystywanej na potrzeby świadczenia usług dla klientów wchodzących w skład administracji rządowej (GovNet); ogólnopolską platformę teletransmisyjną wykorzystywaną przez służby bezpieczeństwa i porządku publicznego oraz ratownictwa (OST 112); a także infrastrukturę umożliwiającą przesyłanie danych i realizację usług między interesariuszami europejskimi, tj. Komisją Europejską, agencjami i instytucjami europejskimi oraz administracjami Państw Członkowskich UE (TESTA-ng). W kompetencji ministra właściwego do spraw wewnętrznych pozostaje także wykonywanie działalności telekomunikacyjnej na potrzeby Kancelarii Prezydenta RP, Kancelarii Sejmu RP, Kancelarii Senatu RP i administracji rządowej poprzez zapewnienie bezpiecznej łączności rządowej. Do ww. celu wykorzystuje Sieć Łączności Rządowej (SŁR), zarządzaną i administrowaną przez Ministra SWiA, w porozumieniu z Szefem ABW. W przedmiotowej sieci świadczone są dla osób funkcyjnych oraz organów terenowych na poziomie województw, usługi telekomunikacyjne. Infrastruktura ta podlega ochronie realizowanej przez CSIRT GOV prowadzony przez Szefa ABW. W ramach stałej współpracy z CSIRT GOV, MSWiA aktywnie korzysta z ostrzeżeń generowanych przez utrzymywany przez ABW system ARAKIS-GOV.

W roku 2025 w cyberprzestrzeni MSWiA obserwowano znaczny wzrost liczby incydentów związanych z cyberzagrożeniami, co wymuszało konieczność ciągłego doskonalenia systemów bezpieczeństwa, zakupy i modernizację środowisk technologicznych, a także rozwój polityk kadrowych. W odpowiedzi na rosnące wyzwania opracowywane były szczegółowe plany ciągłości działania, uwzględniające zarówno infrastrukturę teleinformatyczną, jak i procedury reagowania na incydenty. Zważywszy, że minister spraw wewnętrznych i administracji jest operatorem Systemu Bezpiecznej Łączności Państwowej (SBŁP), o której mowa w ustawie z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. 2025, poz. 1907), wszystkie działania nakierowane były na zapewnienie niezbędnych działań związanych z adekwatnym zabezpieczeniem SBŁP.

KLUCZOWE PROJEKTY I INICJATYWY:

Projekt A: System Bezpiecznej Łączności Państwowej (SBŁP)[17]

W Ministerstwie Spraw Wewnętrznych i Administracji realizowane były prace koncepcyjne, legislacyjne, a w efekcie wdrożeniowe Systemu Bezpiecznej Łączności Państwowej wynikające z ustawy z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej. Uruchamiane usługi SBŁP MSWiA przyporządkował do czterech mediów transmisyjnych: (1) rządowa łączność stacjonarna, tj. odseparowana od publicznego Internetu infrastruktura GovNet, służąca do bezpiecznej transmisji danych, głosu i obrazu pomiędzy organami administracji rządowej, jednostkami podległymi oraz instytucjami odpowiedzialnymi za zarządzanie kryzysowe, w tym łączność jawna (zarządzana i administrowana przez MSWiA), niejawna (zarządzana i administrowana przez Ministra SWiA

[17] Ustawa z dnia 5 grudnia 2024 r. *o ochronie ludności i obronie cywilnej* (Dz. U. 2024 poz. 1907 oraz z 2025 r. poz. 1705).

w porozumieniu z Szefem ABW), usługi wideokonferencji z wykorzystaniem terminali wideo na potrzeby najważniejszych osób w państwie do poziomu wojewódzkiego (zarządzana przez Ministra SWiA i administrowana w porozumieniu z Komendantem Głównym Policji) oraz dedykowane systemy wymiany informacji europejskich oraz łączności dla obiektów wchodzących w skład SKBN, w tym także komunikacja z IP-RON (MON); (2) radiowa łączność trunkingowa, tj. administrowany przez Komendanta Głównego Policji dedykowany system łączności radiowej umożliwiający bezpośrednią bezpieczną łączność służb resortu swia: Policji, Państwowej Straży Pożarnej, Straży Granicznej oraz Służby Ochrony Państwa; (3) niejawna łączność mobilna, dla której przewiduje się rozwój dedykowanych rozwiązań zapewniających bezpieczną łączność mobilną dla służb odpowiedzialnych za bezpieczeństwo oraz (4) systemy łączności satelitarnej, które docelowo zapewnione zostaną poprzez usługi programu GOVSATCOM i *Secure Connectivity* (IRIS^2), dla których organem zarządzającym i odpowiedzialnym za wdrożenie jest Minister SWiA.

Celem SBŁP jest zapewnienie wydajnych, bezpiecznych i wysoce dostępnych usług łączności i infrastruktury dla systemów teleinformatycznych i telekomunikacyjnych, również w zakresie możliwość wykorzystania łączności krótkofalowej oraz łączności satelitarnej, pozwalających na zapewnienie łączności także w trakcie przemieszczania oraz w przypadkach relokowania stanowisk kierowania i dowodzenia w kontekście ochrony ludności, zwiększenia bezpieczeństwa obywateli i skuteczności reagowania na sytuacje kryzysowe.

Projekt B: Wielkoskalowe Systemy Informatyczne Unii Europejskiej

Wielkoskalowe systemy informacyjne UE (SIS, VIS, ESS, Eurodac, Etias, ECRIS-TCN, IO) stanowią filar infrastruktury bezpieczeństwa cyfrowego oraz bezpieczeństwa wewnętrznego UE. WSIUE są niezastąpionym narzędziem pozwalającym za zarzadzanie granicami, tworzenie wspólnej i jednolitej polityki związanej z zarządzaniem migracją i granicami zewnętrznymi UE. Dodatkowo umacniają współpracę w zakresie egzekwowania prawa i służą do wymiany danych między służbami państw członkowskich, wspierając walkę z przestępczością, terroryzmem, przemytem broni oraz fałszerstwami, w tym kradzieżą tożsamości. Jednym z aspektów wymiaru operacyjnego WSIUE jest biometria, która odgrywa kluczową rolę w bezpieczeństwie granicznym poprzez identyfikację osób na podstawie unikalnych cech fizycznych i behawioralnych. Technologie biometryczne, takie jak skanowanie twarzy, zbieranie odcisków palców, czy analiza tęczówki umożliwiają automatyzację kontroli granicznej. Pozwalają szybko wykrywać fałszywe dokumenty, nielegalną migrację i osoby poszukiwane, minimalizując ludzkie błędy. Dysponowanie nowoczesnymi urządzeniami jest w tym względzie kluczowe. WSIUE stały się fundamentem funkcjonowania każdego państwa członkowskiego. W walce z cyberzagrożeniami WSIUE usprawniają wymianę informacji między państwami członkowskimi i m.in. z Europolem oraz zapewniają organom ścigania UE ulepszone narzędzia do zwalczania przestępczości. MSWiA pełni kluczową rolę jako koordynator wdrażania a także rozwoju Wielkoskalowych Systemów Informacyjnych UE w Polsce, dbając o ich efektywne i bezpieczne funkcjonowanie oraz współpracę z administracją krajową i unijną. Celem jest przyczynienie się do efektywniejszego zarządzania zewnętrznymi granicami strefy Schengen oraz zwiększenia bezpieczeństwa wewnętrznego całej UE.

Projekt C: Integracja z europejskimi systemami GOVSATCOM i Secure Connectivity

W kontekście bezpiecznej łączności satelitarnej szczególne znaczenie ma rozwój programu GOVSATCOM i *Secure Connectivity*. Obejmują one budowę wspólnego systemu łączności satelitarnej Państw Członkowskich UE na potrzeby bezpieczeństwa, reagowania kryzysowego oraz obronności pn. IRIS^2. Strategicznym celem IRIS^2 jest zbudowanie przez UE własnej, niezależnej i bezpiecznej sieci komunikacji satelitarnej. Ma ona uniezależnić Europę od systemów komercyjnych, które pozostają pod kontrolą podmiotów spoza UE. System będzie służył w pierwszej kolejności administracji publicznej, służbom odpowiedzialnym za bezpieczeństwo i zarządzanie kryzysowe, wojsku a także kluczowym sektorom gospodarki, takim jak energetyka czy transport. Program ma na celu zapewnienie Państwom Członkowskim dostępu do bezpiecznych usług satelitarnych o podwyższonym poziomie ochrony.

Integracja Polski z IRIS^2 stwarza możliwość zwiększenia poziomu bezpieczeństwa i odporności komunikacji satelitarnej poprzez korzystanie ze wspólnych zasobów oraz rozwiązań o wysokim standardzie ochrony. Celem jest zapewnienie bezpiecznych i efektywnych kosztowo zdolności komunikacyjnych na potrzeby operacji o krytycznym znaczeniu dla bezpieczeństwa. Minister Spraw Wewnętrznych i Administracji realizuje to zadanie za pomocą jednostek *Competent GOVSATCOM Authority* (CGA) i *Competent Secure Connectivity Authority* (CSCA). System docelowo będzie elementem europejskiego systemu komunikacji krytycznej (EUCCS), który dotyczy przede wszystkim współpracy policji i służb granicznych. Dzięki systemowi zapewniona będzie niezawodna komunikacja w celu zapewnienia bezpieczeństwa w Europie, również wobec zagrożeń pojawiających się spoza Europy m.in. przeciwdziałania przestępczości, zwalczania nielegalnych migracji, przemytu, handlu ludźmi i substancjami niedozwolonymi.

OBSERWOWANE TRENDY I WYZWANIA:

Trend 1: Braki kadrowe

Rosnące zapotrzebowanie na specjalistów w zakresie cyberbezpieczeństwa konfrontowane jest z trudnościami w pozyskaniu tych specjalistów. Dysproporcja płacowa między administracją, a sektorem prywatnym skutkuje wysoką rotacją kadr eksperckich, szczególnie w obszarze cyberbezpieczeństwa, który jest stale rozwijającą się branżą rynku IT. Utrata kapitału ludzkiego w jednostkach publicznych obniża wydolność reakcji na zagrożenia. Brak adaptacji w obszarze polityki kadrowej sektora publicznego może uniemożliwić skuteczne zabezpieczanie cyberprzestrzeni publicznych usług IT, szczególnie jeśli weźmie się pod uwagę szybko zmieniającą się sytuację rynku pracy IT oraz sytuację geopolityczną, która wpływa z kolei na liczbę cyberzagrożeń.

Trend 2: Wzrastająca ilość ataków phisingowych, w tym także z wykorzystaniem AI

System monitorowania zasobów i zdarzeń bezpieczeństwa w systemie poczty elektronicznej MSWiA wykazuje radykalnie zwiększający się ruch związany z przekazywaniem podejrzanych wiadomości e-mail. Kwartalnie system pocztowy przetwarza ok. 1,5 miliona wiadomości e-mail, z czego około 70% stanowi zablokowany ruch sklasyfikowany jako spam (tj. wiadomości niechciane i potencjalnie niebezpieczne), a około 0,02% to próby jawnego dostarczenia znanego złośliwego oprogramowania. Wymusza to konieczność stałego modernizowania systemów ochrony, w tym także poprzez zakupy nowych rozwiązań technologicznych.

Trend 3: Potrzeba niejawnych systemów łączności mobilnej

Łączność mobilna oferuje potencjał wzmocnienia bezpieczeństwa komunikacji, a także zapewnienia priorytetyzacji ruchu w sieciach komórkowych dla służb odpowiedzialnych za bezpieczeństwo państwa. Ministerstwo Spraw Wewnętrznych i Administracji zauważa, że infrastruktura cyfrowa stanowi fundament komunikacji, a ta z kolei jest podstawą wszelkich podejmowanych działań. Zasadne jest dalsze wprowadzenie rozwiązań teleinformatycznych (w tym służących przekazywaniu informacji niejawnych), które spowodują wykorzystanie kanałów komunikacyjnych odseparowanych od Internetu jako głównego medium służącego do wymiany danych pomiędzy organami oraz instytucjami rządowymi.

Trend 4: Potrzeba uruchomienia resortowego centrum kompetencyjnego ds. cyberbezpieczeństwa

Zauważona została potrzeba zbudowania resortowego centrum kompetencyjnego MSWiA odpowiedzialnego za cyberbezpieczeństwo. Do jego zadań należeć będzie monitorowanie stanu bezpieczeństwa systemów i sieci teleinformatycznych, za obsługę których odpowiada MSWIA, a w których nie są przetwarzane informacje niejawne w rozumieniu przepisów ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Resortowe centrum kompetencyjne MSWiA obejmie swym zakresem poziom wojewódzki, w tym także szpitale podległe MSWiA. Struktura oparta będzie na wyodrębnionych zespołach kompetencyjnych, które pozwolą na efektywne działanie w różnych obszarach SBŁP. Powstanie Security Operations Center (SOC) odpowiedzialne za monitorowanie

zagrożeń w czasie rzeczywistym. Powstanie jednolita platforma teleinformatyczna zwiększająca gotowość i zdolność reagowania służb dyżurnych (cywilnych i wojskowych) na wszystkich poziomach zarządzania kryzysowego, w tym w szczególności możliwość bieżącego monitorowania i prognozowania rozwoju kryzysu (zasoby informatyczne oraz oprogramowanie).

ANALIZA I OCENA FUNKCJONOWANIA KSC:

Funkcjonowanie KSC w ocenie MSWiA jest zadowalające. MSWiA znajduje się w obszarze właściwości Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV, działającego pod nadzorem Szefa Agencji Bezpieczeństwa Wewnętrznego. W ramach stałej współpracy z CSIRT GOV, MSWiA zgłasza do Zespołu incydenty cyberbezpieczeństwa, a także aktywnie korzysta z dostarczanych ostrzeżeń oraz na bieżąco wdraża przekazywana rekomendacje. Kierownicy komórek uczestniczą również w niejawnych posiedzeniach PCOC. Jednostki podległe MSWiA wyrażają zadowolenie ze współpracy z CSIRT GOV, wyróżniając skuteczność komunikacji i czas reakcji w minionym roku.

Biorąc pod uwagę nowelizację UKSC zidentyfikowano obszar, mogący ograniczać efektywność systemu w obliczu docelowej implementacji dyrektywy NIS2. Możliwe jest nasycenie przepustowości istniejących CSIRT, ponieważ nowelizacja KSC z pewnością przyczyni się do wzrostu liczby podmiotów objętych ustawowymi wymaganiami, co z kolei wygeneruje znacznie więcej zdarzeń przekładających się na ryzyko paraliżu analitycznego CSIRT poziomu krajowego. Brak pełnej automatyzacji procesów, triażu zgłoszeń, może prowadzić do wydłużenia czasu obsługi incydentów o niższym priorytecie, co w warunkach ataku hybrydowego może maskować działania o charakterze krytycznym.

REKOMENDACJE NA 2026 - REKOMENDACJE DLA PEŁNOMOCNIKA RZĄDU DS. CYBERBEZPIECZEŃSTWA:

W perspektywie 2026 roku, kluczowe działania Pełnomocnika powinny skupić się na następujących obszarach:

- Dążenie do wdrożenia ogólnokrajowej platformy klasy MISP (Malware Infromation Sharing Platform) w celu skupienia informacji o zagrożeniach z różnych źródeł w jednym miejscu, a także ułatwienie i przyspieszenie wymiany informacji między IK objętych NIS2. System powinien umożliwiać automatyczną dystrybucję danych o zagrożeniach do systemów bezpieczeństwa, minimalizując czas reakcji ze względu na manualną obsługę incydentów.
- Świadczenia teleinformatyczne wypłacane osobom realizującym zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2021 r. poz. 2333) są bardzo potrzebnym i wartościowym mechanizmem. Warto podjąć prace zmierzające do zmiany sposobu uwzględniania tego świadczenia, bez zmiany charakteru z dodatku czasowego i uznaniowego, ale w sposób umożliwiający dodanie otrzymywanych przez specjalistów kwot do wynagrodzenia zasadniczego, tak by dodatek ten mógł być wliczany do wysługi lat.

RZĄDOWE CENTRUM BEZPIECZEŃSTWA (RCB)

PODSUMOWANIE ROCZNE:

Cyberprzestrzeń stanowi jeden z kluczowych obszarów wpływających na bezpieczeństwo narodowe oraz ciągłość funkcjonowania infrastruktury krytycznej państwa. Rządowe Centrum Bezpieczeństwa pełni centralną rolę platformy współpracy, koordynacji i wymiany informacji pomiędzy administracją publiczną, operatorami infrastruktury krytycznej oraz partnerami krajowymi i międzynarodowymi w obszarze cyberbezpieczeństwa.

Aktualna sytuacja w cyberprzestrzeni charakteryzuje się utrzymującym się wysokim poziomem zagrożeń, w tym działań o charakterze hybrydowym, ukierunkowanych na zakłócenie dostępności, integralności i poufności systemów kluczowych dla funkcjonowania państwa. Szczególną uwagę zwracają incydenty wymierzone w sektory energii, łączności, transportu oraz administracji publicznej, często poprzedzone zaawansowanymi kampaniami rozpoznawczymi i socjotechnicznymi.

RCB, jako integrator działań w obszarze bezpieczeństwa infrastruktury krytycznej, zapewnia ramy do skoordynowanego reagowania na incydenty, wzmacniania odporności systemowej oraz budowania wspólnego obrazu sytuacji. Kluczowe znaczenie mają rozwój mechanizmów współdzielenia informacji, standaryzacja procedur, ćwiczenia międzysektorowe oraz podnoszenie świadomości decydentów i operatorów. Skuteczność ochrony cyberprzestrzeni wymaga trwałej współpracy, ciągłej adaptacji oraz konsekwentnego integrowania cyberbezpieczeństwa z krajowym systemem zarządzania kryzysowego.

KLUCZOWE PROJEKTY I INICJATYWY:

Projekt A: Zintegrowany Program Kompetencji i Świadomości Cyberbezpieczeństwa

Cel: Budowa i utrzymanie wysokiego poziomu kompetencji oraz świadomości cyberbezpieczeństwa wśród kadry decyzyjnej, operatorów infrastruktury krytycznej i administracji publicznej.

Status: Projekt realizowany w sposób ciągły poprzez organizację cyklicznych Seminariów Cyberbezpieczeństwa oraz Krajowego Forum Ochrony Infrastruktury Krytycznej. Wsparciem działań jest udział pracowników RCB w roli prelegentów podczas branżowych konferencji i seminariów. Istotnym elementem realizacji Programu Kompetencji i Świadomości Cyberbezpieczeństwa są działania dydaktyczno-edukacyjne realizowane między innymi na takich uczelniach jak Uniwersytet Warszawski, Politechnika Warszawska, Szkoła Główna Handlowa, Uniwersytet Civitas czy też w Akademii Policji w Szczytnie.

Stałym zadaniem jest prowadzenie raportowania i ostrzegania w ramach stopni alarmowych CRP oraz realizowanie kampanii informacyjnych skierowanych do obywateli w ramach Cyber_RCB.

Efekty: Wzrost świadomości zagrożeń cybernetycznych, poprawa jakości decyzji podejmowanych w sytuacjach kryzysowych oraz wzmocnienie odporności państwa poprzez rozwój kompetencji kluczowych kadr.

Projekt B: Minimalne wymagania bezpieczeństwa infrastruktury krytycznej i strategia odporności podmiotów krytycznych

Cel: Wypracowanie i wdrożenie jednolitych minimalnych wymagań bezpieczeństwa infrastruktury krytycznej, w tym cyberbezpieczeństwa, jako narzędzia realizacji Strategii Odporności Podmiotów Krytycznych. Celem jest systemowe zwiększenie odporności podmiotów krytycznych poprzez zapewnienie niezakłóconego świadczenia usług kluczowych oraz ciągłości funkcjonowania infrastruktury krytycznej w warunkach zagrożeń cybernetycznych, fizycznych i hybrydowych. Opracowanie aktów wykonawczych w randze rozporządzenia do nowelizowanej ustawy o zarządzaniu kryzysowym.

Status: W 2025 r. Rządowe Centrum Bezpieczeństwa realizowało prace nad opracowaniem dokumentu minimalnych wymagań bezpieczeństwa dla operatorów infrastruktury krytycznej, stanowiącego jeden z kluczowych elementów wdrażania Strategii Odporności Podmiotów Krytycznych. Działania prowadzono w ścisłym powiązaniu z Krajową Oceną Ryzyka, analizą zagrożeń oraz wynikami ćwiczeń i stress testów realizowanych z udziałem operatorów IK. Minimalne wymagania zostały zaprojektowane jako narzędzie wspierające wdrażanie adekwatnych środków organizacyjnych, technicznych i proceduralnych, proporcjonalnych do poziomu ryzyka oraz specyfiki poszczególnych sektorów.

Efekty: Minimalne wymagania bezpieczeństwa stanowią praktyczne narzędzie implementacji Strategii Odporności Podmiotów Krytycznych, umożliwiając ujednolicenie podejścia do bezpieczeństwa w skali kraju oraz stopniowe podnoszenie poziomu odporności podmiotów krytycznych. Ich wdrożenie przyczynia się do ograniczenia podatności infrastruktury krytycznej, poprawy zdolności zapobiegania i reagowania na incydenty oraz zwiększenia gotowości państwa do utrzymania ciągłości usług kluczowych w sytuacjach kryzysowych, w tym o charakterze cybernetycznym i hybrydowym.

Projekt C: Utworzenie ISAC dla Infrastruktury Krytycznej (ISAC-IK)

Cel: Celem projektu jest utworzenie krajowego Information Sharing and Analysis Center dla infrastruktury krytycznej jako trwałego elementu systemu bezpieczeństwa państwa, umożliwiającego skoordynowaną, opartą na zaufaniu współpracę pomiędzy operatorami infrastruktury krytycznej, administracją publiczną, zespołami reagowania na incydenty oraz innymi podmiotami KSC ISAC-IK ma zapewnić wspólną analizę zagrożeń, wczesne ostrzeganie, wymianę informacji o incydentach i podatnościach oraz wsparcie procesów decyzyjnych w sytuacjach kryzysowych, wzmacniając odporność infrastruktury krytycznej i ciągłość świadczenia usług kluczowych. Wiodącą rolę w realizacji projektu pełni Rządowe Centrum Bezpieczeństwa, działające jako integrator współpracy i element krajowego systemu zarządzania kryzysowego.

Status: W 2025 r. Rządowe Centrum Bezpieczeństwa rozpoczęło realizację działań przygotowawczych związanych z utworzeniem ISAC-IK. Prace obejmowały analizy koncepcyjne i organizacyjne dotyczące modelu funkcjonowania ISAC w warunkach krajowych, zakresu podmiotowego i sektorowego, zasad uczestnictwa oraz mechanizmów bezpiecznej i zaufanej wymiany informacji. Dokonano przeglądu istniejących struktur koordynacyjnych i operacyjnych, w tym PCOC oraz ZIK, w celu zapewnienia komplementarności i uniknięcia dublowania kompetencji. Równolegle analizowano powiązania IK-ISAC z KSC, systemem zarządzania kryzysowego oraz kierunkami wynikającymi z implementacji dyrektyw NIS2 i CER. Podjęte działania stanowią podstawę do dalszej formalizacji projektu oraz rozpoczęcia etapu wdrożeniowego.

Efekty: Realizacja działań przygotowawczych do utworzenia ISAC-IK pozwoliła na zbudowanie podstaw organizacyjnych, proceduralnych i analitycznych dla systemowej współpracy w obszarze cyberbezpieczeństwa infrastruktury krytycznej. Wypracowane założenia funkcjonowania ISAC umożliwiają uruchomienie stałych mechanizmów wymiany informacji o zagrożeniach, podatnościach

i incydentach cybernetycznych pomiędzy operatorami infrastruktury krytycznej a administracją publiczną. Projekt przyczynia się do poprawy zdolności wczesnego ostrzegania, zwiększenia świadomości sytuacyjnej oraz skrócenia czasu reakcji na incydenty o potencjale systemowym. W dłuższej perspektywie działania te wspierają wzrost odporności infrastruktury krytycznej, poprawę ciągłości świadczenia usług kluczowych oraz wzmocnienie roli RCB jako centralnej platformy koordynacji bezpieczeństwa państwa.

OBSERWOWANE TRENDY I WYZWANIA:

Trend 1: Wzrost złożonych zagrożeń hybrydowych ukierunkowanych na infrastrukturę krytyczną

W 2025 r. jednym z kluczowych zjawisk w cyberprzestrzeni było dalsze nasilenie zagrożeń o charakterze hybrydowym, łączących działania cybernetyczne z operacjami informacyjnymi, dezinformacją oraz presją na procesy decyzyjne i systemy techniczne państwa. Z perspektywy RCB szczególnie istotne były działania ukierunkowane na infrastrukturę krytyczną, w tym sektory energii, łączności, transportu oraz administracji publicznej, których celem było zakłócenie ciągłości świadczenia usług kluczowych lub obniżenie zaufania publicznego. Zagrożenia te charakteryzowały się wysokim poziomem złożoności, długotrwałym rozpoznaniem oraz wykorzystaniem podatności organizacyjnych i ludzkich. Zjawisko to potwierdziło konieczność dalszej integracji cyberbezpieczeństwa z systemem zarządzania kryzysowego, rozwoju mechanizmów wczesnego ostrzegania oraz wzmacniania współpracy pomiędzy administracją publiczną, operatorami infrastruktury krytycznej i służbami odpowiedzialnymi za bezpieczeństwo państwa.

Trend 2: Wyzwania regulacyjne, organizacyjne i kadrowe w obszarze odporności cybernetycznej

Rok 2025 przyniósł istotne wyzwania związane z wdrażaniem nowych regulacji krajowych i unijnych w obszarze cyberbezpieczeństwa i odporności, w szczególności wynikających z dyrektyw NIS2 oraz CER. Z perspektywy RCB zauważalna była znaczna rozbieżność w poziomie dojrzałości organizacyjnej, proceduralnej i kompetencyjnej podmiotów odpowiedzialnych za bezpieczeństwo infrastruktury krytycznej. Dla wielu operatorów i jednostek administracji publicznej wyzwaniem okazało się równoległe wdrażanie nowych obowiązków, prowadzenie analiz ryzyka, raportowanie incydentów oraz zapewnienie ciągłości działania przy ograniczonych zasobach kadrowych. Narastające braki specjalistów ds. cyberbezpieczeństwa oraz rosnące obciążenie obowiązkami sprawozdawczymi zwiększały ryzyko podejścia formalnego kosztem realnej odporności. W tych warunkach wzrosło znaczenie RCB jako platformy koordynacyjnej, wspierającej wymianę informacji, harmonizację podejść oraz budowanie spójności działań państwa w obszarze cyberbezpieczeństwa.

ANALIZA I OCENA FUNKCJONOWANIA KSC:

Skuteczność komunikacji

W 2025 r. KSC funkcjonował w oparciu o ustalone kanały wymiany informacji pomiędzy podmiotami systemu, w tym zespołami CSIRT, administracją publiczną oraz operatorami infrastruktury krytycznej. Istotną rolę w tym zakresie odgrywało PCOC, które stanowiło forum bieżącej koordynacji, wymiany informacji sytuacyjnych oraz uzgadniania działań pomiędzy kluczowymi interesariuszami. Funkcjonowanie PCOC przyczyniało się do poprawy przepływu informacji w sytuacjach wymagających szybkiej synchronizacji działań, jednak doświadczenia operacyjne wskazywały na potrzebę dalszego ujednolicenia formatu i zakresu przekazywanych informacji, w szczególności na styku poziomu operacyjnego i decyzyjnego.

Czas reakcji na incydenty

Czas reakcji w ramach KSC był w wielu przypadkach adekwatny do skali i charakteru incydentów cybernetycznych. PCOC pełniło istotną funkcję w skracaniu czasu koordynacji działań w przypadku incydentów wielopodmiotowych lub o potencjale systemowym, umożliwiając szybkie zwoływanie posiedzeń oraz wymianę informacji pomiędzy CSIRT-ami i innymi podmiotami. Jednocześnie w przypadku incydentów złożonych lub o charakterze hybrydowym zauważalna była potrzeba dalszego wzmacniania mechanizmów wczesnego ostrzegania oraz standaryzacji procedur eskalacji.

Interoperacyjność z zespołami CSIRT

Interoperacyjność KSC z zespołami CSIRT była realizowana m.in. poprzez współpracę operacyjną i analityczną w ramach PCOC. Centrum to umożliwiało bieżącą synchronizację działań, wymianę ocen sytuacyjnych oraz uzgadnianie priorytetów reagowania. Jednocześnie poziom integracji narzędzi, procedur i modeli analitycznych pomiędzy poszczególnymi CSIRT pozostawał zróżnicowany, co wskazuje na potrzebę dalszego rozwoju wspólnych standardów, ćwiczeń międzyinstytucjonalnych oraz lepszego powiązania działań CSIRT z systemem zarządzania kryzysowego i ochrony infrastruktury krytycznej.

REKOMENDACJE NA 2026 - REKOMENDACJE DLA PEŁNOMOCNIKA RZĄDU DS. CYBERBEZPIECZEŃSTWA:

A. Wspieranie wykorzystania RCB jako punktu syntezy informacji o cyberzagrożeniach o znaczeniu państwowym

Zasadne jest promowanie praktyki, w której Rządowe Centrum Bezpieczeństwa przygotowuje przekrojowe oceny sytuacyjne oraz syntetyczne raporty dotyczące incydentów cybernetycznych występujących u operatorów infrastruktury krytycznej, mogących mieć wpływ na funkcjonowanie państwa, w szczególności w obszarze bezpieczeństwa publicznego.

B. Wspieranie rozwoju PCOC jako forum koordynacji i wymiany informacji

Wskazane jest dalsze wspieranie PCOC jako platformy bieżącej współpracy i uzgadniania działań pomiędzy podmiotami systemu, przy wykorzystaniu doświadczenia i roli RCB w zakresie porządkowania informacji i zapewniania spójnego obrazu sytuacji jako Krajowego Centrum Zarządzania Kryzysowego.

C. Wzmacnianie współpracy RCB z operatorami infrastruktury krytycznej

Zasadne jest dalsze rozwijanie współpracy RCB z operatorami infrastruktury krytycznej w obszarze cyberbezpieczeństwa, w tym poprzez działania szkoleniowe, ćwiczeniowe i analityczne, jako elementu wspierającego wymianę informacji i budowanie odporności systemowej. W tym zakresie konieczne są działania realizowane poprzez wsparcie np. NASK PIB związane z podniesieniem kompetencji pracowników RCB, ale także bezpośrednio kluczowego personelu odpowiedzialnych za cyberbezpieczeństwo u operatorów infrastruktury krytycznej.

D. Wspieranie roli RCB w ocenie wpływu cyberincydentów na ciągłość działania państwa oraz niezakłócone świadczenie usług kluczowych.

Celowe jest dalsze wzmacnianie roli RCB w zakresie całościowej oceny skutków incydentów cybernetycznych dla ciągłości działania państwa oraz niezakłóconego świadczenia usług kluczowych. RCB, dysponując przekrojową wiedzą o funkcjonowaniu IK oraz mechanizmach ZK, może wspierać procesy decyzyjne poprzez integrowanie informacji technicznych, operacyjnych i kontekstowych pochodzących z różnych źródeł. Takie podejście pozwala właściwe określenie priorytetów reagowania oraz terminowe uruchamianie adekwatnych mechanizmów koordynacyjnych, bez dublowania kompetencji zespołów odpowiedzialnych za techniczne aspekty reagowania.

MINISTERSTWO ROZWOJU I TECHNOLOGII (MRIT)

PODSUMOWANIE ROCZNE:

W Ministerstwie w związku z zaistniałymi zmianami organizacyjnymi aktualizowane są regulacje wewnętrzne dotyczące bezpieczeństwa informacji i bezpieczeństwa teleinformatycznego.

Stan bezpieczeństwa teleinformatycznego w Ministerstwie był na odpowiednim poziomie.

Wdrożone zabezpieczenia technicznie oraz organizacyjne zapewniły: niezakłóconą realizację zadań publicznych przez Ministerstwo, dostępność usług elektronicznych świadczonych przez Urząd, funkcjonowanie systemów wewnętrznych oraz bezpieczeństwo informacji przetwarzanych w MRiT.

Nie odnotowano zdarzeń skutkujących utratą podstawowych atrybutów informacji w systemach informacyjnych Ministerstwa.

KLUCZOWE PROJEKTY I INICJATYWY:

Projekt A: „Zwiększenie dojrzałości cyfrowej i cyberbezpieczeństwa firm poprzez udostępnienie usług cyfrowych na Biznes.gov.pl"

Celem jest zapewnienie przedsiębiorcom realnego wsparcia w zarządzaniu bezpieczeństwem cyfrowym. Moduł w serwisie biznes.gov.pl obejmuje diagnozę dojrzałości cyfrowej i poziomu cyberbezpieczeństwa – **usługa dostępna.** Weryfikacja obowiązków wynikających z dyrektywy NIS2 wraz ze wsparciem w planowaniu działań dostosowawczych – **usługa będzie dostępna w lutym 2026; Usługa** analizy zgodności z wymogami Cyber Resilience Act (CRA) oraz generowanie odpowiedniej dokumentacji – **usługa będzie dostępna w marcu 2026.** Przedsiębiorcy otrzymają dostęp do **call center** oferującego ekspercką pomoc dotyczącą przepisów, certyfikacji oraz dobrych praktyk w dziedzinie cyberbezpieczeństwa – **usługa będzie dostępna w marcu 2026.**

Projekt B: Kampania edukacyjno-informacyjna KEI MŚP

Celem jest upowszechnienie korzyści wynikających z cyfryzacji i budowania kultury bezpieczeństwa. Jest realizowana poprzez: **webinary** oraz **działania informacyjne** z obszaru cyberbezpieczeństwa skrojone na potrzeby przedsiębiorców, w tym firm z sektorów chemii, produkcji oraz przestrzeni kosmicznej, **spotkania stacjonarne** z przedsiębiorcami w całej Polsce, **publikacja** materiałów edukacyjnych i promujących cyberbezpieczne praktyki w branżach wrażliwych

OBSERWOWANE TRENDY I WYZWANIA:

Trend 1:Trudności w pozyskaniu kadr o oczekiwanych umiejętnościach w odniesieniu do potrzeb urzędu

Opis: Przeprowadzane rekrutacje na stanowiska związane z cyberbezpieczeństwem nie doprowadziły do zatrudnienia osób. Problemem były niewystarczające kompetencje kandydatów.

Trend 2: Długotrwałe obowiązywanie stopni alarmowych CRP

Opis: Przy wieloletnim obowiązywaniu stopni alarmowych CRP może wystąpić spowszednienie postrzegania ich jako szczególny czas i realizacja części zadań staje się wyzwaniem. Wykaz zadań jakie należy realizować w poszczególnych stopniach powstał dekadę temu i wydaje się, że nie został

przystosowany do tak długiego obowiązywania np. zapewnienie dostępności pracowników w trybie alarmowym.

ANALIZA I OCENA FUNKCJONOWANIA KSC:

W 2025r. współpraca MRiT z CSiRT GOV, CERT PL oraz wymiana informacji o zagrożeniach w cyberprzestrzeni odbywała bardzo sprawnie.

REKOMENDACJE NA 2026 - REKOMENDACJE DLA PEŁNOMOCNIKA RZĄDU DS. CYBERBEZPIECZEŃSTWA:

Rekomendujemy rozważenie podjęcia działań analitycznych mających na celu określenie czy zasadne byłoby ujednolicenie funkcjonowania bezpieczeństwa informacji I cyberbezpieczeństwa w podmiotach administracji publicznej np. taki sam System Zarządzania Bezpieczeństwem Informacji, takie same struktury.

Rozważanie podjęcia działań w celu usprawnienia komunikacji pomiędzy podmiotami administracji publicznej w zakresie kwestii szeroko rozumianego bezpieczeństwa teleinformatycznego poprzez utworzenie wspólnej bazy kontaktów osób I informacji kompetencyjnych z poszczególnych podmiotów.

MINISTERSTWO FINANSÓW (MF)

PODSUMOWANIE ROCZNE:

W roku 2025 Ministerstwo Finansów, realizowała przygotowania do roli podmiotu kluczowego w rozumieniu UKSC.

W instytucji funkcjonują mechanizmy bezpieczeństwa informacji obejmujące środki techniczne, procedury organizacyjne oraz działania związane z zarządzaniem ryzykiem. System cyberbezpieczeństwa jest systematycznie rozwijany i dostosowywany do aktualnych zagrożeń oraz obowiązujących wymogów regulacyjnych.

Szczególną uwagę poświęca się rozwojowi kompetencji personelu. Szkolenia dla pracowników odpowiedzialnych za cyberbezpieczeństwo są realizowane zgodnie z przyjętym programem szkoleniowym, natomiast działania podnoszące świadomość cyberzagrożeń obejmują również pozostałych pracowników instytucji.

W 2025 roku zarejestrowano łącznie około 12 000 zdarzeń i zgłoszeń z obszaru cyberbezpieczeństwa, z których jedynie niewielka część została zakwalifikowana jako incydenty, co potwierdza skuteczność funkcjonujących mechanizmów monitorowania, detekcji oraz reagowania.

Z przeprowadzonej w Resorcie Finansów oceny poziomu dojrzałości cyberbezpieczeństwa wynika, że instytucja osiągnęła status GOTOWY do spełnienia wymogów dyrektywy NIS2, z uwagi na fakt, iż podmiot spełnia minimalne wymagania we wszystkich obszarach zgodności objętych oceną. Dalsze działania będą koncentrować się na utrzymaniu osiągniętego poziomu zgodności, dalszym rozwoju kompetencji pracowników, inwestycjach w systemy cyberbezpieczeństwa oraz ciągłym monitorowaniu ryzyk, co pozwoli na zwiększenie odporności instytucji na zagrożenia cybernetyczne oraz zapewnienie ciągłości realizacji jej zadań.

W obszarze cyberbezpieczeństwa związanego z informacjami niejawnymi w 2025 roku zastosowane rozwiązania organizacyjne oraz środki bezpieczeństwa zadziałały zgodnie z założeniami, w tym skutecznie zmitygowały ryzyko do poziomu rezydualnego. Przeprowadzone audyty bezpieczeństwa systemu w obszarze informacji niejawnych potwierdziły skuteczność zastosowanych zabezpieczeń.

Departament Audytu Środków Publicznych Ministerstwa Finansów realizujący zadania Instytucji Audytowej, w zakresie cyberbezpieczeństwa wykonywał m. in. audyty bezpieczeństwa systemów informatycznych, w instytucjach biorących udział w dystrybucji środków pochodzących z budżetu UE. W 2025 r. przeprowadzono audyty 7 systemów informatycznych w 6 instytucjach (Instytucjach Zarządzających i Pośredniczących w programach Polityki Spójności PF 2021-2027), audyt certyfikacyjny w obszarze Informacja i komunikacja: Bezpieczeństwo systemów informacyjnych w zakresie Wspólnej Polityki Rolnej oraz 11 audytów w instytucjach odpowiedzialnych za realizację reform/ inwestycji KPO o obszarze ochrony danych osobowych.

Ministerstwo Finansów realizowało również zadania z zakresu cyberhigieny oraz działania informacyjne. Przykłady publikacji:

- Ostrzeżenie przed fałszywymi mailami dotyczącymi płatności za przejazd w systemie e-TOLL (24.03.2025), link: https://etoll.gov.pl/artykuly/ostrzezenie-przed-falszywymi-mailami-dotyczacymi-platnosci-za-przejazd-w-systemie-e-toll-1/

- Ostrzeżenie przed podejrzanymi SMS-ami dotyczącymi płatności w e-TOLL (3.04.2025), link: https://etoll.gov.pl/artykuly/ostrzezenie-przed-podejrzanymi-sms-ami-dotyczacymi-platnosci-w-e-toll/
- Zidentyfikowanie nielegalnych domen podszywających się pod serwis e-TOLL, (22-28.04.2025), zamieszczono na stronie https://etoll.gov.pl/ alert po wejściu na stronę dotyczący pojawienia się domen podszywających się pod serwis e-TOLL.
- Zgłoszenie informacji o fałszywych SMS otrzymywanych przez klientów dot. konieczności „wyrównania salda opłat drogowych" (1 oraz 4 lipca2025 r.), zamieszczono na stronie https://etoll.gov.pl/ alert z ostrzeżeniem przed podejrzanymi SMS-ami dotyczącymi płatności w e-TOLL.

KLUCZOWE PROJEKTY I INICJATYWY:

Projekt A: Audyty bezpieczeństwa systemów informatycznych wykorzystywanych w perspektywie finansowej 2021-2027.

Realizacja na podstawie rodziny norm ISO 27000 audytów bezpieczeństwa głównych i lokalnych systemów informatycznych agregujących dane w zakresie wykorzystania środków programów polityki spójności PF 2021-2027, w celu dokonania oceny Kluczowego Wymogu 6 i ustanowionych w instytucjach SZBI. Zadania zakończone, wydano rekomendacje które częściowo zostały wdrożone. Niewdrożone rekomendacje są monitorowane i będą przedmiotem audytu follow-up w 2026 roku.

Projekt B: Ocena kryteriów akredytacyjnych w zakresie bezpieczeństwa systemów informatycznych wykorzystywanych do obsługi środków w ramach Wspólnej Polityki Rolnej.

Realizacja na podstawie rodziny norm ISO 27000 audytu bezpieczeństwa systemów informatycznych w instytucji odpowiedzialnej za dystrybucję środków Wspólnej Polityki Rolnej (Agencji Restrukturyzacji i Modernizacji Rolnictwa). Audyt obejmował wybrane obszary SZBI, systemy dziedzinowe oraz systemy raportowania wyników. Zadanie zakończone, wydano rekomendacje, które zostały wdrożone.

Projekt C: Audyt reform i inwestycji w ramach Krajowego Plan Odbudowy.

Organ Odpowiedzialny za Audyt przeprowadził audyt reform i inwestycji w ramach Krajowego Planu Odbudowy w celu dokonania oceny Kluczowego Wymogu 6, w tym oceny obszaru ochrony danych osobowych na podstawie wymagań normy ISO/IEC 27002. Badaniem objętych zostało 11 instytucji odpowiedzialnych za realizację reform/ inwestycji. Zadania zakończone, wydano rekomendacje, które częściowo zostały wdrożone. Niewdrożone rekomendacje są monitorowane i będą przedmiotem audytu follow-up w 2026 roku.

Projekt D: Budowa Platformy Wysokiej Dostępności dla usług IT Resortu Finansów i administracji publicznej.

Głównym celem projektu jest zapewnienie zwiększonej dostępności i ciągłości działania systemów informatycznych wspierających krytyczne/kluczowe usługi biznesowe świadczone przez administrację publiczną na rzecz jej interesariuszy poprzez budowę publicznych systemów informatycznych. Obecnie trwa proces pozyskania infrastruktury niezbędnej do realizacji projektu. Ponadto w ramach prowadzonych prac finalizowane są założenia architektoniczne, budowane są środowiska testowe oraz trwają prace wdrożeniowe.

Projekt E: PIIO KAS – niejawny system teleinformatyczny wdrożony i funkcjonujący w Krajowej Administracji Skarbowej w całej Polsce.

Nadzór systemu służącego do wspomagania realizacji zadań w zakresie zwalczania przestępczości ekonomicznej i nadużyć finansowych. Infrastruktura systemu zintegrowana jest z zewnętrznymi podmiotami (dostawcami) oraz instytucjami rządowymi. Wdrożenie systemu podniosło efektywność i usprawniło działania w obszarze zwalczania przestępczości.

Projekt F: Wdrożenie Zapasowego Centrum Przetwarzania Danych SPOE KAS

Celem projektu było zapewnienie ciągłości działania SPOE KAS poprzez uruchomienie środowiska Zapasowego CPD. W ramach prac projektowych w dniu 25.03.2025 nastąpiło uruchomienie środowiska Zapasowego CPD SPOE KAS. W wyniku wdrożenia uzyskano poniższe efekty w zakresie SPOE KAS:

1) Minimalizowanie utraty danych, minimalizacja niedostępności systemu oraz zabezpieczenie wpływów do KFD.
2) Spełnienie wymogów bezpieczeństwa w zakresie Polityki Bezpieczeństwa Teleinformatycznego Ministerstwa Finansów.
3) Zabezpieczenie działania Systemu Poboru Opłaty Elektronicznej Krajowej Administracji Skarbowej.

OBSERWOWANE TRENDY I WYZWANIA:

Trend 1: Prace związane z planowanym wdrożeniem CSIRT sektorowego (Sektorowego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego) w Resorcie Finansów to kluczowy element wdrażania unijnej dyrektywy NIS 2 oraz nowelizacji UKSC.

Opis: Planowanym celem jest stworzenie wyspecjalizowanych zespołów dla Resortu Finansów, które będą wspierać MF jako operatora usług kluczowych i ważnych. Powołanie tych struktur ma na celu szybszą reakcję na cyberataki, lepsze monitorowanie zagrożeń w konkretnych branżach oraz efektywniejsze wsparcie dla Ministerstwa Finansów, które są kluczowe dla funkcjonowania gospodarki i państwa.

Trend 2: Wzrost ataków kierowanych do interesariuszy Resortu Finansów

Opis: Zaobserwowało znaczny wzrost fałszywych mali i wiadomości sms kierowanych do interesariuszy Resortu Finansów np. do lipca 2025 roku dotyczących płatności za przejazd w systemie e-TOLL oraz zwiększoną liczbę maili z kategorii "spam terrorystyczny" (maile z groźbami).

URZĄD OCHRONY DANYCH OSOBOWYCH (UODO)

PODSUMOWANIE ROCZNE:

Rok 2025 był dla UODO czasem intensywnych działań zarówno w związku z pracami legislacyjnymi nad nowelizacją UKSC jak i wobec wzrostu liczby zgłaszanych skarg i naruszeń, w tym związanych z naruszeniami ochrony danych osobowych w wyniku incydentów.

W swoich wystąpieniach w toku prac legislacyjnych Prezes UODO zwracał uwagę na ryzyka związane z użyciem nowych technologii w kontekście cyberbezpieczeństwa i konieczność przeprowadzania analizy ryzyka dla przetwarzanych danych osobowych z uwagi na wysokie ryzyko naruszenia praw lub wolności osób. W uwagach do Projektu Strategii Cyberbezpieczeństwa organ nadzorczy wskazał m.in. na konieczność wdrażania rozwiązań zapobiegających kradzieży tożsamości, ochrony przed technologiami śledzącymi czy podszywaniem się pod osoby przy użyciu narzędzi sztucznej inteligencji.

Prezes UODO sygnalizował też konieczność uwzględnienia celów, ról i uprawnień istniejących organów nadzorczych właściwych dla poszczególnych sektorów oraz horyzontalnych obszarów sprawowanego nadzoru i przejrzystego ukształtowania zakresu współpracy w obszarze stosowania aktów unijnych.

KLUCZOWE PROJEKTY I INICJATYWY:

Projekt A: Rozszerzenie funkcjonalności Systemu S46 – dokonywanie zgłoszeń naruszeń ochrony danych osobowych

Wspólnie z MC i NASK-PIB podjęto inicjatywę rozszerzenia funkcjonalności Systemu S46 – narzędzia wykorzystywanego przez podmioty KSC do wymiany informacji o incydentach, podatnościach i cyberzagrożeniach. W 2025 r. wdrożono w Systemie S46 formularz do dokonywania zgłoszeń naruszeń ochrony danych osobowych. Prace te realizowane są w ramach implementacji dyrektywy NIS 2 do polskiego porządku prawnego.

Projekt B: Ustalenie ram prawnych określających współpracę przy zgłaszaniu naruszeń ochrony danych osobowych za pomocą Systemu S46

Rozszerzenie funkcjonalności Systemu S46 wymagało ustalenia ram prawnych określających współpracę przy zgłaszaniu naruszeń ochrony danych osobowych. W tym celu w projekcie ustawy o zmianie UKSC cyberbezpieczeństwa oraz niektórych innych ustaw wprowadzono przepisy zapewniające podstawę prawną do dokonywania zgłoszenia naruszenia ochrony danych osobowych, o których mowa w art. 33 rozporządzenia 2016/679 i art. 44 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2023 r. poz. 1206) przez podmioty kluczowe lub podmioty ważne.
Nadto, w listopadzie 2025 r. Prezes UODO i Minister Cyfryzacji podpisali Porozumienie w sprawie współpracy przy zgłaszaniu naruszeń ochrony danych osobowych za pomocą systemu S46, które m.in. określa zasady współadministrowania danymi w nim przetwarzanymi.

Projekt C: XV edycja programu „Twoje dane – Twoja sprawa"

W 2025 r. przeprowadzono XV edycję programu „Twoje dane - Twoja sprawa", w który zaangażowanych było 5921 nauczycieli, a 61348 uczniów wzięło udział łącznie w 4378 lekcjach na temat ochrony danych osobowych. Nauczyciele i uczniowie podjęli łącznie 6213 działań edukacyjnych, w tym 449 z okazji Dnia

Ochrony Danych Osobowych. Koordynatorzy Programu kontynuowali cykl #ODOlekcji – zajęć w formie online, w trakcie których starano się podejmować szczególnie bliskie uczniom i osobom odpowiedzialnym za ich bezpieczeństwo zagadnienia. Tematem pierwszej przeprowadzonej w 2025 r. lekcji była „Świadomość rodzica i dobre wsparcie dla dziecka – ważne informacje o danych osobowych i prywatności w cyfrowym świecie". Wśród tematów zajęć znalazły się również zagadnienia dotyczące m.in. cyfrowych śladów i ochrony wizerunku. Ogromnym zainteresowaniem cieszyło się webinarium „Naruszenie prywatności w mediach społecznościowych – mediacje jako narzędzie ochrony danych osobowych i rozwiązywania konfliktów?".

W ramach Programu uczestnicy otrzymują dostęp do materiałów edukacyjnych, które stanowią źródło praktycznej wiedzy z zakresu ochrony danych osobowych w cyberprzestrzeni i życiu realnym.

Wśród publikowanych materiałów jest cykl porad „Warto wiedzieć" skierowany do uczniów, nauczycieli i rodziców. W XV edycji opublikowane zostały m.in. porady na temat:

- „Ryzyko udostępniania wizerunku dzieci w sieci",
- „Bezpieczeństwo w cyfrowym świecie. Jak dbać o prywatność w internecie?",
- „AI w placówkach oświatowych a dane osobowe. Jak chronić dane osobowe w edukacji w dobie rozwoju sztucznej inteligencji?",
- „Cyfrowy ślad - co warto o nim wiedzieć i jak go kontrolować?".

22–23 października 2025 r. dwudniowa konferencja szkoleniowa zainaugurowała XVI edycję Programu. Motywem przewodnim edycji jest ochrona danych osobowych w dobie dynamicznego rozwoju nowych technologii, ze szczególnym uwzględnieniem sztucznej inteligencji.

20 listopada 2025 r. odbyło się webinarium, w którym Pan Mirosław Wróblewski, Prezes Urzędu Ochrony Danych Osobowych, miał wystąpienie pt. „Twój wizerunek i Twoje dane – jak nie stracić kontroli, korzystając z nowych aplikacji?".

Program stanowi odpowiedź na rzeczywiste wyzwania edukacyjne we współczesnej rzeczywistości cyfrowej. Aktywnie angażuje uczniów i nauczycieli, wspierając rozwój ich kompetencji oraz budowanie odpowiedzialnych postaw podczas korzystania z nowoczesnych technologii.

OBSERWOWANE TRENDY I WYZWANIA:

Trend 1: Zwiększenie liczby skarg i naruszeń ochrony danych w wyniku incydentów

Opis: W 2025 r. istotnie zwiększyła się liczba zgłaszanych do Prezesa UODO skarg i naruszeń ochrony danych związanych z incydentami. Najczęstszą przyczyną takich naruszeń było niewdrożenie odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający zidentyfikowanemu ryzyku.

Trend 2: Naruszenia związane z użyciem narzędzi opartych o AI

Opis: W 2025 r. do Prezesa UODO zgłoszono naruszenia związane z nieuprawnionym przetwarzaniem danych osobowych przy użyciu narzędzi wykorzystujących AI. Należy założyć wzrostową tendencję tego typu naruszeń, nie tylko z uwagi na złośliwe wykorzystanie AI, ale również z uwagi na znaczące ilości danych przetwarzanych przez takie systemy, jak też ich upowszechnienie. Deepfake może być też wykorzystywany do omijania systemów bezpieczeństwa, takich jak systemy uwierzytelniania biometrycznego, co może stanowić bezpośrednie zagrożenie dla bezpieczeństwa systemów informacji podmiotów publicznych i prywatnych.

ANALIZA I OCENA FUNKCJONOWANIA KSC:

Na poziomie krajowym i sektorowym UODO współpracuje z organami właściwymi do spraw cyberbezpieczeństwa, zgodnie z art. 34 ust. 2 i art. 39 ust. 7 UKSC (Dz.U. z 2026 r., poz. 20).

UODO przykłada również dużą uwagę do szkoleń z zakresu cyberbezpieczeństwa. W 2025 r. tematyka cyberhigieny, zagrożeń wynikających ze stosowania nowych technologii oraz cyberszpiegostwa stanowiła element szkolenia pracowników przeprowadzanego przez ABW.

REKOMENDACJE NA 2026 - REKOMENDACJE DLA PEŁNOMOCNIKA RZĄDU DS. CYBERBEZPIECZEŃSTWA:

Z perspektywy Prezesa UODO w 2025 r. najpoważniejsze zagrożenia wynikały z nieprzeprowadzania analiz ryzyka, a w konsekwencji niewdrażaniu przez administratorów odpowiednich środków technicznych i organizacyjnych, co wielokrotnie skutkowało nakładaniem administracyjnych kar pieniężnych (treść decyzji udostępniana jest pod adresem https://orzeczenia.uodo.gov.pl).

Należy też zwrócić uwagę na ryzyka związane z upowszechnieniem urządzeń IoT oraz danych w przemyśle motoryzacyjnym. Zarówno urządzenia domowe, jak i urządzenia wearables, a także pojazdy w coraz większym stopniu wykorzystują znaczne ilości danych, w tym danych osobowych szczególnych kategorii (np. o stanie zdrowia). Wszystkie przedmioty internetu rzeczy podłączone do sieci mogą przekazywać dane w sposób niekontrolowany, jak również – z uwagi na brak wsparcia producentów i aktualizacji – mogą stanowić zagrożenie dla innych urządzeń sieciowych. Mając powyższe na uwadze rekomendowane jest zintensyfikowanie działań w celu uwzględnienia ochrony danych w fazie projektowania systemów teleinformatycznych, jak też zapewnienia domyślnej ochrony danych. Szczególną uwagę należy też zwrócić na obowiązek regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Z zagrożeń systemowych, widocznych z poziomu Prezesa UODO, należy wymienić niewystarczające zasoby do realizacji zadań z obszaru zabezpieczenia cybernetycznego w podmiotach sektora publicznego. Zapewnienie prawidłowego zabezpieczenia cyberprzestrzeni w instytucjach publicznych stanowi ogromne wyzwanie z uwagi na zwiększającą się liczbę zagrożeń przy niewystarczających zasobach kadrowych i płacowych.

REALIZOWANE DZIAŁANIA W ZAKRESIE ZAPEWNIENIA CYBERBEZPIECZEŃSTWA NA POZIOMIE KRAJOWYM

ROZWÓJ KSC

MAPA POLSKIEGO SEKTORA CYBERBEZPIECZEŃSTWA

Krajowe Centrum Kompetencji Cyberbezpieczeństwa zleciło również prace badawcze mające na celu zobrazowanie liczebności i charakterystyki polskiego sektora cyberbezpieczeństwa. W wyniku tych działań zidentyfikowano i zmapowano podmioty działające w obszarze cyberbezpieczeństwa z uwzględnieniem rodzaju podmiotu, jego lokalizacji, specjalizacji czy zasięgu działalności. Osobna baza stworzona została dla sektora MŚP jako najliczniejszego. Druga z baz dotyczy natomiast dużych przedsiębiorstw, uczelni, organizacji badawczych, podmiotów publicznych, NGO, organizacji normalizacyjnych i innych podmiotów działających w obszarze cyberbezpieczeństwa.

Przedsięwzięcie ułatwi planowanie przyszłych działań NCC-PL skierowanych do krajowego ekosystemu cyberbezpieczeństwa.

PROGRAM CYBERSECIDENT

W 2025 r. kontynuowano realizację programu CYBERSECIDENT „Cyberbezpieczeństwo i eTożsamość", którego celem jest wytwarzanie rozwiązań nakierowanych na podniesienie poziomu bezpieczeństwa cyberprzestrzeni RP. Realizowane zadania polegały na koordynacji procesu zawierania umów, w wyniku których Minister Cyfryzacji nabył autorskie prawa majątkowe do rozwiązań w obszarze cyberbezpieczeństwa wypracowanych w ramach programu, a także procesu udzielania wykonawcy licencji na ww. rozwiązania

PROMOCJA KRAJOWEGO SYSTEMU CERTYFIKACJI CYBERBEZPIECZEŃSTWA

Przedstawiciele urzędu obsługującego Pełnomocnika promowali nowe inicjatywy w zakresie utworzonego krajowego systemu certyfikacji cyberbezpieczeństwa. W ramach tych działań m.in. wystąpili na konferencji informatycznej „The Hack Summit 2025" z prezentacją dotyczącą krajowego systemu certyfikacji cyberbezpieczeństwa i szans jakie certyfikacji oferuje przedsiębiorcom. Ponadto zorganizowane zostały 2 wydarzenia dotyczące certyfikacji cyberbezpieczeństwa:

- Wymagania cyberbezpieczeństwa dla oprogramowania i sprzętu sektora ochrony zdrowia zorganizowane wspólnie z Naukową i Akademicką Siecią Komputerową – Państwowym Instytutem Badawczym.
- Szkolenie z zakresu metodologii Common Criteria zorganizowane we współpracy z Instytutem Łączności – Państwowym Instytutem Badawczym.

PLANY DZIAŁAŃ PRZEDSIĘBIORCÓW TELEKOMUNIKACYJNYCH W SYTUACJI SZCZEGÓLNEGO ZAGROŻENIA

Ministerstwo Cyfryzacji w 2025 r. realizowało stałe zadanie w zakresie uzgadniania planów działania przedsiębiorców telekomunikacyjnych w sytuacji szczególnego zagrożenia. Obowiązek sporządzenia planu i zakres uzgodnień obecnie wynika z art. 39 ust. 2 ustawy Prawo komunikacji elektronicznej oraz rozporządzenia Rady Ministrów z dnia 19 sierpnia 2020 r. w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych. Posiadanie planu działań jest istotne z punktu widzenia potrzeby efektywnego reagowania na przypadki wystąpienia sytuacji kryzysowych, stanów

nadzwyczajnych i bezpośrednich zagrożeń dla bezpieczeństwa lub integralności infrastruktury telekomunikacyjnej[18]. Zadanie to będzie kontynuowane w 2026 r.

W 2025 r. Ministerstwo Cyfryzacji kontynuowało prace legislacyjne nad projektem rozporządzenia Rady Ministrów w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń, które ma dostosować istniejące przepisy do uchwalonej w 2024 r. ustawy - Prawo komunikacji elektronicznej.

CENTRUM ROZOWOJU KOMPETENCJI CYFROWYCH MC (CRKC)

CRKC we współpracy z NASK zrealizowało w 2025 zadania będące kontynuacją zadań opisanych w ubiegłorocznym sprawozdaniu. W tym 3 główne działania w zakresie przeciwdziałania dezinformacji w ramach dotacji dla NASK:

- Monitoring treści o potencjale dezinformacyjnym w mediach społecznościowych i stronach internetowych oraz prace rozwojowe nad budowaniem odporności administracji publicznej oraz społeczeństwa wobec zjawiska dezinformacji poprzez działania naukowe i edukacyjne. (umowa nr 75/CRKC/25 z dnia 11.02.2025 r.).
- Osłona informacyjna kampanii Wyborczej w 2025 r. (umowa nr 92/CRKC/25 z dnia 17.02.2025 r.).
- Broń się w Necie – konkurs dla uczniów szkół średnich – działanie wzmacniające odporność społeczeństwa na dezinformację (umowa nr 262/CRKC/25 z dnia 24.06.2025 r.).

„OSŁONA INFORMACYJNA KAMPANII WYBORCZEJ 2025 R.” DZIAŁANIA BYŁY REALIZOWANE W OKRESIE STYCZEŃ – PAŹDZIERNIK 2025 R. A WARTOŚĆ PRZYZNANEJ DOTACJI TO 3 803 092,63 ZŁ.

W związku z realizowanym zadaniem publicznym w roku 2025 Naukową i Akademicką Sieć Komputerową w ramach zadania publicznego realizowała:

- rozbudowę i utrzymanie przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy (NASK-PIB) w roku 2025 strony http://www.bezpiecznewybory.pl/. Serwis ten jest skoncentrowany na szkodliwych treściach wyborczych, pełniąc rolę wiarygodnego kanału do wykrywania, weryfikacji informacji. Serwis stanowił miejsce zgłaszania treści szkodliwych do właścicieli mediów społecznościowych oraz umożliwiał publikację artykułów specjalistycznych. Można było w nim znaleźć zweryfikowane treści, potwierdzone u źródła informacje na temat procesu wyborczego oraz poradniki i wskazówki.
- Weryfikację treści przesłanych od użytkowników serwisu i obywateli.
- Realizowano regularny monitoring polskojęzycznych mediów społecznościowych w okresie przedwyborczym i w dniu wyborów prezydenckich.
- Przygotowano raporty badawcze z okresu wyborów prezydenckich 2025 r. oraz dodatkowe raporty analityczne obejmujące główne narracje i aktorów zaangażowanych w dezinformację w okresie przedwyborczym.

[18] "Z tego względu plan powinien zawierać, m.in. zasady współpracy z innymi przedsiębiorcami telekomunikacyjnymi, z podmiotami i służbami wykonującymi zadania w zakresie ratownictwa, niesienia pomocy ludności, a także zadania na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego; wykaz przygotowanych technicznych i organizacyjnych środków zapewnienia bezpieczeństwa i integralności infrastruktury telekomunikacyjnej i świadczonych usług, w tym ochrony przed wystąpieniem incydentów w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa; opis sposobów utrzymania ciągłości świadczenia usług telekomunikacyjnych lub dostarczania sieci telekomunikacyjnej oraz ich odtworzenia w przypadku utraty możliwości świadczenia tych usług (ważne, w sytuacji świadczenia usług dla służb ratowniczych oraz wykonujących zadania na rzecz bezpieczeństwa i obronności państwa)."

- Przeprowadzono szkolenia związane z identyfikacją treści dezinformacyjnych dla Komitetów Wyborczych oraz pracowników ambasad RP zaangażowanych w proces wyborczy.
- Wyprodukowano i wyemitowano krótkie filmy edukacyjne dotyczące zachowań związanych z weryfikacją dezinformacji.

Głównym elementem dotacji był monitoring treści publikowanych w polskiej infosferze a także działania edukacyjne i szkoleniowe.

„PARASOL WYBORCZY"

Projekt "Parasol Wyborczy", uruchomiony w lutym 2025 r. z inicjatywy Ministerstwa Cyfryzacji (MC) we współpracy z Ministerstwem Spraw Wewnętrznych i Administracji (MSWiA), objął trzy kluczowe obszary: ochronę przed zagrożeniami w cyberprzestrzeni, **przeciwdziałanie dezinformacji** oraz edukację i współpracę międzyinstytucjonalną. W realizację tego działania włączyły się: MC, Agencja Bezpieczeństwa Wewnętrznego (ABW), Służba Kontrwywiadu Wojskowego (SKW), Ministerstwo Spraw Zagranicznych (MSZ), Centralny Ośrodek Informatyki (COI), poszczególne CSIRT-y (zespoły reagowania na incydenty bezpieczeństwa komputerowego) oraz Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK). Połączenie kompetencji tych podmiotów umożliwiło kompleksowe działania zgodnie z wyznaczonymi im ustawowo zakresami zadań.

„MONITORING TREŚCI O POTENCJALE DEZINFORMACYJNYM W MEDIACH SPOŁECZNOŚCIOWYCH I STRONACH INTERNETOWYCH ORAZ PRACE ROZWOJOWE NAD BUDOWANIEM ODPORNOŚCI ADMINISTRACJI PUBLICZNEJ ORAZ SPOŁECZEŃSTWA WOBEC ZJAWISKA DEZINFORMACJI POPRZEZ DZIAŁANIA NAUKOWE I EDUKACYJNE"

Działania były realizowane w okresie styczeń – grudzień 2025 r. a wartość przyznanej dotacji to 18 132 578,80 zł. W ramach projektu „Monitoring treści o potencjale dezinformacyjnym w mediach społecznościowych i stronach internetowych oraz prace rozwojowe nad budowaniem odporności administracji publicznej oraz społeczeństwa wobec zjawiska dezinformacji poprzez działania naukowe i edukacyjne" w ramach zadania publicznego zrealizowano m.in.:

- Ciągły monitoring infosfery. W tym Analiza i ocena treści pod kątem dezinformacji. Archiwizacja treści w repozytorium. Zgłaszanie wybranych treści do platform społecznościowych, i odpowiednich służb.
- Analizy dezinformacji, Opracowywanie ilościowe oraz/lub jakościowe treści dezinformacyjnych z uwzględnieniem: FIMI, DIMI, infosfery polskiej, rosyjskiej oraz chińskiej.
- Kontynuowane były badania nad wpływem dezinformacji na społeczeństwo oraz badania na temat predykcji trendów w dezinformacji i polaryzacji społecznej, oraz edukacja interesariuszy z administracji publicznej oraz różnych grup społecznych (w tym dzieci i młodzieży) w zakresie przeciwdziałania dezinformacji.

PRZECIWDZIAŁANIE DEZINFORMACJI - PROJEKT „BROŃ SIĘ W NECIE"

Realizowany w 2025 r. przez NASK-PIB we współpracy z Ministrem Cyfryzacji oraz Agencją Bezpieczeństwa Wewnętrznego (ABW) o wartości **2 463 009,05 zł.**
Był to ogólnopolski konkurs edukacyjny dla uczniów szkół ponadpodstawowych, którego celem było zwiększanie świadomości młodzieży na temat cyberprzemocy – ze szczególnym uwzględnieniem mowy nienawiści i hejtu – a także dezinformacji i radykalizacji.
Uczestnicy – w drużynach składających się z 10 uczniów i nauczyciela – realizowali kursy e-learningowe z testami wiedzy, a następnie przygotowywali własne materiały wideo w formie kampanii społecznych. Nagrodzonych zostało aż 55 drużyn – uczniowie otrzymali smartwatche, nauczyciele elektroniczne

notatniki, a szkoły konsole do gier z pełnym wyposażeniem. Gala kończąca projekt i wręczenie nagród zostało przygotowane przez zespół MC w siedzibie KPRM.

„HIGIENA CYFROWA 2025”

CRKC we współpracy z NASK zrealizowało w 2025 roku działania edukacyjne w ramach zadania „Higiena cyfrowa 2025” (umowa nr 155/CRKC/25 z dnia 18.04.2025 r.).

Zadanie publiczne pn. „Higiena cyfrowa 2025” było realizowane od 14 kwietnia do 31 grudnia 2025 r. , na zadanie przekazano dotację w wysokości 1 960 996,49 zł.

Zakresem przedmiotowym zadania było przygotowanie i przeprowadzenie dla uczniów klas IV-VIII szkół podstawowych zajęć o tematyce cyfrowej higieny oraz bezpieczeństwa w sieci. Zajęcia te przeprowadzone były przez nauczycieli przeszkolonych w ramach realizacji niniejszego zadania. Projekt zakładał realizację działań takich jak:

- promowanie higieny cyfrowej jako elementu zdrowego stylu życia,
- pokazywanie zależności pomiędzy zdrowym i zrównoważonym trybem życia a codziennym samopoczuciem i ogólną kondycją w zakresie korzystania z internetu,
- promowanie postaw poprawiających koncentrację, efektywność, poziom energii i zdrowy sen,
- przekazywanie wiedzy na temat bezpieczeństwa w sieci, m.in. cyberzagrożeń i dezinformacji.

W ramach zadania przygotowany został także film edukacyjny dla rodziców dzieci ze szkół podstawowych.

Długofalowym efektem realizacji projektu będzie wzmocnienie kompetencji cyfrowych wśród uczniów szkół podstawowych, ze szczególnym uwzględnieniem higieny cyfrowej i bezpiecznego korzystania z internetu. Dzięki udziałowi w zajęciach uczniowie nauczyli się dostrzegać różnice pomiędzy światem online i offline, zyskali większą kontrolę nad czasem spędzanym w internecie oraz wykształcili nawyki umożliwiające zrównoważone korzystanie z nowych technologii.

„SZKOLENIA Z ZAAWANSOWANYCH KOMPETENCJI CYFROWYCH DLA FUNKCJONARIUSZY I PRACOWNIKÓW POLICJI I PAŃSTWOWEJ STRAŻY POŻARNEJ Z ZAKRESU SZTUCZNEJ INTELIGENCJI, DEZINFORMACJI, CYBERBEZPIECZEŃSTWA, W TYM CYBERHIGIENY”

MC w 2025 roku zleciło do NASK - PIB realizację projektu (umowa nr 261/CRKC/25 z 29.07.2025 r.).

Zadanie było realizowane od 1 sierpnia do 31 grudnia 2025 roku, na zadanie przekazano dotację w wysokości 2 534 575,93 zł. W ramach zadania NASK-PIB przeprowadził specjalistyczne szkolenia w obszarze sztucznej inteligencji, dezinformacji, cyberbezpieczeństwa, w tym cyberhigieny dla poniższych dla poniższych grup odbiorców:

- Policja: funkcjonariusze pełniący służbę w jednostkach organizacyjnych Policji (służby: kryminalna, śledcza, spraw wewnętrznych, prewencyjne (w tym również wyodrębnione oddziały prewencji), kontrterrorystyczne, wspomagające (w tym również pracowników cywilnych)) na wszystkich szczeblach organizacyjnych;
- Państwowa Straż Pożarna (PSP): funkcjonariusze i pracownicy cywilni pełniący służbę/zatrudnieni w jednostkach organizacyjnych Państwowej Straży Pożarnej wymienionych w art. 8 ustawy z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej1, zwanej dalej „Ustawą o PSP”.

Program szkoleń był dopasowany do potrzeb szkoleniowych grup docelowych tak aby zapewnić uczestnikom niezbędną wiedzę oraz umiejętności umożliwiające skuteczne przeciwdziałanie incydentom dezinformacji oraz cyberbezpieczeństwa. Ponadto w zadaniu przewidziano jeszcze zakup i przekazanie

uniwersalnych narzędzi umożliwiających bezpieczne uwierzytelnienie w sieci. Urządzenia te zostały przez NASK-PIB zakupione i przekazane instytucjom objętych szkoleniem.

PROJEKT PN. „SZKOŁA MIĘDZYPOKOLENIOWA"

MC w 2025 roku zleciło do NASK - PIB realizację projektu „Projekt pn. *Szkoła międzypokoleniowa*

Projekt jest realizowany z inicjatywy Ministerstwa Cyfryzacji, we współpracy z Ministerstwem Edukacji Narodowej oraz Ministrem do spraw Polityki Senioralnej. Operatorem projektu jest NASK – Państwowy Instytut Badawczy.

Celem działań jest integracja międzypokoleniowa oraz rozwój kompetencji cyfrowych wśród osób starszych, przy wsparciu i zaangażowaniu uczniów klas VII–VIII szkół podstawowych oraz uczniów szkół ponadpodstawowych.

W okresie realizacji **pilotażu przedsięwzięcia w latach 2024-2025 zorganizowano ponad 5,5 tys. warsztatów edukacyjnych, zaangażowano 1554 szkoły z całej Polski, udział wzięło ponad 20 tysięcy uczestników**, w tym seniorzy i uczniowie. Zajęcia skupiały się na praktycznym rozwijaniu umiejętności korzystania z internetu (w tym z usług cyfrowych), obsługi urządzeń cyfrowych oraz rozpoznawania zagrożeń online. Młodzież pełniła rolę przewodników cyfrowych, dzieląc się wiedzą i wspierając seniorów w nauce, jednocześnie korzystając z możliwości wymiany międzypokoleniowych doświadczeń.

Projekt będzie kontynuowany w kolejnych latach.

PROJEKT SZKOLENIOWY DLA SENIORÓW W SANATORIACH PN. „EFAJFY"

Celem projektu jest przygotowanie i przeprowadzenie pilotażowego cyklu bezpłatnych szkoleń z zakresu bezpieczeństwa w sieci oraz korzystania z e-usług publicznych dla seniorów (60+) przebywających w sanatoriach na terenie Polski, wraz z opracowaniem materiałów edukacyjnych wspierających proces dydaktyczny.

W czasie trwania projektu przeszkolono 1 015 seniorów w 76 sanatoriach. Rezultatem zadania było również merytoryczne i graficzne opracowanie przez NASK-PIB broszury edukacyjno-informacyjnej, stanowiącej element standardu edukacyjnego projektu.

Wśród przykładowych modułów merytorycznych szkoleń w 2025 roku były: wsparcie seniorów w pierwszych krokach z technologią (w tym zakładanie konta e-mail, instalacja komunikatorów oraz swobodniejsze poruszanie się po internecie), przedstawienie korzyści płynących z korzystania z profilu zaufanego oraz e-usług i aplikacji publicznych (w tym m.in. wsparcie w założeniu profilu zaufanego, prezentacja aplikacji mObywatel oraz Internetowego Konta Pacjenta), wprowadzenie w zagadnienia związane z podstawami bezpieczeństwa w internecie, temat phishingu i metody "na wnuczka" oraz zbudowanie pewności siebie oraz poczucia komfortu i bezpieczeństwa w korzystaniu z internetu, realizując codzienne potrzeby online, jak zakupy czy rozrywka.

KAMPANIA RADIOWA PN. *W CYFROWYM ŚWIECIE*

W 2025 roku zrealizowano cykl 8 audycji radiowych emitowanych w 17 Rozgłośniach Regionalnych Polskiego Radia, co sumarycznie dało 136 audycji produkowanych regionalnie. Kampania była skierowana do osób dorosłych, z naciskiem na ludzi w wieku 55+.

Kampania miała na celu m.in. zachęcenie obywateli do ciągłego podnoszenia kompetencji cyfrowych, podnoszenie świadomości obywateli o zagrożeniach i problemach występujących w świecie cyfrowym oraz zbudowanie przekonania o konieczności świadomego i bezpiecznego korzystania z szeroko rozumianej technologii.

ROZWÓJ APLIKACJI MOBYWATEL

W 2025 r. udostępniono w aplikacji **mObywatel** nową usługę, która umożliwia szybki i wygodny zapis na bezpłatne, dobrowolne szkolenia obronne, organizowane przez Ministerstwo Obrony Narodowej.

Program obejmuje różne moduły, w tym **moduł z zakresu cyberbezpieczeństwa**, określany również jako **kurs cyberhigieny**. Szkolenie ma na celu zwiększyć świadomość zagrożeń cyfrowych i wyrobić praktyczne umiejętności, które pozwolą ochronić użytkownika i jego dane przed atakami cyfrowymi.

Użytkownicy mogą wybrać lokalizację szkolenia na udostępnionej mapie, zapoznać się z zakresem kursu i zgłosić udział bezpośrednio poprzez aplikację. Szkolenia nie wymagają wcześniejszego przygotowania i nie są związane ze służbą wojskową ani składaniem przysięgi.

W szkoleniach mogą wziąć udział wszyscy pełnoletni obywatele Polski, którzy mają mDowód. Aby zapisać się przez aplikację, użytkownik:

1. wchodzi w Usługi i wybiera Szkolenia obronne,
2. wybiera Indywidualne szkolenia obronne,
3. zapoznaje się z wyświetlonymi informacjami i naciska przycisk Zgłoś się,
4. wybiera z listy rozwijanej typ szkolenia (podstawowy kurs bezpieczeństwa, kurs przetrwania, kurs medyczny lub kurs cyberhigieny),
5. wskazuje na mapie miejsce, w którym chce odbyć szkolenie,
6. zapoznaje się z informacjami o dacie i podmiocie, który realizuje szkolenie, a następnie potwierdza swój wybór, wybierając Dalej,
7. podaje swoje dane kontaktowe.

Po wykonaniu tych czynności zgłoszenie zostaje zarejestrowane.

Jeśli wybrane szkolenie cieszy się dużą popularnością, użytkownik zostanie zapisany na listę rezerwową. Po poprawnym zapisie uczestnik otrzyma potwierdzenie na wskazany w zgłoszeniu adres e- mail.

W aplikacji użytkownik może przejrzeć szkolenia, na które jest zapisany. Jeśli użytkownik nie może wziąć udziału w szkoleniu, może z niego zrezygnować.

Po zakończeniu zajęć uczestnicy otrzymują certyfikat, który potwierdza nowe umiejętności.

PRACE NAD DOKUMENTEM STRATEGICZNYM W DZIEDZINIE INFORMATYZACJI PAŃSTWA

Strategia Cyfryzacji Państwa wyznacza cele i działania w najważniejszych obszarach cyfryzacji państwa, gospodarki i społeczeństwa. Nadrzędnym celem jest poprawa jakości życia obywateli dzięki cyfryzacji.

Dokument ten zostanie przyjęty na mocy ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne (art. 12aa), a w jej realizację i wdrażanie będą zaangażowani członkowie Rady Ministrów, pełnomocnicy do spraw informatyzacji oraz Komitet do spraw Cyfryzacji.

W pracy nad dokumentem zidentyfikowano kluczowe (horyzontalne) obszary, stanowiące czynniki o fundamentalnym wpływie na realizację celu głównego tj. zapewnienie cyberbezpieczeństwa, zapewnienie dostępu do szybkich, wydajnych i bezpiecznych usług telekomunikacyjnych, a także wzmocnienie kompetencji przyszłości oraz poprawa koordynacji cyfrowej transformacji kraju. Horyzontalne obszary mają również kluczowe znaczenie dla powodzenia realizacji pozostałych szczegółowych celów Strategii Cyfryzacji, które zostały zgrupowane w trzech kategoriach: Państwo, Ludzie oraz Biznes i nowe technologie.

Szczególną rolę w procesie wdrażania i realizacji Strategii odegrają pełnomocnicy ds. informatyzacji, powoływani w urzędach obsługujących ministrów kierujących działami administracji rządowej oraz

w Kancelarii Prezesa Rady Ministrów, których głównymi zadaniami będzie koordynacja realizacji strategii, nadzorowanie jej wdrażania oraz diagnozowanie obszaru koniecznych zmian w zakresie działu.

Na aktualnym etapie prac Ministerstwo Cyfryzacji analizuje otrzymane w toku konsultacji publicznych, uzgodnień i opiniowania uwagi do projektu Strategii, znacząco zmienionego w efekcie prekonsultacji z udziałem licznych interesariuszy.

Więcej informacji pod adresem: https://www.gov.pl/web/cyfryzacja/strategia-cyfryzacji-panstwa-startuja-ponowne-konsultacje-projektu

KRAJOWY PLAN DZIAŁANIA DO PROGRAMU POLITYKI „DROGA KU CYFROWEJ DEKADZIE" DO 2030 R.

Ministerstwo Cyfryzacji, we współpracy z właściwymi interesariuszami na poziomie krajowym, opracowało Krajowy plan działań do programu polityki „Droga ku cyfrowej dekadzie" do 2030 r., który został przyjęty uchwałą nr 125 Rady Ministrów z dnia 22 października 2024 r. i został opublikowany w Monitorze Polskim poz. 989. Przyjęcie planu jest odpowiedzią na zobowiązania wynikające z Decyzji Parlamentu Europejskiego i Rady (UE) 2022/2481 z dnia 14 grudnia 2022 r. ustanawiającej program polityki „Droga ku cyfrowej dekadzie" do 2030 r. Celem programu „Droga ku cyfrowej dekadzie" jest osiągnięcie wspólnych dla całej Unii Europejskiej celów cyfrowych do 2030 roku.

Projekt Krajowego planu wskazuje m.in. na wdrożone i planowane polityki, interwencje i działania, które Polska zobowiązuje się podjąć w celu przyśpieszenia transformacji cyfrowej, zmierzając do osiągnięcia celów ogólnych i celów cyfrowych programu polityki „Droga ku cyfrowej dekadzie" do 2030 r. Jednym z celów ogólnych ww. programu polityki jest poprawa odporności na cyberataki, przyczynianie się do zwiększenia świadomości ryzyka oraz szerzenia wiedzy na temat procedur cyberbezpieczeństwa, przy intensyfikacji wysiłków organizacji publicznych i prywatnych.

Aktualnie finalizowane są prace w zakresie rewizji Krajowego planu działania do programu polityki „Droga ku cyfrowej dekadzie" do 2030 r. Polska, tak jak wszystkie państwa członkowskie, zobowiązana jest przedłożyć Komisji korektę dokumentu, zgodnie z rekomendacjami zawartymi w sprawozdaniu krajowym, w ramach raportu na temat stanu cyfrowej dekady. Rewizja Krajowego Planu Działania zostanie przyjęta na mocy uchwały Rady Ministrów zmieniającej uchwałę nr 125 Rady Ministrów z dnia 22 października 2024 r. w sprawie Krajowego planu działania do programu polityki „Droga ku cyfrowej dekadzie" do 2030 r.

Więcej informacji pod adresem: https://www.gov.pl/web/cyfryzacja/program-polityki-droga-ku-cyfrowej-dekadzie-do-2030-r2

PODNIESIENIE POZIOMU ODPORNOŚCI SYSTEMÓW INFORMACYJNYCH ADMINISTRACJI PUBLICZNEJ I SEKTORA PRYWATNEGO ORAZ OSIĄGNIĘCIE ZDOLNOŚCI DO SKUTECZNEGO ZAPOBIEGANIA I REAGOWANIA NA INCYDENTY

CERTYFIKACJA W CYBERBEZPIECZEŃSTWIE

W 2025 r. ponownie zlecono realizację zadania pn. „Realizowanie zadań uczestnika oraz akredytowanej Jednostki Certyfikującej spełniającej wymagania". NASK-PIB, w ramach udzielonej dotacji, realizował zadania na poziomie operacyjnym polegające na wykonywaniu w imieniu Rządu RP zadań Uczestnika w ramach Umowy o wzajemnym uznawaniu certyfikatów oceny bezpieczeństwa teleinformatycznego oraz w ramach Porozumienia w sprawie uznawania Certyfikatów Common Criteria w dziedzinie bezpieczeństwa teleinformatycznego, a także wykonywaniu zadań Jednostki Certyfikującej Spełniającej Wymagania (ang. Compliant Certification Body), odpowiedzialnej za zarządzanie Programem Oceny i Certyfikacji Bezpieczeństwa IT oraz za autoryzację laboratoriów badawczych.

Ponadto, zlecono realizację zadania pn. „Działania związane z funkcjonowaniem Europejskiej Ramy Certyfikacji cyberbezpieczeństwa w Polsce: 1. w europejskim programie certyfikacji cyberbezpieczeństwa zgodnym z Common Criteria (EUCC), 2. przygotowanie do wspierania krajowego organu ds. certyfikacji cyberbezpieczeństwa i krajowego systemu certyfikacji cyberbezpieczeństwa". Celem działań IŁ-PIB w ramach zadania było zapewnienie dla Laboratorium Oceny Bezpieczeństwa Produktów Teleinformatycznych w IŁ-PIB poziomu uzasadnienia zaufania „wysoki", czyli wyższego poziomu z CSA. Wskazaniem IŁ-PIB do realizacji zadania było zwiększanie przedmiotowe poziomu wysokiego uzasadnienia zaufania w dokumentach na poziomie europejskim w najbliższych latach – nowe obowiązki nakłada Akt o cyberodporności (CRA), Dyrektywa NIS 2 i Rozporządzenie UE o Sztucznej Inteligencji (AI Act). Aby zapewnić realną możliwość przeprowadzania certyfikacji oraz rozwijać rynek certyfikacji w Polsce, konieczny jest rozwój jednostek certyfikacyjnych oraz laboratoriów.

PARTNERZY PWCYBER WZMACNIAJĄ WSPÓŁPRACĘ NA RZECZ CYBERBEZPIECZEŃSTWA POLSKI

W 2025 r. Ministerstwo Cyfryzacji kontynuowało współpracę o charakterze partnerstwa publiczno-prywatnego w ramach Programu Współpracy w Cyberbezpieczeństwie (PWCyber) uruchomionego w 2019 r. Kluczowym obszarem współpracy w ramach partnerstwa jest podnoszenie kompetencji podmiotów KSC w zakresie świadomości zagrożeń, metod ataków w cyberprzestrzeni oraz prawnych, organizacyjnych i technicznych umiejętności przeciwdziałania zagrożeniom w systemach i sieciach teleinformatycznych

Program PWCyber nie zwalnia tempa. W gronie partnerów przybywa firm, które w sposób aktywny działają na rzecz poprawy cyberbezpieczeństwa w Polsce. Od momentu powstania w 2019 roku, rozrósł się on do ponad 60 partnerów. Statystyki pokazują dynamiczny rozwój wspólnych inicjatyw. W 2025 roku do grona partnerów Programu PWCyber dołączyło 12 firm: Mastercard Europe SA, Tekniska Polska Przemysłowe Systemy Transmisji Danych Sp. z o.o., Rublon sp. z o.o., Kyndryl Global Services Delivery Centre Polska Sp. z o. o, Integrity Partners sp. z o.o., Uniteam sp. z o .o., P4 sp. z o.o. (Play), Euvic Solution sp. z o.o., Siltec sp. z o.o., Visa Technology Europe sp. z o.o., IDENTT Sp. z o.o., oraz T-mobile Polska S.A.

W wyniku ewaluacji Programu PWCyber wprowadzono Regulamin oraz ankietę kwalifikacyjną dla kandydatów chcących dołączyć do Programu.

W ramach współpracy odbywały się warsztaty techniczne, wizyty studyjne oraz spotkania.

27 stycznia 2025 r. pracownicy Departamentu Cyberbezpieczeństwa odbyli **wizytę studyjną w Europejskim Centrum Cyberbezpieczeństwa - European Cyber Resilience Centre firmy Mastercard** w Waterloo pod Brukselą.

Ilustracja 2 Wizyta studyjna w Europejskim Centrum Cyberbezpieczeństwa

Podczas wizyty zwiedzono m.in. Fusion Centre odpowiedzialne za reagowanie na incydenty organizacyjne Mastercard oraz CSI Lab - laboratorium kryminalistyki cyfrowej. Podczas spotkań zaprezentowane zostały usługi i produkty oferowane przez firmę oraz jej partnerów z obszaru cyberbezpieczeństwa m.in. z zakresu cyber threat intelligence (bieżącej analizy zagrożeń), czy analizy ryzyka. Warsztaty były okazją do wymiany wiedzy i doświadczeń na temat aktualnych zagrożeń cyberbezpieczeństwa zarówno w Polsce, jak i Europie oraz dyskusji o nadchodzących wyzwaniach związanych m.in. ze zmianami regulacyjnymi wynikającymi z wdrażania europejskich przepisów, takich jak NIS2 czy DORA. Podczas spotkań omówiono także możliwe obszary wspólnych działań oraz inicjatyw w ramach Programu PWCyber.

SPECJALISTYCZNE WARSZTATY Z ZAKRESU CYBER THREAT INTELLIGENCE

20 marca 2025 r. w siedzibie Ministerstwa Cyfryzacji odbyły się **specjalistyczne warsztaty z zakresu Cyber Threat Intelligence**, zorganizowane przez Google Cloud Poland sp. z o.o. – partnera Programu Współpracy w Cyberbezpieczeństwie (PWCyber).

W warsztatach uczestniczyli przedstawiciele kilkunastu instytucji tworzących KSC w tym m.in.: pracownicy CSIRT KNF (Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego polskiego sektora finansowego), CSIRT GOV (Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego poziomu krajowego mieszczącego się w Agencji Bezpieczeństwa Wewnetrznego), Ministerstwa Infrastruktury, Centralnego Biura Zwalczania Cyberprzestępczości, Centralnego Ośrodka Informatyki, a także Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji.

Warsztaty CTI są kolejnym krokiem we wzmacnianiu współpracy w ramach PWCyber w zakresie zwiększania kompetencji specjalistów IT sektora publicznego w obszarze cyberbezpieczństwa.

Ilustracja 3 Warsztaty PWCyber

VII FORUM CYBERBEZPIECZEŃSTWA

W dniach 2-4 września 2025 r. podczas VII Forum Cyberbezpieczeństwa w ramach XXXIV Forum Ekonomicznego w Karpaczu nie zabrakło głosu przedstawicieli partnerów Programu PWCyber.

Dzięki ich zaangażowaniu, Forum stało się przestrzenią otwartej wymiany doświadczeń i inspiracji.

Jednym z wydarzeń, które współtworzyli partnerzy PWCyber, była „Flop Night – Noc porażek", podczas której eksperci otwarcie dzielili się historiami nieudanych projektów, które stały się trampoliną do dalszych sukcesów.

Zorganizowano także spotkanie z młodymi uczestnikami Forum, którzy mieli okazję poznać ścieżki kariery w branży technologicznej i porozmawiać z ekspertami. Gościem specjalnym sesji Młodzi@Forum był Krzysztof Gawkowski, wicepremier oraz minister cyfryzacji, zaś branżę reprezentowali m.in. partnerzy PWCyber: Xopero Software S.A, Samsung, Kyndryl.

Dzięki partnerom PWCyber Forum nabrało praktycznego i edukacyjnego wymiaru – rozmowy o cyfrowej przyszłości miały solidne oparcie w realiach biznesu i codziennych wyzwaniach społeczeństwa.

Ilustracja 4 VII FORUM CYBERBEZPIECZEŃSTWA

Głównym wydarzeniem podsumowującym współpracę w 2025 roku było **II Doroczne spotkanie z partnerami zorganizowane w dniu 2 grudnia 2025 r. w Warszawie.** W spotkaniu uczestniczyło blisko 100 przedstawicieli sektora publicznego i prywatnego, aby wspólnie omawiać priorytety, wyzwania legislacyjne i kierunki rozwoju kompetencji w cyberbezpieczeństwie.

Ilustracja 5 Spotkanie z partnerami PWCyber

W 2025 r. dzięki współpracy z ekspertami partnerów technologicznych PWCyber odbyły się 33 szkolenia online w których uczestniczyło ponad 43,5 tys. osób.

PROJEKTY W RAMACH DZIAŁANIA 2.2. PROGRAMU FUNDUSZE EUROPEJSKIE NA ROZWÓJ CYFROWY 2021-2027 (FERC)

Projekt „Cyberbezpieczny Samorząd” – w roku 2025 Ministerstwo Cyfryzacji, we współpracy z Centrum Projektów Polska Cyfrowa oraz NASK – Państwowym Instytutem Badawczym, realizowało dalsze etapy wdrażania największego przedsięwzięcia grantowego w ramach programu FERC, ukierunkowanego na systemowe podniesienie poziomu bezpieczeństwa informacji w jednostkach samorządu terytorialnego. Działania podejmowane w ramach projektu koncentrowały się na wzmacnianiu odporności organizacyjnej i technicznej JST, a także na zwiększeniu ich zdolności do zapobiegania, wykrywania oraz skutecznego reagowania na incydenty naruszające bezpieczeństwo systemów informacyjnych. Odbiorcami wsparcia były wszystkie jednostki samorządu terytorialnego w Polsce, tj. łącznie 2807 JST (100%), wraz z jednostkami organizacyjnymi im podległymi.

Do końca 2025 roku samorządy otrzymały 1,3 mld zł. Gminy, powiaty jak i samorządy województw wydatkują środki na trzy kluczowe obszary wsparcia:

- organizacyjny – związany z procedurami obowiązującymi w obszarze cyberbezpieczeństwa (w szczególności wdrożenie i audyt Systemu Zarządzania Bezpieczeństwem Informacji);
- kompetencyjny – obejmujący szkolenia pracowników JST, w tym zarówno zaawansowanych szkoleń dla personelu informatycznego jak i szkoleń podstawowych związanych z budowaniem świadomości cyberzagrożeń i umiejętności reagowania na nie;
- techniczny – w ramach którego możliwy jest szeroki wachlarz działań: począwszy od zakupu sprzętu informatycznego, poprzez licencje, oprogramowanie oraz usługi wspierające cyberbezpieczeństwo.

Zgodnie z zapisami regulaminu konkursu środki pozyskane z grantów samorządy będą mogły wykorzystać maksymalnie do połowy 2026 r.

Więcej informacji pod adresem: https://www.gov.pl/web/cyfryzacja/15-mld-zl-dla-samorzadow-na-cyberbezpieczenstwo

CENTRUM CYBERBEZPIECZEŃSTWA NASK (CCN)

Celem strategicznym projektu CCN jest wzmocnienie KSC poprzez utworzenie Centrum Cyberbezpieczeństwa, na które złożą się jakościowo nowe tematyczne specjalistyczne centra, ośrodki i laboratoria istotne z punktu widzenia wzmocnienia KSC. Na projekt ten składają się 3 następujące powiązane ze sobą podzadania:

1. Utworzenie obiektu CCN;

2. Utworzenie 7 specjalistycznych centrów, ośrodków i laboratoriów, tj.:

- Krajowego Centrum Odzyskiwania Danych;
- Krajowego Centrum Operacyjnego Cyberbezpieczeństwa;
- Modelowego Ośrodka Treningowo-Szkoleniowego w obszarze Cyberbezpieczeństwa;
- Laboratorium Bezpieczeństwa AI;
- Laboratorium Fuzzingu i Badania Złośliwego Oprogramowania;
- Krajowego Centrum Wsparcia Security dla JST;
- Ośrodka Modelowania Certyfikacji Cyberbezpieczeństwa;

3. Rozbudowa infrastruktury NASK PIB działającej na rzecz CSIRT NASK.

Jest to inwestycja o łącznej wysokości 310 mln zł, w zdolność i gotowość państwa do reagowania na obecne i przyszłe zagrożenia z cyberprzestrzeni.

W 2025 roku kontynuowane były prace projektowe w poszczególnych zespołach dedykowanych związanych z utworzeniem ww. laboratoriów i ośrodków. Realizowane były prace ukierunkowane na złożenie wniosku o wydanie pozwolenia na budowę obiektu. W 2026 roku planowana jest realizacja następnych etapów prac ukierunkowanych na powstanie budynku Centrum.

Więcej informacji pod adresem: *https://www.gov.pl/web/cyfryzacja/przelom-w-projekcie-centrum-cyberbezpieczenstwa-nask*

PROJEKTY REALIZOWANE W RAMACH KPO

Istotny element wzmacniania KSC stanowią przedsięwzięcia realizowane w ramach Krajowego Planu Odbudowy i Zwiększania Odporności, w szczególności działania ujęte w Inwestycji C3.1.1 „CyberPL", których celem jest podniesienie poziomu odporności oraz bezpieczeństwa cyfrowego państwa. W 2025 roku prowadzone były intensywne prace w zakresie realizacji czterech przedsięwzięć o łącznej wartości 1,030 mld zł. Były to:

- Ustanowienie sieci 4 sektorowych zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) – Celem tego przedsięwzięcia jest utworzenie lub rozwój 4 sektorowych CSIRT w sektorach kluczowych w rozumieniu UKSC. W dniu 30.04.2025 r. zakończył się nabór wniosków, w którym podpisano 4 umowy o objęcie wsparciem; Sektorowe zespoły cyberbezpieczeństwa, o których mowa w art. 44 ust. 1 ustawy z dnia 5 lipca 2018 r. o UKSC (Dz. U. z 2024 r. poz. 1077,1222), będą budowane lub rozwijane dla sektorów: transportu, ochrony zdrowia, bankowości i infrastruktury rynków finansowych, infrastruktury cyfrowej, oraz zaopatrzenia w wodę pitną i jej dystrybucji.
  Więcej informacji pod adresem: https://www.gov.pl/web/cyfryzacja/prawie-66-mln-zl-na-rozwoj-csirt-ow-sektorowych
- Utworzenie sieci specjalistów w dziedzinie cyberbezpieczeństwa na szczeblu wojewódzkim, aby wesprzeć organy publiczne w radzeniu sobie z incydentami i odzyskiwaniu danych oraz podejmowanie działań służących podnoszeniu świadomości w zakresie cyberbezpieczeństwa – Celem tego przedsięwzięcia jest modernizacja i profesjonalizacji zespołów Policji, które będą wspierać zaatakowane podmioty KSC w obsłudze incydentów i odzyskiwaniu danych. W dniu

30.05.2025 r. zakończył się nabór wniosków oraz podpisano umowę o objecie przedsięwzięcia wsparciem; Zadanie realizowane będzie do 30.06.2026 roku.
Więcej informacji pod adresem: https://www.gov.pl/web/cyfryzacja/policja-i-nask-z-nowym-systemem-do-walki-z-cyberatakami--rusza-projekt-cropt

- Podłączenie 385 podmiotów KSC do zintegrowanego systemu zarządzania cyberbezpieczeństwem – W dniu 3.09.2024 r. podpisana została umowa pomiędzy Centrum Projektów Polska Cyfrowa i NASK-PIB na jego dofinansowanie. Aktualnie postępuje proces realizacji projektu oraz wzrasta liczba podłączeń. Do końca 2025 r. zrealizowano już ponad 70% założonego celu; Projekt będzie wdrażany do 30.06.2026 roku.
Więcej informacji pod adresem: https://www.gov.pl/web/cppc/zawarlismy-umowe-z-nask-o-objecie-przedsiewziecia-wsparciem

Udzielenie 500 podmiotom wsparcia na rzecz modernizacji i rozbudowania infrastruktur cyberbezpieczeństwa przy wykorzystaniu technologii informacyjnej i technologii operacyjnej – przedsięwzięcie to zostało podzielone na 2 nabory, tj.:

- I nabór pn. „Cyberbezpieczny Rząd" – celem tego naboru jest udzielenie wsparcia grantowego centralnym i naczelnym organom administracji rządowej oraz wojewodom w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa w sieciach IT. Nabór w konkursie grantowym zakończył się 31.03.2025 r. Podpisano umowy z 48 grantobiorcami. Wypłacono wszystkie granty o wartości 258 mln zł;
Więcej informacji pod adresem: https://www.gov.pl/web/cyfryzacja/cyberbezpieczny-rzad--wszystkie-umowy-juz-podpisane

- II nabór pn. „Cyberbezpieczne wodociągi" – celem tego naboru jest udzielenie wsparcia grantowego dla przedsiębiorstw wodociągowo-kanalizacyjnych, wykorzystujących technologie informacyjne (IT) oraz operacyjne (OT) stosowane w przemysłowych systemach sterowania (ICS) w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa w sieciach IT. Nabór wniosków w tym konkursie zakończył się w dniu 2.10.2025 r. W jego wyniku zostało złożonych 896 wniosków o dofinansowanie.
Więcej informacji pod adresem: https://www.gov.pl/web/cyfryzacja/cyberbezpieczne-wodociagi--blisko-900-wnioskow-o-dofinansowanie

FUNDUSZ CYBERBEZPIECZEŃSTWA – ŚWIADCZENIE TELEINFORMATYCZNE

Fundusz Cyberbezpieczeństwa, którego dysponentem jest minister właściwy do spraw informatyzacji, został powołany ustawą z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa. Głównym zadaniem Funduszu, jako państwowego funduszu celowego, jest wsparcie działań zmierzających do zapewnienia bezpieczeństwa systemów teleinformatycznych przed cyberzagrożeniami poprzez finansowanie świadczenia teleinformatycznego, tj. dodatku do wynagrodzenia za pracę, a w przypadku funkcjonariuszy i żołnierzy zawodowych świadczenia pieniężnego.

Świadczenie teleinformatyczne może zostać przyznane osobom realizującym zadania z zakresu cyberbezpieczeństwa na rzecz podmiotów wymienionych w ustawie, m.in. w CSIRT poziomu krajowego, służbach odpowiedzialnych za bezpieczeństwo państwa oraz bezpieczeństwo powszechne, a także w niektórych urzędach administracji publicznej.

Warunkiem ubiegania się o wsparcie ze środków Funduszu jest złożenie przez uprawniony podmiot wniosku do ministra właściwego do spraw informatyzacji. Wnioski spełniające wymagania formalne

przekazywane są do Kolegium do Spraw Cyberbezpieczeństwa, które wydaje opinię w zakresie wnioskowanych kwot.

W 2025 r. Minister Cyfryzacji zawarł 152 umowy o udzielenie wsparcia ze środków Funduszu Cyberbezpieczeństwa na łączną kwotę 377 326 260,50 zł. Świadczenie teleinformatyczne otrzymało blisko 7 000 osób realizujących zadania w zakresie zapewnienia cyberbezpieczeństwa w kluczowych instytucjach w kraju.

Więcej informacji pod adresem: https://www.gov.pl/web/baza-wiedzy/przypominamy-zasady-ubiegania-sie-o-srodki-z-funduszu-cyberbezpieczenstwa

ZWIĘKSZENIE POTENCJAŁU NARODOWEGO W ZAKRESIE TECHNOLOGII CYBERBEZPIECZEŃSTWA

KONKURS GRANTOWY DLA MAŁYCH I ŚREDNICH PRZEDSIĘBIORCÓW Z SEKTORA CYBERBEZPIECZEŃSTWA W RAMACH PROGRAMU WSPARCIA FINANSOWEGO STRON TRZECICH.

Cel konkursu to wzmocnienie pozycji przedsiębiorców z branży cyberbezpieczeństwa na rynku krajowym i międzynarodowym dzięki oferowanym innowacyjnym rozwiązaniom oraz promocji ich produktów i usług.

Nabór został otwarty w sierpniu 2025 r. i rozstrzygnięty w styczniu 2026 r. Eksperci ocenili 150 wniosków, z czego 32 zostało wybranych do dofinansowania. Autorzy tych projektów łącznie otrzymają wsparcie w wysokości ponad 1,7 mln EUR. Dofinansowanie zostanie przeznaczone na:

- rozwój istniejących produktów lub usług – 18 projektów (56%)
- utworzenie nowych produktów lub usług – 11 projektów (34%)
- zwiększenie rozpoznawalności oferty – 3 projekty (10%).

Nabór jest realizowany w ramach projektu „National Coordination Centre – Poland”.

BADANIE RYNKU MŚP BRANŻY CYBERBEZPIECZEŃSTWA.

W 2025 r. Krajowe Centrum Kompetencji Cyberbezpieczeństwa zleciło badanie dotyczące małych i średnich przedsiębiorców sektora cyberbezpieczeństwa, w którym wzięło udział 200 podmiotów. Badanie zostało zrealizowane w ramach projektu „National Coordination Centre – Poland”. Było to pierwsze kompleksowe badanie rynku MŚP branży cyberbezpieczeństwa w Polsce.

Celem kwerendy była diagnoza sektora MŚP i okoliczności mających wpływ na jego rozwój – jego liczebności, specjalizacji i charakterystyki organizacyjnej, a także napotykanych barier rozwojowych, potrzeb i oczekiwań w stosunku do administracji publicznej.

Podsumowanie przebiegu i wniosków z badania znalazło się w Raporcie „Mapa MŚP sektora cyberbezpieczeństwa w Polsce: diagnoza, potrzeby, rekomendacje”. Materiał uwzględnia perspektywę przedsiębiorców, mierzących się na co dzień z wyzwaniami rynku, ograniczeniami regulacyjnymi, barierami wejścia na rynki zagraniczne oraz lukami kadrowymi. Zawiera także rekomendacje współtworzone przez samych przedsiębiorców i ekspertów cyberbezpieczeństwa – wskazówki dla administracji rządowej i decydentów co do tego jak usunąć bariery rozwojowe, z jakimi boryka się krajowy przemysł cyberbezpieczeństwa.

Raport z badania dostępny jest na stronie internetowej Krajowego Centrum Kompetencji Cyberbezpieczeństwa.

STANDARDY I REKOMENDACJE CYBERBEZPIECZEŃSTWA

W 2025 r. Ministerstwo Cyfryzacji opracowało i zamieściło w bazie wiedzy o cyberbezpieczeństwie na portalu gov.pl (*Rekomendacje cyberbezpieczeństwa - Baza wiedzy - Portal Gov.pl*) kolejnych 5 publikacji rekomendujących dobre praktyki i zalecenia konfiguracyjne podnoszące poziom cyberbezpieczeństwa w ramach skutecznego zarządzania ryzykiem, osiągania bezpieczeństwa w systemach informacyjnych oraz przetwarzania w chmurze.

Ponadto wspólnie z Partnerami Programu Współpracy w Cyberbezpieczeństwie (PWCyber) opracowanych i zamieszczonych w *Poradniki PWCyber - Baza wiedzy - Portal Gov.pl* osiem publikacji zalecających stosowanie w życiu codziennym uwierzytelniania wieloskładnikowego (*ang. Multi-factor Authentication - MFA*). Dotychczas opublikowano 57 publikacje w zakresie wymagań organizacyjno-technicznych rekomendujących rozwiązania bezpieczeństwa informacji.

PROJEKT PIONIER-Q W RAMACH EUROPEAN QUANTUM COMMUNICATION INFRASTRUCTURE

Projekt PIONIER-Q jest oficjalnym wkładem Polski do europejskiej inicjatywy - European Quantum Communication Infrastructure (EuroQCI10) uruchomionej w 2019 roku. EuroQCI będzie bezpieczną infrastrukturą łączności kwantowej obejmującą całą UE. Komisja Europejska współpracuje ze wszystkimi 27 państwami członkowskimi UE oraz Europejską Agencją Kosmiczną (ESA) w celu zaprojektowania, opracowania i wdrożenia EuroQCI, który będzie składał się z segmentu naziemnego opartego na sieciach łączności światłowodowej, łączących strategiczne obiekty na poziomie krajowym i transgranicznym oraz segmentu kosmicznego opartego na satelitach. Będzie ona integralną częścią IRIS²11, nowego unijnego systemu bezpiecznej komunikacji opartej na przestrzeni kosmicznej. EuroQCI będzie chronić wrażliwe dane i infrastrukturę krytyczną poprzez integrację systemów kwantowych z istniejącą infrastrukturą komunikacyjną, zapewniając dodatkową warstwę bezpieczeństwa opartą na fizyce kwantowej. Wzmocni ochronę europejskich instytucji rządowych, ich centrów danych, szpitali, sieci energetycznych i innych. Realizacja projektu PIONIER-Q jest kluczowym elementem dla efektywnego udziału Polski w tej inicjatywie.

W ramach Projektu zostanie uruchomiona infrastruktura oraz usługi związane z generowaniem oraz przesyłaniem kluczy w technologii kwantowej dystrybucji kluczy (QKD – Quantum Key Distribution). Jest to metoda bezpiecznego generowania oraz dystrybucji kluczy oparta na zasadach mechaniki kwantowej, które następnie mogą zostać wykorzystane np. do szyfrowania danych lub uwierzytelniania usług i użytkowników. Technologia QKD może zostać wykorzystana w aktualnych algorytmach do symetrycznego szyfrowania danych lub do przyszłych rozwiązań algorytmów szyfrowania danych typu post quantum, będących aktualnie przedmiotem standaryzacji. Sieci komunikacji kwantowej są potencjalnym elementem do łączenia oraz skalowania infrastruktur obliczeń kwantowych. Długofalowym celem projektu jest wypracowanie rozwiązań oraz zbudowanie fundamentów pod sieci bezpiecznej komunikacji między innymi dla jednostek administracji lokalnej, centralnej oraz na poziomie transgranicznym (pomiędzy państwami członkowskimi i instytucjami UE). Dotyczy to zarówno komunikacji w segmencie naziemnym, jak i satelitarnym.

W grudniu 2023 r. Prezes Rady Ministrów powierzył Konsorcjum PIONIER-Q realizację zadania z zakresu informatyzacji sektora publicznego oraz innowacji cyfrowych, polegającego na utrzymaniu zdolności zleceniobiorców do realizacji projektu pn. „PIONIER-Q: Ogólnopolska Kwantowa Infrastruktura Komunikacyjna", będącego wkładem Polski do inicjatywy EuroQCI – budowy europejskiej infrastruktury komunikacji kwantowej. Po stronie rządowej działania w tym zakresie realizowane są przez Ministerstwo Cyfryzacji.
W skład Konsorcjum PIONIER-Q wchodzą:

- Poznańskie Centrum Superkomputerowo-Sieciowe
- Akademickie Centrum Komputerowe Cyfronet AGH

- Interdyscyplinarne Centrum Modelowania Matematycznego i Komputerowego
- Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy
- Centrum Informatyczne TASK
- Wrocławskie Centrum Sieciowo-Superkomputerowe

Od 2023 r. MC współfinansuje projekt PIONIER-Q w wysokości 25%.

BUDOWANIE ŚWIADOMOŚCI I KOMPETENCJI SPOŁECZNYCH W ZAKRESIE CYBERBEZPIECZEŃSTWA

ZACHĘCANIE MŁODYCH TALENTÓW DO PODJĘCIA KARIERY W CYBERBEZPIECZEŃSTWIE

Już po raz drugi grupa polskich uczennic wzięła udział w międzynarodowym obozie letnim CyberWizards w Estonii, zorganizowanym przez estoński Krajowy Ośrodek Koordynacji (NCC-EE). Podczas obozu uczestniczki:

- poznawały tajniki cyberbezpieczeństwa,
- uczestniczyły w praktycznych zajęciach i warsztatach
- zyskały inspirację do rozwijania kariery w jednej z najbardziej przyszłościowych branż technologicznych

Inicjatywa miała na celu zachęcenie młodych kobiet do odkrywania swoich talentów w cyberbezpieczeństwie i pokazanie, że ta ścieżka zawodowa jest dla nich pełna możliwości.

SPOTKANIE WICEMINISTRA CYFRYZACJI PAWŁA OLSZEWSKIEGO Z PREZES URZĘDU ZAMÓWIEŃ PUBLICZNYCH AGNIESZKĄ OLSZEWSKĄ

30 kwietnia 2025 r. Zorganizowano **spotkanie wiceministra cyfryzacji Pawła Olszewskiego z prezes Urzędu Zamówień Publicznych Agnieszką Olszewską** to efekt działania Grupy roboczej powstałej w ramach PWCyber. Spotkanie miało na celu omówienie wspólnych działań na rzecz bezpieczniejszych i bardziej efektywnych zamówień publicznych w obszarze technologii. Rozmowy dotyczyły kluczowych zagadnień związanych z włączaniem cyberbezpieczeństwa do procedur zakupowych. Strony spotkania zadeklarowały kontynuację współpracy, w tym udział w grupach roboczych, które będą pracować nad propozycjami zmian w przepisach krajowych i unijnych. Celem jest nie tylko poprawa procedur, lecz także popularyzacja wiedzy eksperckiej i dobrych praktyk w zakresie zamówień publicznych w obszarze nowych technologii i cyberbezpieczeństwa.

Ilustracja 6 spotkanie wiceministra cyfryzacji Pawła Olszewskiego z prezes Urzędu Zamówień Publicznych Agnieszką Olszewską

SZKOLENIA Z CYBERBEZPIECZEŃSTWA DLA NAJWAŻNIEJSZYCH OSÓB W PAŃSTWIE – PROJEKT SECUREV

W 2025 r. Ministerstwo Cyfryzacji kontynuowało prowadzone od 2021 r. działania prewencyjno-edukacyjne dla najważniejszych osób w państwie (projekty SecureV). W ramach działania prowadzone są specjalistyczne szkolenia z zakresu cyberbezpieczeństwa adresowane do najważniejszych osób w państwie. Terminy i zakres merytoryczny szkoleń dostosowywane są do konkretnych potrzeb szkolonej osoby. Dodatkowo, każda indywidualnie przeszkolona osoba zostaje wyposażona w uniwersalne narzędzia służące do silnego uwierzytelnienia wraz z instruktażem stosowania narzędzia. Z uwagi na dynamiczną sytuację w cyberprzestrzeni kraju oraz duże zainteresowanie szkoleniami, kolejne edycje projektu uwzględniają coraz większą grupę odbiorców. Początkowo projekt SecureV obejmował wyłącznie parlamentarzystów i kadrę kierowniczą administracji centralnej.

Od 2023 r. zasięg działań prewencyjno-edukacyjnych objął już terytorium całego kraju, a projektem szkoleniowym objęci są parlamentarzyści, kadra kierownicza administracji centralnej i samorządowej, przedstawiciele Krajowego Biura Wyborczego oraz pracownicy Podstawowej Opieki Zdrowotnej.

W edycji SecureV 2025 udział w szkoleniach wzięło prawie 5 000 osób, a od 2021 r., w ramach działań SecureV przeszkolono niemal 17 000 osób.

Dzięki zdobytemu doświadczeniu z poprzednich lat oraz zbudowaniu zespołu trenerskiego, ww. szkolenia będą realizowane również w 2026 r.

Tabela 46. SZKOLENIA Z CYBERBEZPIECZEŃSTWA DLA NAJWAŻNIEJSZYCH OSÓB W PAŃSTWIE – PROJEKT SECUREV

Rok	2021	2022	2023	2024	2025	ŁĄCZNIE
liczba szkoleń	442	1 006	2 959	3 731`	4 284	12 422
liczba przeszkolonych osób	442	1 048	5 288	4 981	4 970	16 729

PROJEKT USTAWY O OCHRONIE MAŁOLETNICH PRZED DOSTĘPEM DO TREŚCI PORNOGRAFICZNYCH W INTERNECIE (UD179)

W 2025 r. kontynuowano pracę nad projektem ustawy o ochronie małoletnich przed dostępem do treści szkodliwych w internecie. Projekt ustawy skierowano do konsultacji publicznych, które trwały od 24 lutego do 26 marca 2025 r. Z kolei 12 marca 2025 r. w siedzibie Ministerstwa Cyfryzacji odbyło się wysłuchanie publiczne, w którym udział wzięli przedstawiciele wielu środowisk: od organów administracji publicznej i państwowych instytutów badawczych poprzez przedsiębiorców, w tym z branży komunikacji elektronicznej, a także środowisk prawniczych, izb i związków gospodarczych, placówek oświatowych i naukowych aż po organizacje pozarządowe

Więcej informacji pod adresem: https://www.gov.pl/web/cyfryzacja/wysluchanie-publicznie-w-sprawie-rzadowego-projektu-ustawy-o-ochronie-dzieci-przed-dostepem-do-tresci-szkodliwych-w-internecie.

Obecnie projekt dotyczyć będzie wyłącznie treści pornograficznych dostępnych w usługach świadczonych drogą elektroniczną, co znalazło swoje odzwierciedlenie w zmianie tytułu projektu. Jak wynikało z wielu uwag zgłoszonych w toku konsultacji publicznych, zagadnienie dostępu do treści szkodliwych wymaga pogłębionej analizy. Problematyka dostępu małoletnich do treści szkodliwych jest bardziej złożona z uwagi na szeroki zakres tego rodzaju treści oraz zróżnicowane kanały ich dystrybucji. Przygotowanie przepisów regulujących wspomnianą materię wymaga zatem dodatkowych analiz i konsultacji i powinno być przedmiotem odrębnego procesu legislacyjnego. Natomiast problem zbyt łatwego dostępu do treści pornograficznych osób małoletnich został dobrze zbadany, znana jest jego skala i specyfika, co pozwala na zaprojektowanie adekwatnych rozwiązań legislacyjnych.

Zgodnie z założeniami projektu usługodawca umożliwiający dostęp do treści pornograficznych stosować będzie weryfikację wieku uniemożliwiającą dostęp do tego rodzaju treści przez małoletnich. Projekt ustawy przewiduje wytyczne dotyczące weryfikacji wieku, w tym stosowanie metod umożliwiających jednoznaczne potwierdzenie pełnoletniości wieku (z wyłączeniem metod szacowania wieku oraz tych opartych na biometrii) bez przetwarzania innych danych osobowych, niesłużących ustaleniu wieku. Nazwy domen internetowych umożliwiających małoletnim dostęp do treści pornograficznych bez uprzedniego stosowania mechanizmu weryfikacji wieku będą podlegać wpisowi do rejestru a co za tym idzie blokadzie dostępu przez dostawców usługi dostępu do internetu. O blokadzie decydować będzie Prezes UKE, na co abonentowi nazwy domeny przysługiwać będzie sprzeciw. Nieuwzględniony przez Prezesa UKE sprzeciw może zostać zaskarżony przez ten podmiot do sądu powszechnego.

Projekt został skierowany do ponownych konsultacji publicznych 2 września 2025 r. W 2026 r. planowane są dalsze prace nad projektem. Po zakończeniu analizy uwag otrzymanych w konsultacjach i uzgadniania sposobu ich uwzględnienia planowanie jest przekazanie projektu na Stały Komitet Rady Ministrów w pierwszym kwartale 2026 r.

PROJEKT USTAWY O KRAJOWYM SYSTEMIE PRZETWARZANIA, ANALIZY I KLASYFIKACJI TREŚCI PRZEDSTAWIAJĄCYCH SEKSUALNE WYKORZYSTYWANIE MAŁOLETNICH (UD306)

W 2025 r. Ministerstwo Cyfryzacji rozpoczęło pracę nad projektem ustawy o krajowym systemie przetwarzania, analizy i klasyfikacji treści przedstawiających seksualne wykorzystywanie małoletnich. Powodem, dla którego rozważane są wspomniane regulacje jest brak ogólnokrajowego systemu teleinformatycznego, do którego mogłyby mieć dostęp organy ścigania w celu szybkiej i pewnej identyfikacji materiałów CSAM (Child Sexual Abuse Material). Projekt ustawy przewiduje utworzenie systemu dwóch zintegrowanych, ale zarządzanych niezależnie baz danych - bazy hashy CSAM (zawierającej wyłącznie metadane umożliwiające zidentyfikowanie treści CSAM), oraz bazy zobrazowań CSAM (zawierająca szczegółowe dane dot. CSAM, w tym samą treść, informacje dot. opinii biegłego i wyroków w sprawach związanych z danym CSAM). Zgodnie z założeniami projektu, za obsługę bazy hashy CSAM odpowiedzialny będzie Naukową i Akademicką Siecią Komputerową – Państwowym Instytutem Badawczym (NASK-PIB), natomiast za bazę zobrazowań Komenda Główna Policji.

Utworzenie baz danych ma usprawnić postępowania karne, odciążyć biegłych i umożliwić lepsze zagospodarowanie posiadanych przez właściwe organy zasobów oraz umożliwić współpracę międzynarodową na wyższym poziomie technicznym oraz prawnym. Ponadto stworzenie systemu baz danych CSAM wypełni postanowienia zawarte w Krajowym Planie Przeciwdziałania Przestępstwom Przeciwko Wolności Seksualnej i Obyczajności na Szkodę Małoletnich na lata 2023–2026.

PROJEKT USTAWY O KRAJOWYM SYSTEMIE PRZETWARZANIA, ANALIZY I KLASYFIKACJI TREŚCI PRZEDSTAWIAJĄCYCH SEKSUALNE WYKORZYSTYWANIE MAŁOLETNICH UZYSKAŁ WPIS DO WYKAZU PRAC LEGISLACYJNYCH RADY MINISTRÓW 16 WRZEŚNIA 2025 R. (UD306).

Obecnie projekt ustawy znajduje się w fazie roboczej. Prace nad jego treścią są prowadzone wewnętrznie w Ministerstwie Cyfryzacji, w uzgodnieniu z Prokuraturą Krajową, Ministerstwem Sprawiedliwości, Ministerstwem Spraw Wewnętrznych i Administracji, Komendą Główną Policji oraz NASK-PIB. Na potrzeby wspomnianych uzgodnień powołano do życia nieformalną grupę roboczą, w skład której weszli przedstawiciele wyżej wymienionych instytucji. Pierwsze spotkanie wspomnianej grupy odbyło się 5 listopada 2025 r. w siedzibie Ministerstwa Cyfryzacji. Dalsze zadania związane z przedmiotowym projektem będą kontynuowane w 2026 r.

W 2025 r. Ministerstwo Cyfryzacji nadal było największym dostawcą terminali Starlink zapewniających dostęp do internetu, co miało kluczowe znaczenie dla zapewnienia ciągłości funkcjonowania państwa ukraińskiego i udzielania pomocy humanitarnej oraz zagwarantowania bezpiecznej łączności.

SZKOLENIA ONLINE DLA PODMIOTÓW KSC

W roku 2025 Ministerstwo Cyfryzacji kontynuowało prowadzone od 2020 r. szkolenia online dla podmiotów KSC. Szkolenia prowadzone są przez ekspertów i praktyków na co dzień zajmujących się kwestiami cyberbezpieczeństwa – ekspertów NASK-PIB, partnerów technologicznych PWCyber. Szkolenia realizowane są na różnym poziomie zaawansowania wiedzy z zakresu cyberbezpieczeństwa, dostosowane do bieżącej sytuacji i zgłaszanych potrzeb.

Od 2024 r. część szkoleń realizowana jest z udziałem tłumaczy na Polski Język Migowy (PJM)

W ramach szkoleń online w 2025 r. zorganizowano:

- 8 szkoleń z zakresu higieny cyfrowej (4 cykle) we współpracy z NASK-PIB. Cykl składa się z dwóch szkoleń: Cyberzagrożenia - bądź na bieżąco! oraz Podstawowe zasady cyberhigieny w pracy i w życiu prywatnym. Z uwagi na ogromne zainteresowanie szkoleniami z podstaw cyberbezpieczeństwa, od 2023 roku cykl jest powtarzany regularnie raz na kwartał. W 2025 r. w szkoleniach z podstaw higieny cyfrowe udział wzięło 18 099 osób.
- 24 szkolenia online zrealizowane we współpracy z partnerami PWCyber, w których udział wzięło 42 849 osób.

Celem szkoleń jest nie tylko zwiększenie świadomości kadr KSC na temat cyberzagrożeń, ale również podniesienie umiejętności praktycznych związanych z wykorzystywaniem narzędzi informatycznych oraz radzenia sobie w sytuacjach kryzysowych.

Łącznie, w 2025 r. zrealizowano 32 **szkolenia online**, w których uczestniczyło prawie 43 **tys. osób**.

Tabela 47. SZKOLENIA ONLINE DLA PODMIOTÓW KSC

Rok	2021	2022	2023	2024	2025	ŁĄCZNIE
l. szkoleń	17	22	28	42	32	141
l. przeszkolonych osób	4 834	7 486	16 682	33 639	42 849	105 490

PROJEKTY WSPIERAJĄCE EDUKACJE O CYBERBEZPIECZEŃSTWIE - CYBERLEKCJE

Minister Cyfryzacji realizuje różnego rodzaju inicjatywy wspierające edukacje o bezpieczeństwie online wśród najmłodszych użytkowników sieci. Projekt Cyber lekcje realizowany jest od 2021 roku wspólnie z Państwowym Instytutem Badawczym NASK. Adresowany jest do nauczycieli i pedagogów, chcących podczas swoich zajęć przekazywać dzieciom i młodzieży zasady i wskazówki dotyczące bezpiecznego poruszania się w Internecie. W ramach projektu Cyberlekcje powstało 18 gotowych scenariuszy zajęć lekcyjnych o cyberbezpieczeństwie, które obejmują różne tematy, takie jak bezpieczeństwo online, prywatność, relacje w sieci, zagrożenia online, zarządzanie danymi, nadużywanie nowych technologii i dobrostan psychiczny

W 2024 r. zrealizowano pilotażowo kolejną odsłonę projektu, której celem było m.in. upowszechnienie przygotowanych materiałów w latach poprzednich, poprzez bezpośredni kontakt z pedagogami. Celem pilotażu była również organizacja szkoleń, które wyposażą nauczycieli w wiedzę z obszaru cyberhigieny i socjotechnik wykorzystywanych przez oszustów w cyberprzestrzeni. Prowadzone w ramach pilotażu szkolenia kadry pedagogicznej oraz lekcje pokazowe na bazie scenariuszy Cyberlekcji 3.0, wskazały na **zasadność kontynuacji projektu, a także rozszerzenie jego zakresu o nowe scenariusze oraz**

przeprowadzenie szkoleń we wszystkich pozostałych 15 województwach, dlatego projekt jest rozwijany i kontynuowany. Realizacja projektu w 2025 r. objęła

- **2-dniowe szkolenia dla dyrektorów oraz kadry pedagogicznej szkolnych placówek** podstawowych i ponadpodstawowych. W 2025 r. udział w takich szkoleniach wzięło 543 osoby.
- **Zajęcia bazujące na scenariuszach Cyberlekcji dla uczniów** szkół podstawowych i ponadpodstawowych wraz ze szkoleniem dla **kadry pedagogicznej** placówkach, które zgłoszą potrzebę przeprowadzenia szkoleń w różnych regionach Polski. Przeprowadzono 89 lekcji, w których wzięło udział 2995 uczniów oraz 34 dwugodzinne szkolenia dla nauczycieli, w których udział wzięło 1274 nauczycieli.
- **Przeprowadzenie 22 ogólnodostępnych lekcji online** bazujących na scenariuszach Cyberlekcji dla uczniów szkół podstawowych i ponadpodstawowych. Łącznie w lekcjach - uczestniczyło 4033 klas i 66 798 uczniów
- **Opracowanie 7 nowych scenariuszy Cyberlekcji** (nowe tematy to m.in. Poszanowanie praw autorskich, Treści szkodliwe - seksting, Dezinformacja).

Projekt będzie kontynuowany w 2026 r.

SZKOLENIA STACJONARNE DLA SPECJALISTÓW SEKTOROWYCH ZESPOŁÓW CSIR REALIZOWANE NA PODSTAWIE POROZUMIENIA MC-MON

Zawarte zostało Porozumieniu o współpracy pomiędzy Ministerstwem Cyfryzacji a Ministerstwem Obrony Narodowej – Eksperckim Centrum Szkolenia Cyberbezpieczeństwa (ECSC), w ramach którego wspólnie realizowane były przedsięwzięcia mające na celu rozwijanie specjalistycznych kompetencji z obszaru cyberbezpieczeństwa wśród kadr odpowiedzialnych za cyberbezpieczeństwo w podmiotach publicznych.

Pierwszym z ww. działań było uruchomienie pilotażowego projektu szkoleniowego adresowanego do specjalistów sektorowych zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT sektorowe). Program szkoleń obejmował zarówno część teoretyczną, jak i praktyczną. Zajęcia prowadzone były przez instruktorów ECSC, którzy dysponują doświadczeniem w realizacji specjalistycznych kursów z zakresu bezpieczeństwa informacji oraz ochrony systemów teleinformatycznych.

Od września 2025 r. do końca 2025 r. przeprowadzone zostały w Wałczu, w siedzibie ECSC, dwa szkolenia:

- Działania adwersarzy z wykorzystaniem sieci IP.
- Badania i ocena bezpieczeństwa rozwiązań ICT.

Szkolenia to stanowią przykład efektywnej współpracy między Ministerstwem Obrony Narodowej a Ministerstwem Cyfryzacji, opartej na wymianie wiedzy i doświadczeń w dziedzinie cyberbezpieczeństwa.

BAZA WIEDZY O CYBERBEZPIECZEŃSTWIE NA PORTALU GOV.PL

W trybie ciągłym rozwijana jest baza wiedzy o cyberbezpieczeństwie na portalu gov.pl. W 2025 r. w bazie wiedzy opublikowano ponad 130 nowych publikacji (artykuły, rekomendacje dotyczące problematyki bezpieczeństwa w cyberprzestrzeni a także komunikaty i ostrzeżenia CSIRT NASK).

ĆWICZENIA KSC – KSC-EXE 2025

Ilustracja 7 KSC-EXE-2025

W dniu 26 listopada 2025 r. odbyły się ćwiczenia KSC- KSC-EXE 2025.

W ćwiczeniach wzięło udział ponad 100 przedstawicieli instytucji odpowiedzialnych za cyberbezpieczeństwo w Polsce. Wśród nich znalazły się:

- **organy właściwe:** Ministerstwo Energii, Ministerstwo Infrastruktury, Ministerstwo Zdrowia, Ministerstwo Obrony Narodowej, Komisja Nadzoru Finansowego, Ministerstwo Cyfryzacji;
- **CSIRT:** CSIRT GOV, CSIRT MON, CSIRT NASK;
- **zespoły sektorowe:** CSIRT KNF, CSIRT Centrum e-Zdrowia;
- **inne instytucje KSC:** Ministerstwo Spraw Zagranicznych, Prokuratura Krajowa, Rządowe Centrum Bezpieczeństwa, Urząd Komunikacji Elektronicznej, Centralne Biuro Zwalczania Cyberprzestępczości.

KSC-EXE 2025 umożliwiły kompleksową analizę aktualnych procedur reagowania na incydenty i współdziałania między podmiotami systemu. Scenariusze obejmowały różnorodne zagrożenia, od zakłóceń infrastruktury krytycznej po złożone kampanie cyberataków.

Tegoroczne ćwiczenia odbyły się w kluczowym momencie – w przededniu nowelizacji UKSC która wprowadzi do polskiego prawa wymogi **dyrektywy NIS 2**. KSC-EXE 2025 pełnią rolę praktycznego przygotowania administracji i instytucji do nadchodzących zmian, wzmacniając zdolności operacyjne całego KSC.

.

BUDOWANIE SILNEJ POZYCJI MIĘDZYNARODOWEJ RP W OBSZARZE CYBERBEZPIECZEŃSTWA

WSPÓŁPRACA W RAMACH UNII EUROPEJSKIEJ – PODSUMOWANIE PREZYDENCJI POLSKI W RADZIE UE

Cyberbezpieczeństwo stanowiło jeden z kluczowych priorytetów polskiej prezydencji w Radzie UE, a Ministerstwo Cyfryzacji odgrywało kluczową rolę w koordynacji prac w tym obszarze. Działania MC koncentrowały się na wzmocnieniu odporności UE na incydenty cybernetyczne, pogłębieniu współpracy międzynarodowej oraz wypracowaniu wspólnych mechanizmów reagowania kryzysowego.

Najważniejszym osiągnięciem prezydencji było uzgodnienie i przyjęcie przez Radę UE zrewidowanego EU Cyber Blueprint, tj. wspólnych ram reagowania UE na incydenty cybernetyczne dużej skali. Dokument, przyjęty jednogłośnie, wprowadził bardziej operacyjny model współpracy na poziomie technicznym, operacyjnym i politycznym, w tym m.in. zróżnicowane tryby reagowania kryzysowego, wzmocnioną rolę komunikacji kryzysowej oraz zalecenie opracowania wspólnej taksonomii incydentów przez sieć EU-CyCLONe. Prace nad Blueprintem były intensywnie prowadzone w ramach Horyzontalnej Grupy Roboczej ds. Cyberprzestrzeni (HWPCI), której posiedzeniom przewodniczyła strona polska.

Równolegle, z inicjatywy polskiej prezydencji, przygotowano Apel Warszawski w sprawie wyzwań związanych z cyberbezpieczeństwem, który stanowił polityczny impuls do rewizji Cyber Blueprintu. Dokument odnosił się m.in. do incydentów dużej skali, synergii cyberbezpieczeństwa cywilnego i wojskowego, inwestycji w cyberbezpieczeństwo w UE, cyberdyplomacji, niedoboru kadr oraz ochrony infrastruktury krytycznej.

W obszarze współpracy politycznej i eksperckiej Ministerstwo Cyfryzacji zorganizowało lub współorganizowało szereg wydarzeń wysokiego szczebla poświęconych cyberbezpieczeństwu, w tym:

- nieformalne posiedzenie ministrów UE ds. cyfrowych w Warszawie, w całości poświęcone cyberbezpieczeństwu, reagowaniu na incydenty dużej skali, inwestycjom w cyber oraz synergii cywilno-wojskowej,
- Cyber Certification Week w Warszawie, organizowany w Warszawie, organizowany we współpracy z ENISA, obejmujący spotkania ECCG, podgrup certyfikacyjnych oraz doroczną konferencję ENISA nt. certyfikacji cyberbezpieczeństwa,
- Cyber Week w Krakowie, obejmujący spotkania sieci CSIRT, EU-CyCLONe oraz Grupy Współpracy NIS, poświęcone reagowaniu na incydenty i kryzysy cybernetyczne,
- Baltic Digital Security Forum w ramach Digital Summit w Gdańsku – zamknięte spotkanie wysokiego szczebla poświęcone bezpieczeństwu cyfrowemu w regionie.

Ministerstwo Cyfryzacji przewodniczyło również intensywnym pracom w ramach unijnych grup roboczych, w szczególności HWPCI oraz WP TELECOM, prowadząc dyskusje m.in. na temat horyzontalnego charakteru dyrektywy NIS2, pojedynczego punktu zgłoszeń incydentów oraz roli ENISA w systemie zarządzania cyberbezpieczeństwem UE.

Działania realizowane w trakcie prezydencji wzmocniły pozycję Polski jako jednego z liderów debaty europejskiej w obszarze cyberbezpieczeństwa oraz przyczyniły się do zwiększenia spójności i gotowości UE do reagowania na poważne zagrożenia w cyberprzestrzeni, stanowiąc istotny wkład w rozwój międzynarodowej współpracy cyfrowej.

Ponadto, jako prezydencja w zakresie cyberbezpieczeństwa Polska przeprowadziła serię debat eksperckich na temat rozmaitych, zarówno globalnych jak i europejskich aspektów cyberbezpieczeństwa. Debaty dotyczył m.ni. cyberdyplomacji, standaryzacji, sztucznej inteligencji oraz umiejętności w zakresie cyberbezpieczeństwa jak również współpracy UE z państwami trzecimi. Przyjęły one różne formy, w tym konferencji i warsztatów.

Listę spotkań obejmowały, m.in.:

- Cyber tydzień: spotkanie Sieci CyCLONe, Sieci CSIRT i Grupy Współpracy NIS (20-24 stycznia, Bruksela);
- Tydzień certyfikacji cyberbezpieczeństwa (10-14 marca, Warszawa);
- Konferencja SECURE International Summit (3-4 kwietnia, Bydgoszcz);
- Wspólne posiedzenie Rady Zarządzającej ENISA i Rady Zarządzającej ECCC oraz spotkanie Rady Zarządzającej ENISA (7-8 kwietnia, Warszawa);
- Cyber tydzień: spotkanie Sieci CyCLONe, Sieci CSIRT i Grupy Współpracy NIS (12-16 maja, Kraków).

Ministerstwo Cyfryzacji, w ramach współpracy ze Stałym Przedstawicielstwem RP przy UE w Brukseli zrealizowało następujące priorytety z obszaru cyberbezpieczeństwa:

- Rada Unii przyjęła Apel Warszawski w sprawie wyzwań związanych z cyberbezpieczeństwem, który dał impuls do wypracowania Cyber Blueprint. Apel stanowi nieformalne podejście państw UE do kluczowych kwestii w obszarze cyberbezpieczeństwa;
- Rada Unii w dniu 6 czerwca 2025 r. przyjęła Cybersecurity Blueprint;
- Prezydencja polska przygotowała liczne raporty podsumowujące dyskusje w Radzie (m.in. dotyczące współdziałania w obszarze cyberbezpieczeństwa w sektorze ochrony zdrowia czy też wspólnego punktu raportowania incydentów).

Cybersecurity BluePrint to nowy model reagowania na incydenty cyfrowe dużej skali został przyjęty dzięki polskiej prezydencji. Po 8 latach od ostatniej aktualizacji UE zyskała narzędzie lepiej dostosowane do dzisiejszych realiów i zagrożeń.

Unijny plan zarządzania cyberkryzysami (Cybersecurity Blueprint) wskazuje jak Unia powinna reagować w przypadku cyberincydentów na dużą skalę lub cyberkryzysów. Plan wskazuje jak państwa powinny na nie reagować i przywracać sprawność operacyjną, a także jak wyciągać z nich wnioski na przyszłość.

Plan zrealizował priorytet polskiej prezydencji o Europie bezpieczniejszej, bardziej odpornej i lepiej przygotowanej na kryzysy.

Obecnie działamy na rzecz wdrożenia Planu poprzez udział w ćwiczeniach oraz przygotowywanie dokumentów implementujących (np. taksonomii incydentów).

Jednocześnie, w ramach współpracy unijnej Ministerstwo Cyfryzacji realizowało zadania związane z koordynacją współpracy między organami właściwymi ds. cyberbezpieczeństwa RP z odpowiednimi organami w innych państwa członkowskich UE. Dotyczy to udziału w grupie współpracy NIS oraz w pracach następujących zespołów: WS5 - dostawcy usług cyfrowych, WS3 - raportowanie incydentów, WS7 – WS2 – środki bezpieczeństwa, WS5 - dostawcy usług cyfrowych, WS8 - sektor energii, WS10 - infrastruktura cyfrowa, WS12 - sektor zdrowia, WS on 5G and Telecom Security, WS on Supply Chain Security, 5G Toolbox, Sub-group standaryzacja i certyfikacja, europejska sieć zarządzania kryzysami cyfrowymi CyCLONE, Europejska Sieć Bezpieczeństwa Wyborów (ECNE), Horyzontalna Grupa Robocza ds. Cyberprzestrzeni.

WSPARCIE DLA UKRAINY I WSPÓŁPRACA Z UKRAINĄ - CYBERBEZPIECZEŃSTWO – POROZUMIENIE PL–UA I DZIAŁANIA MC 2025

W sierpniu 2022 r. Polska i Ukraina podpisały Porozumienie w sprawie cyberbezpieczeństwa, które stanowi podstawę formalną dwustronnej współpracy.

Ministerstwo Cyfryzacji realizowało to porozumienie w toku 2025 r. poprzez: współpracę zespołów reagowania na incydenty bezpieczeństwa komputerowego (Computer Security Incident Response Teams – CSIRT), wymianę informacji o zagrożeniach, działania eksperckie i analityczne.

Ministerstwo Cyfryzacji uczestniczy w koordynacji KSC i wdrażaniu rozwiązań unijnych do porządku prawnego Polski – współpracujemy w tym zakresie ze stroną ukraińską.

W 2025 r. Polska i Ukraina mierzyły się z podobnymi zagrożeniami hybrydowymi ze strony Federacji Rosyjskiej, w tym: atakami malware i ransomware, operacjami hybrydowymi.

Wzmocnienie operacyjnej współpracy w obszarze cyberbezpieczeństwa pomiędzy Polską a Ukrainą wymaga pogłębienia współpracy pomiędzy zespołami CSIRT oraz usprawnienia koordynacji działań w zakresie reagowania na zagrożenia cybernetyczne na poziomie UE.

W ramach działań bilateralnych odbyły się w 2025 r. m.in.: rozmowa Wicepremiera - Ministra Cyfryzacji z wicepremierem Ukrainy Mychajło Fedorowem, w trakcie której omawiano wsparcie cyfrowe, współpracę w zakresie łączności oraz cyberbezpieczeństwa w kontekście polsko-ukraińskim oraz kwestie związane z cyberzagrożeniami i wsparciem infrastruktury cyfrowej Ukrainy. Ponadto odbyła się rozmowa Wicepremiera-Ministra Cyfryzacji z wicepremierem Ukrainy Ołeksijem Czernyszowem, podczas której poruszano m.in. kwestie integracji Ukrainy z UE, cyberbezpieczeństwa i łączności satelitarnej.

MECHANIZM TALLIŃSKI

Mechanizm Talliński został sformalizowany w 2023 r. przez ministerstwa spraw zagranicznych CAN, CZ, DK, EE, FR, DE, IT, NO, NL, PL, SE, UK i USA. Mechanizm koordynuje wsparcie 13 państw, w tym Polski, dla ukraińskiej infrastruktury cyfrowej oraz zdolności reagowania na cyberataki.

Obecnie inicjatywa Mechanizmu Tallińskiego przechodzi reorganizację, która pozwoli na sprawniejsze współdziałanie z sektorem prywatnym państw członkowskich. Jednocześnie planowana jest współpraca z Bankiem Światowym celem pozyskania źródeł finansowania dla projektów realizowanych w ramach inicjatywy.

W 2025 r. Mechanizm Talliński osiągnął kolejny etap rozwoju organizacyjnego, w tym uruchomienie „Tallinn Mechanism Project Office (TMPO)" w Kijowie, które ma na celu zapewnienie trwałej koordynacji i realizacji działań wspierających cyberodporność Ukrainy. Ministerstwo Cyfryzacji w 2025 r. kontynuowało funkcję koordynatora „Back Office" w gromadzeniu i przekazywaniu potrzeb cyberbezpieczeństwa Ukrainy, a także było zaangażowane w rozwój projektu i struktur Mechanizmu oraz jego współpracę międzynarodową, w tym z instytucjami publicznymi i prywatnymi państw członkowskich. Polska, z udziałem Ministerstwa Cyfryzacji działa także aktywnie w ramach Regionalnego Centrum Cyberobrony (RCDC) w Wilnie.

WSPÓŁPRACA BILATERALNA I MULTILATERALNA

W 2025 r. Ministerstwo Cyfryzacji kontynuowało oraz rozwijało współpracę bilateralną i multilateralną w obszarze cyberbezpieczeństwa oraz nowych technologii. Jednym z kluczowych elementów działań było zacieśnianie relacji międzynarodowych poprzez zawieranie porozumień o współpracy oraz aktywny udział w inicjatywach wielostronnych.

W 2025 r. podpisano:

- Memorandum of Understanding pomiędzy Ministrem Cyfryzacji a Rządowym Urzędem ds. Bezpieczeństwa Informacji Republiki Słowenii w zakresie współpracy w tym obszarze. Porozumienie przewiduje m.in. wymianę informacji i dobrych praktyk dotyczących zagrożeń w cyberprzestrzeni, współpracę pomiędzy właściwymi instytucjami oraz wspólne działania na rzecz wzmacniania cyberodporności obu państw.
- Memorandum of Understanding pomiędzy Ministerstwem Cyfryzacji a Ministerstwem Bezpieczeństwa Publicznego Socjalistycznej Republiki Wietnamu w sprawie cyberbezpieczeństwa. Porozumienie dotyczy pogłębionej współpracy dwustronnej, obejmującej przede wszystkim wymianę informacji, wspólne szkolenia oraz podnoszenie kompetencji

ekspertów w zakresie zapobiegania i zwalczania cyberprzestępczości. Przewiduje ono także organizację warsztatów i konferencji, jak również wymianę doświadczeń w obszarze wykrywania incydentów cybernetycznych i reagowania na nie, co ma na celu wzmocnienie cyberodporności obu państw w obliczu globalnych zagrożeń cyfrowych

W 2025 r. Ministerstwo Cyfryzacji brało aktywny udział w działaniach ukierunkowanych na wzmacnianie globalnej współpracy w zakresie przeciwdziałania cyberprzestępczości, w szczególności w ramach prac nad Konwencją ONZ przeciwko cyberprzestępczości. Konwencja została podpisana w imieniu Rzeczypospolitej Polskiej przez Wicepremiera i Ministra Cyfryzacji podczas wizyty w Hanoi w październiku 2025 r.

Równolegle Ministerstwo Cyfryzacji prowadziło intensywny dialog oraz realizowało spotkania eksperckie i polityczne w obszarze cyberbezpieczeństwa z licznymi partnerami międzynarodowymi, w tym z Niemcami, Kanadą, Australią oraz Mołdawią. Szczególny nacisk położono na rozwój współpracy z Republiką Mołdawii, obejmującej w szczególności wsparcie w zakresie zabezpieczenia procesów wyborczych oraz wzmacniania odporności instytucji publicznych na zagrożenia cybernetyczne.

ORGANIZACJE MIĘDZYNARODOWE

Organizacja Narodów Zjednoczonych (ONZ)

Ministerstwo Cyfryzacji brało aktywny udział w pracach Zgromadzenia Ogólnego ONZ („ZO") dotyczących dokumentu końcowego posiedzenia wysokiego szczebla ZO, poświęconego ogólnemu przeglądowi realizacji wyników Światowego Szczytu Społeczeństwa Informacyjnego (WSIS).

Minister Cyfryzacji uczestniczył w światowej edycji Forum Zarządzania Internetem (IGF) w Norwegii w czerwcu 2025 r. W ramach wydarzenia wygłosił wystąpienie inauguracyjne, w którym zwrócił uwagę na rosnące znaczenie wzmacniania cyberbezpieczeństwa w obliczu współczesnych wyzwań.

Minister Cyfryzacji odbył spotkanie z Wysłannikiem Sekretarza Generalnego Organizacji Narodów Zjednoczonych ds. technologii w trakcie Forum Zarządzania Internetem (IGF). Podczas rozmów poinformował o aktualizacji planu zarządzania incydentami cyberbezpieczeństwa w Unii Europejskiej, przeprowadzonej w ramach polskiej prezydencji w Radzie UE, oraz podkreślił otwartość Polski na współpracę w obszarze cyberbezpieczeństwa na forum ONZ.

Organizacja Współpracy Gospodarczej i Rozwoju (OECD)

W toku konsultacji projektów dokumentów oraz raportów opracowywanych przez OECD Ministerstwo Cyfryzacji dokonywało oceny, czy zagadnienia cyberbezpieczeństwa zostały ujęte w sposób adekwatny i zgodny z obowiązującymi standardami.

Organizacja Bezpieczeństwa i Współpracy w Europie (OBWE)

W związku z wyborami prezydenckimi przeprowadzonymi w Rzeczypospolitej Polskiej w 2025 r. Ministerstwo Cyfryzacji współpracowało z misją obserwacyjną Biura Instytucji Demokratycznych i Praw Człowieka OBWE. W ramach tej współpracy przekazano informacje na temat działań podejmowanych przez resort, ukierunkowanych na zapewnienie kompleksowych krajowych ram bezpieczeństwa procesu wyborczego oraz przeciwdziałanie dezinformacji, w tym dezinformacji pochodzącej z zagranicy.

Międzynarodowy Związek Telekomunikacyjny (ITU)

Ministerstwo Cyfryzacji aktywnie uczestniczy w pracach Międzynarodowego Związku Telekomunikacyjnego (ITU), w ramach których realizowane są globalne inicjatywy na rzecz cyberbezpieczeństwa, obejmujące m.in. opracowywanie standardów, działania szkoleniowe, rozwój zespołów reagowania na incydenty oraz wspieranie współpracy międzynarodowej.

Internetowa Korporacja ds. Nadanych Nazw i Numerów (ICANN)

Jako członek Rządowego Komitetu Doradczego ICANN (Governmental Advisory Committee – GAC) Ministerstwo Cyfryzacji uczestniczyło w procesie konsultacyjnym dotyczącym opracowywania przepisów oraz rekomendacji w zakresie polityk mających na celu zapobieganie celowym nadużyciom infrastruktury systemu nazw domen (DNS abuse), w tym takim zjawiskom jak phishing, złośliwe oprogramowanie, botnety, pharming czy wykorzystywanie spamu do przeprowadzania ataków. Działania ICANN w tym obszarze obejmują m.in. ustanawianie zasad dla rejestrów i rejestratorów, monitorowanie nadużyć, współpracę z podmiotami branżowymi oraz wspieranie inicjatyw służących podnoszeniu poziomu bezpieczeństwa ekosystemu DNS.

POJEDYNCZY PUNKT KONTAKTOWY

Ministerstwo Cyfryzacji realizowało również zadania Pojedynczego Punktu Kontaktowego, o którym mowa w Dyrektywie NIS, oraz koordynowało współpracę z podmiotami odpowiedzialnymi za cyberbezpieczeństwo, jak również prowadziło konsultacje z przedstawicielami resortów kluczowych w ramach współpracy w ramach cyberbezpieczeństwa.

Więcej informacji pod adresem: https://www.gov.pl/web/ia/pojedynczy-punkt-kontaktowy

PRACE LEGISLACYJNE W RAMACH UE

Ministerstwo Cyfryzacji brało ponadto udział w pracach legislacyjnych na poziomie europejskim nad:

- Zaleceniem Rady w sprawie Planu działania UE na rzecz zarządzania cyberkryzysami (CyberBlueprint)
- Rozporządzeniem UE ustanawiającym przepisy mające na celu zapobieganie i zwalczanie seksualnego wykorzystywania dzieci (CSAM).
- Ministerstwo Cyfryzacji brało także udział w pracach Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa oraz Europejskiego Komitetu Certyfikacji Cyberbezpieczeństwa. W ramach tych prac prezentowane było stanowisko Polski dotyczące europejskich programów certyfikacji. W szczególności Ministerstwo brało udział w przyjęciu pierwszego aktu implementującego europejski program certyfikacji cyberbezpieczeństwa – European Union Common Criteria.

WSPÓŁPRACA W RAMACH ENISA

W 2025 r. Ministerstwo Cyfryzacji kontynuowało prace w ramach ENISA Support Action Fund – krótkoterminowych projektów wsparcia zapewnianych przez Komisję Europejską za pośrednictwem Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) państwom członkowskim w świetle podwyższonego zagrożenia złośliwymi działaniami w cyberprzestrzeni w związku z trwającymi konfliktami. Wsparcie ma na celu uzupełnienie już realizowanych działań przez państwa członkowskie na rzecz zwiększenia poziomu bezpieczeństwa i odporności na cyberzagrożenia.

To wsparcie odbywa się poprzez realizowanie przez ENISA usług ex-ante i ex-post. ENISA wspiera państwa członkowskie w ich działaniach na rzecz zapobiegania, wykrywania, analizowania oraz wzmacniania zdolności w zakresie reagowania na zagrożenia i cyberincydenty. Ministerstwo Cyfryzacji jako punkt kontaktowy, przekazuje do ENISA listę beneficjentów wraz z określonym priorytetem, współpracując z podmiotami KSC, mogącymi ubiegać się o środki.

Więcej informacji pod adresem: https://www.gov.pl/web/cyfryzacja/konsultacje-spoleczne-w-sprawie-oceny-agencji-unii-europejskiej-ds.-bezpieczenstwa-sieci-i-informacji-enisa

WSPÓŁPRACA ZAGRANICZNA

We wrześniu 2025 r. zawarto Memorandum Of Understanding pomiędzy Ministerstwem Cyfryzacji a Urzędem ds. Bezpieczeństwa Informacji Rządowej Republiki Słowenii. Głównymi obszarami

współpracy jest wymiana informacji dotyczących zagrożeń w cyberprzestrzeni, cyberbezpieczeństwo nowych technologii, rozwiązania legislacyjne w cyberbezpieczeństwie.

W październiku 2025 r. zawarto Memorandum of Understanding z Ministerstwem Bezpieczeństwa Publicznego Socjalistycznej Republiki Wietnamu. Podobnie jak w przypadku Słowenii, głównymi obszarami współpracy jest wymiana informacji dotyczących zagrożeń w cyberprzestrzeni, cyberbezpieczeństwo nowych technologii, rozwiązania legislacyjne w cyberbezpieczeństwie.

Jednocześnie Ministerstwo Cyfryzacji prowadzi uzgodnienia z Singapurem, Tajwanem, Japonią, Koreą Południową, Nową Zelandią, Kanadą w celu podpisania porozumień o wzajemnej współpracy w ramach cyberbezpieczeństwa.

W dniach 2-4 września 2025 r. z hasłem przewodnim "Czas transformacji – jaka będzie Europa przyszłości?", w ramach XXXIV Forum Ekonomicznego w Karpaczu, odbyło się 7. Forum Cyberbezpieczeństwa organizowane przez Ministerstwo Cyfryzacji. Goście Forum Cyberbezpieczeństwa mieli okazję wysłuchać dyskusji krajowych i międzynarodowych ekspertów z obszaru cyberbezpieczeństwa podczas 3-dniowej sesji paneli tematycznych. Forum to znakomita okazja do

wymiany doświadczeń i poglądów w środowisku międzynarodowym, a część dyskusji dotyczyła zbliżającej się Prezydencji Polski w Radzie UE.

COUNTER RANSOMWARE INITIATIVES

Ministerstwo Cyfryzacji uczestniczyło w międzynarodowej inicjatywie koordynowanej przez USA pn. „Counter Ransomware Initiatives", która ma na celu połączenie wysiłku działań zaangażowanych państw w zwalczanie zagrożeń typu ransomware. Inicjatywa została zapoczątkowana w październiku 2021 r. przez U.S. National Security Council przy Białym Domu i aktualnie liczy prawie 70 członków. Ministerstwo Cyfryzacji aktywnie uczestniczy w pracach grup roboczych CRI. W szczególności w ramach filaru ICRTF (The International Counter Ransomware Task Force), wspólnie z NASK-PIB, amerykańskim Departamentem Bezpieczeństwa Krajowego (DHS) oraz instytutem SANS Ministerstwo Cyfryzacji w pierwszym kwartale 2024 zakończyło projekt RACER (Ransomware Attack Collective Effective Resilience). Obecnie Ministerstwo Cyfryzacji szuka partnerów by rozpocząć analizy działalności grup Advanced Persistent Threat Groups działających w polskiej cyberprzestrzeni w porównaniu z innymi krajami inicjatywy.

WSPARCIE DLA UKRAINY I WSPÓŁPRACA Z UKRAINĄ

W 2025 r. Polska była największym dostawcą terminali Starlink zapewniających dostęp do internetu, co ma kluczowe znaczenie dla zapewnienia ciągłości funkcjonowania państwa ukraińskiego, udzielania pomocy humanitarnej oraz zagwarantowania bezpiecznej łączności, także dla realizowania zadań wojskowych.

MECHANIZM TALLIŃSKI

Polska bierze aktywny udział w inicjatywach wspierających Ukrainę zaatakowaną przez Federację Rosyjską. Jedną z nich jest Mechanizm Talliński. Jest to grupa państw sojuszniczych w ramach NATO, która ma na celu koordynację i wzajemne wspieranie działań poprawiających cyberbezpieczeństwo Ukrainy oraz budowanie jej odporności na cyberzagrożenia. Od momentu powołania do życia inicjatywy do końca 2025 r. kraje Mechanizmu Tallińskiego dostarczyły Ukrainie usług oraz sprzętu software/hardware w obszarze cyberbezpieczeństwa na kwotę ponad 200 mln USD.

INNE ORGANIZACJE MIĘDZYNARODOWE

Ministerstwo Cyfryzacji było zaangażowane w działania w zakresie cyberbezpieczeństwa w ramach Organizacji Narodów Zjednoczonych (ONZ), Organizacji Współpracy Gospodarczej i Rozwoju (OECD),

Organizacji Bezpieczeństwa i Współpracy w Europie (OBWE), Międzynarodowego Związku Telekomunikacyjny (ITU).

Polska od października 2022 r. jest członkiem Regionalnego Centrum Cyberobrony (RCDC). W ramach tej inicjatywy Ministerstwo Cyfryzacji współpracuje z pozostałymi krajami Litwy, Stanów Zjednoczonych Ameryki, Ukrainy i Gruzji. Regionalne Centrum Cyberbezpieczeństwa zostało otwarte w lipcu 2021 r. i służy jako główna platforma praktycznej współpracy z USA w zakresie cyberobrony, a pozostałymi członkami są Ukraina i Gruzja. RCDC przeprowadza regionalne analizy zagrożeń cybernetycznych i wymienia odpowiednie dane z partnerami, organizuje ćwiczenia i szkolenia, a także badania analityczne w dziedzinie cyberbezpieczeństwa.

REALIZACJA PROJEKTU „NATIONAL COORDINATION CENTRE – POLAND" WSPÓŁFINANSOWANEGO Z PROGRAMU CYFROWA EUROPA.

Działania projektowe mają na celu rozwijanie krajowych zdolności w zakresie cyberbezpieczeństwa:

- budowanie silnej społeczności cyberbezpieczeństwa w Polsce,
- wzmacnianie współpracy krajowej i transgranicznej, wymiany informacji i łączenia partnerów do realizacji międzynarodowych projektów,
- działania zmierzające do zwiększenia konkurencyjności polskich podmiotów na europejskim i globalnym rynku.

AWS RE:INFORCE

W dniach 16-18 czerwca 2025 r. w Filadelfii odbyła się kolejna **edycja AWS re:Inforce - prestiżowej konferencji poświęconej bezpieczeństwu w chmurze or**ganizowane przez Amazon Web Services – naszego partnera PWCyber.

Uczestnicy konferencji mieli dostęp do ponad 250 sesji technicznych, warsztatów, laboratoriów typu hands-on oraz tzw. AWS Jams – symulowanych scenariuszy zagrożeń, w których można przetestować wiedzę w praktyce. Program obejmował zagadnienia dot. ochrony danych, bezpieczeństwa aplikacji, zarządzania tożsamością, detekcji zagrożeń oraz zabezpieczaniu środowisk AI.

Wydarzenie było okazją do rozmów przedstawicieli Departamentu Cyberbezpieczeństwa z ekspertami firmy AWS (Eric Strom - Manager AWS Cyber Threat Intelligence, Anthony Elton – Principal, AWS Office of the CISO, Nima Sharifi Mehr - Principal Security Engineering oraz Daniel Grabski - Principal Security Strategist) o szczególnych rozwiązaniach wspomagających bieżącą pracę przy analizach danych dużej skali pod kątem prewencyjnej ochrony przez cyberatakami.

Nie zabrakło również przestrzeni do rozmów z partnerami technologicznymi AWS w specjalnej strefie Expo, gdzie swoje rozwiązania miało okazję zaprezentować ponad 70 firm z branży cyberbezpieczeństwa.

SPIS TABEL:

SPIS ILUSTRACJI:

OZNACZENIA TLP

Traffic Light Protocol (TLP) jest to zestaw reguł, pogrupowanych w 4 kategorie, używanych w celu lepszego zdefiniowania grupy odbiorców wrażliwych informacji. Dla ułatwienia kategorie opisywane są czterema kolorami (czerwony, pomarańczowy, zielony oraz biały). Zakwalifikowanie do odpowiedniej kategorii leży po stronie organizacji, z której pochodzą informacje. Jeśli odbiorca chciałby podzielić się uzyskanymi informacjami z szerszym gronem, musi uzyskać odpowiednią akceptację od autora wiadomości.

Tabela 48. Oznaczenia TLP

Oznaczenie	Odbiorca wiadomości	Autor wiadomości
TLP:RED	Odbiorcy nie mogą dzielić się przekazanymi informacjami z nikim, z wyjątkiem innych odbiorców tych wiadomości.	Oznaczenie wiadomości, które mogą za sobą nieść poważne zagrożenie ujawnienia wrażliwych danych w wyniku ich nieprawidłowego przetworzenia, jak również, gdy ich wykorzystanie przez innych niż odbiorcy nie ma sensu.
TLP:AMBER	Odbiorcy mogą dzielić się informacjami jedynie w obrębie swojej organizacji (a także jej klientów i consituency) z osobami, które muszą poznać wiadomości oraz jedynie w zakresie niezbędnym do podjęcia stosownych działań. Dodatkowe ograniczenia mogą zostać wyspecyfikowane przez nadawcę w dowolnym zakresie i muszą być przestrzegane. Jednym ze standardowych ograniczeń jest oznaczenie TLP:AMBER+STRICT, które pozwala dzielić się informacjami wyłącznie w obrębie organizacji.	Oznaczenie wiadomości wymagających podjęcia odpowiednich kroków przez dodatkowe osoby. Informacje te niosą ze sobą ryzyko ujawnienia zbyt wielu wrażliwych danych, jeśli zostałyby przekazane podmiotom innym niż bezpośrednio zaangażowanym.
TLP:GREEN	Odbiorcy mogą dzielić się informacji ze swoimi współpracownikami, w ramach swojej i partnerskich organizacji oraz w swoim środowisku. Nie można jednak udostępniać tych informacji przez publiczne kanały informacyjne.	Oznaczenie wiadomości niosących ze sobą informacje ogólnie przydatne dla wszystkich organizacji partnerskich oraz w obrębie środowiska.
TLP:CLEAR	Dystrybucja informacji nie podlega żadnym ograniczeniom (z wyjątkiem praw autorskich).	Oznaczenie wiadomości, których wykorzystanie nie powinno wiązać się z żadnym bądź minimalnym ryzykiem niewłaściwego użycia.

Źródło: *cert.pl*