

OPIS ZAŁOŻEŃ PRZEDSIĘWZIĘCIA INFORMATYCZNEGO O PUBLICZNYM ZASTOSOWANIU

Tytuł przedsięwzięcia	Wsparcie realizacji zadań Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC)		
Wnioskodawca	Minister Cyfryzacji		
Beneficjent	Ministerstwo Cyfryzacji		
Partnerzy	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK-PIB)		
Źródło finansowania	Budżet państwa - część 27 Fundusze Europejskie na Rozwój Cyfrowy 2021–2027, Priorytet IV, Działanie FERC.04.01 „Wzmocnienie cyberbezpieczeństwa oraz rozwój odpornej infrastruktury przetwarzania danych”		
Całkowity koszt przedsięwzięcia	230 000 000,00 zł		
Planowany okres realizacji przedsięwzięcia	08-2026 do 06-2030		
Osoba kontaktowa	Joanna Wójcik	Joanna.Wojcik@cyfra.gov.pl	882377130

1. POWODY PODJĘCIA PRZEDSIĘWZIĘCIA

1.1. Identyfikacja problemu i potrzeb

Przedsięwzięcie to odpowiedź na kluczowe wyzwania związane z funkcjonowaniem KSC, szczególnie w obszarze koordynacji reagowania na incydenty, zapewnienia spójności środowiska teleinformatycznego oraz zwiększenia odporności infrastruktury państwa. Istotą przedsięwzięcia jest przejście od modelu rozproszonego, opartego na częściowo niezależnych narzędziach i rejestrach, do modelu zintegrowanego, w którym dane, procesy i usługi są wzajemnie powiązane i zarządzane centralnie.

Produkty projektu obejmują m.in. rozwój i integrację systemów teleinformatycznych wykorzystywanych w ramach KSC, w tym rozbudowę systemu obsługi incydentów (S46), zakup narzędzia analitycznego CTI, rozbudowa platformy typu Scrubbing Center, które zapewniają ochronę AntyDDoS, a także portalu cyber.gov.pl pełniącego funkcję centralnego punktu kontaktowego. Produkty te przyjmują formę nowych lub zmodyfikowanych modułów systemowych, wspólnej warstwy integracyjnej (API), systemów umożliwiających sprawną wymianę informacji pomiędzy interesariuszami.

Obecnie interesariusze systemu zmagają się z ograniczoną interoperacyjnością narzędzi, co skutkuje fragmentaryzacją informacji, opóźnieniami w reagowaniu i zwiększonym obciążeniem operacyjnym. Brak pełnej automatyzacji procesów wymusza wykonywanie czynności manualnych, co przy rosnącej liczbie incydentów prowadzi do spadku efektywności i zwiększenia ryzyka błędów. Niewystarczający rozwój funkcji analitycznych utrudnia też identyfikację trendów i prognozowanie zagrożeń.

Przedsięwzięcie pozwoli zbudować spójną architekturę systemową, zwiększą się zdolności predykcyjne i poprawi odporność infrastruktury krytycznej. Wzmocni się rola centralnego ośrodka koordynacyjnego.

Planowane zmiany zwiększą funkcjonalność, skalowalność i użyteczność S46, wzmacniając jego

rolę jako narzędzia wspierającego realizację zadań w obszarze cyberbezpieczeństwa oraz współpracę z interesariuszami systemu. W rezultacie zmniejszy się rozbieżność pomiędzy stanem obecnym a oczekiwanym.

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
Minister Cyfryzacji (Wnioskodawca/ Beneficjent)	- brak zintegrowanego narzędzia koordynacji działań PCOC - ograniczone możliwości analityczne i raportowe - brak centralizacji danych	1
Podmioty KSC (CSIRT, administracja publiczna, OIK, podmioty kluczowe i podmioty ważne)	- brak wspólnego obrazu sytuacji cyberbezpieczeństwa - niewystarczająca interoperacyjność systemów - ograniczona automatyzacja wymiany informacji - niewystarczająca odporność infrastruktury	30000
Obywatele pełnoletni	- ryzyko braku ciągłości usług publicznych - ograniczony dostęp do aktualnej informacji o zagrożeniach	30 mln
Przedsiębiorcy	- ryzyko braku ciągłości usług publicznych - ograniczony dostęp do aktualnej informacji o zagrożeniach	3 mln
Służby i instytucje bezpieczeństwa	- ograniczona wymiana informacji międzyinstytucjonalnej - brak standaryzacji procesów	5000

1.2. Opis stanu obecnego

KSC dysponuje funkcjonującymi rozwiązaniami organizacyjnymi i technicznymi wspierającymi reagowanie na incydenty, wymianę informacji oraz ochronę infrastruktury teleinformatycznej, które są rozwijane, lecz pozostają częściowo rozproszone i wymagają dalszej integracji. PCOC pełni rolę mechanizmu współpracy między instytucjami, zapewniając koordynację działań i wymianę informacji, jednak nie posiada pełnej formalizacji ani zintegrowanego zaplecza systemowego.

System S46 stanowi podstawową platformę obsługi incydentów i wymiany informacji w KSC. Jest wykorzystywany operacyjnie, lecz nie obejmuje wszystkich podmiotów, a część procesów wymaga dalszej automatyzacji i ujednolicenia.

Portal cyber.gov.pl pełni funkcję centralnego punktu kontaktowego i dostępu do usług w obszarze cyberbezpieczeństwa, jednak jego integracja z systemami operacyjnymi KSC pozostaje ograniczona.

Rozwiązania AntyDDoS zapewniają ochronę dla wybranych podmiotów publicznych, jednak ich zasięg i zdolności wymagają dalszego rozszerzenia.

Zdolności CTI rozwijane są w sposób rozproszony, bez jednolitej platformy analitycznej, co ogranicza możliwości prognozowania zagrożeń i koordynacji działań.

Obecnie funkcjonują odrębne systemy i rozwiązania wspierające cyberbezpieczeństwo, które wymagają: dalszej integracji, rozbudowy infrastrukturalnej, zwiększenia automatyzacji analitycznej (CTI), zapewnienia zgodności z nowelizowanymi przepisami ustawy o KSC oraz Krajowymi Ramami Interoperacyjności (KRI).

Projekt wspiera także wydawanie rekomendacji Pełnomocnika Rządu ds. Cyberbezpieczeństwa,

w tym dotyczące:

- bieżącej aktualizacji i zarządzania podatnościami w kluczowych systemach
- zapewnienia pełnej widoczności i centralnego nadzoru nad cyberbezpieczeństwem państwa.

2. EFEKTY PRZEDSIĘWZIĘCIA

W jaki sposób przedsięwzięcie realizuje Strategię Cyfryzacji Państwa?

Projekt wpisuje się w realizację Strategii Cyfryzacji Polski do 2035 r., w obszarach cyberbezpieczeństwa, interoperacyjności oraz rozwoju usług cyfrowych państwa. Odpowiada na kluczowe założenie Strategii dotyczące odejścia od silosowości administracji poprzez integrację systemów KSC, budowę wspólnego modelu danych oraz wykorzystanie API do wymiany informacji.

Przedsięwzięcie wzmacnia bezpieczną przestrzeń cyfrową, rozwijając systemy wykrywania i reagowania na incydenty (S46, CTI, AntyDDoS) oraz centralną koordynację w ramach PCOC. W Strategii cyberbezpieczeństwo wskazane jest jako kluczowy warunek stabilności państwa i usług publicznych. System S46 zostanie rozbudowany o nowe funkcjonalności oraz zwiększona zostanie jego pojemność i moc przetwarzania danych. System ADDoS zostanie udostępniony dla kolejnych instytucji, aby ochronić je przed atakami DDoS. Dostęp do platform CTI zostanie rozszerzony o kolejne instytucje, aby mogły wspierać proces analityczny w ramach PCOC.

Projekt realizuje zasadę digital by default, poprzez rozwój zintegrowanych e usług (cyber.gov.pl) oraz wspiera interoperacyjność rejestrów i ponowne wykorzystanie danych w administracji.

Projekt wzmacnia suwerenność cyfrową państwa poprzez rozwój krajowych systemów oraz centralizację przetwarzania danych o zagrożeniach, zapewniając ich bezpieczeństwo i kontrolę. Przedsięwzięcie z uwagi na planowane działania, realizować będzie następujące cele Strategii:

Cel 1.3.1: Funkcjonujący krajowy system cyberbezpieczeństwa jest dojrzały i efektywny,

Cel 1.3.3: Systemy informacyjne w sferze publicznej (w tym militarnej) oraz prywatnej posiadają wysoki poziom odporności,

Cel 1.4.2: Przedsięwzięcia informatyczne są realizowane i zarządzane w sposób skoordynowany, przejrzysty i efektywny,

Cel 2.3.1: Publiczne systemy teleinformatyczne i rejestry publiczne są Interoperacyjne.

Przedsięwzięcie pośrednio przyczynia się do osiągnięcia wskaźnika nr 7 Strategii Cyfryzacji Państwa „Powołanie centralnej instytucji odpowiedzialnej za cyberbezpieczeństwo na poziomie krajowym”. W ramach przedsięwzięcia wspierana będzie realizacja zadań PCOC w obecnym kształcie (art. 62a ustawy o KSC). Natomiast po powołaniu nowej centralnej instytucji odpowiedzialnej za cyberbezpieczeństwo na poziomie krajowym, przedsięwzięcie będzie wspierało realizację zadań tej nowej instytucji.

Jakie inne strategie, polityki publiczne lub wymagania strategiczne realizuje przedsięwzięcie?

Projekt ma znaczenie strategiczne, a zadania zaplanowane w ramach projektu są wprost wskazane w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej, m.in: funkcjonowanie PCOC, rozwój systemu S46, rozwój i usprawnianie mechanizmów koordynacji KSC i należytego zarządzania całym systemem, rozpoznawanie zagrożeń w cyberprzestrzeni (CTI) i zapewnienie ochrony AntyDDoS dla podmiotów publicznych oraz istotnych z punktu widzenia cyberbezpieczeństwa kraju.

2.1. Cele i korzyści wynikające z przedsięwzięcia

Cel - 1	Zwiększenie poziomu cyberbezpieczeństwa państwa poprzez wzmocnienie koordynacji reagowania na incydenty, rozwój centralnych zdolności
---------	---

	analitycznych oraz podniesienie odporności infrastruktury teleinformatycznej podmiotów krajowego systemu cyberbezpieczeństwa, w szczególności poprzez rozwój i integrację systemów wspierających PCOC, S46 oraz wdrażanie rozwiązań ochronnych i monitorujących bezpieczeństwo danych.
Cel strategiczny	Projekt wpisuje się w realizację: 1. Strategii Cyberbezpieczeństwa RP w zakresie a) celu szczegółowego 1 – Rozwój krajowego systemu cyberbezpieczeństwa oraz b) celu szczegółowego 3 - Podniesienie poziomu odporności systemów informacyjnych w sferze publicznej (w tym militarnej) oraz prywatnej. 2. Strategii Cyfryzacji Państwa
Korzyść:	- zwiększenie zdolności instytucji publicznych do projektowania i wdrażania rozwiązań cyfrowych - zmniejszenie liczby skutecznych incydentów cyberbezpieczeństwa - zwiększenie dostępności usług cyfrowych dla interesariuszy - poprawa zdolności wykrywania i analizy zagrożeń i poprawa ochrony przed nimi
KPI:	KPI 1 - Instytucje publiczne otrzymujące wsparcie na opracowywanie usług, produktów i procesów cyfrowych
Wartość aktualna i docelowa KPI:	1
Metoda pomiaru KPI	Metoda i sposób pomiaru: zliczanie liczby instytucji publicznych objętych wsparciem w projekcie na podstawie zawartego porozumienia o dofinansowaniu, pomiar na podstawie potwierdzenia wykorzystania wsparcia (np. dokumentacji księgowej) Źródło danych: dane własne, porozumienie o dofinansowaniu Częstotliwość pomiaru: kwartalnie (raportowanie we wnioskach o płatność postępu rzeczowego) oraz końcowo na zakończenie projektu
Cel - 2	Zwiększenie poziomu cyberbezpieczeństwa państwa poprzez wzmocnienie koordynacji reagowania na incydenty, rozwój centralnych zdolności analitycznych oraz podniesienie odporności infrastruktury teleinformatycznej podmiotów krajowego systemu cyberbezpieczeństwa, w szczególności poprzez rozwój i integrację systemów wspierających PCOC, S46 oraz wdrażanie rozwiązań ochronnych i monitorujących bezpieczeństwo danych.
Cel strategiczny	Projekt wpisuje się w realizację: 1. Strategii Cyberbezpieczeństwa RP w zakresie a) celu szczegółowego 1 – Rozwój krajowego systemu cyberbezpieczeństwa oraz b) celu szczegółowego 3 - Podniesienie poziomu odporności systemów informacyjnych w sferze publicznej (w tym militarnej) oraz prywatnej. 2. Strategii Cyfryzacji Państwa
Korzyść:	- zwiększenie zdolności instytucji publicznych do projektowania i wdrażania rozwiązań cyfrowych - zmniejszenie liczby skutecznych incydentów cyberbezpieczeństwa - zwiększenie dostępności usług cyfrowych dla interesariuszy - poprawa zdolności wykrywania i analizy zagrożeń i poprawa ochrony przed nimi

KPI 2 - Liczba podmiotów wspartych w zakresie cyberbezpieczeństwa

KPI:	
Wartość aktualna i docelowa KPI:	55000 85000
Metoda pomiaru KPI	Metoda i sposób pomiaru: zliczanie liczby podmiotów korzystających z wdrożonych rozwiązań (np. AntyDDoS, S46, CTI), identyfikacja podmiotów przyłączonych do systemów lub objętych ochroną/usługą, Źródło danych: logi i rejestry systemów (S46, CTI, AntyDDoS), bazy podmiotów objętych wsparciem w ramach KSC, raporty operacyjne i statystyki wykorzystania systemów. Częstotliwość pomiaru: kwartalnie i na zakończenie projektu
Cel - 3	Zwiększenie poziomu cyberbezpieczeństwa państwa poprzez wzmocnienie koordynacji reagowania na incydenty, rozwój centralnych zdolności analitycznych oraz podniesienie odporności infrastruktury teleinformatycznej podmiotów krajowego systemu cyberbezpieczeństwa, w szczególności poprzez rozwój i integrację systemów wspierających PCOC, S46 oraz wdrażanie rozwiązań ochronnych i monitorujących bezpieczeństwo danych.
Cel strategiczny	Projekt wpisuje się w realizację: 1. Strategii Cyberbezpieczeństwa RP w zakresie a) celu szczegółowego 1 – Rozwój krajowego systemu cyberbezpieczeństwa oraz b) celu szczegółowego 3 - Podniesienie poziomu odporności systemów informacyjnych w sferze publicznej (w tym militarnej) oraz prywatnej. 2. Strategii Cyfryzacji Państwa
Korzyść:	- zwiększenie zdolności instytucji publicznych do projektowania i wdrażania rozwiązań cyfrowych - zmniejszenie liczby skutecznych incydentów cyberbezpieczeństwa - zwiększenie dostępności usług cyfrowych dla interesariuszy - poprawa zdolności wykrywania i analizy zagrożeń i poprawa ochrony przed nimi
KPI:	KPI 3 - Liczba podmiotów wspartych w zakresie rozwoju usług, produktów i procesów cyfrowych
Wartość aktualna i docelowa KPI:	1
Metoda pomiaru KPI	Metoda i sposób pomiaru: zliczanie liczby podmiotów, które otrzymały wsparcie w zakresie rozwoju/modernizacji usług lub procesów cyfrowych, potwierdzenie poprzez wdrożenie lub korzystanie z produktów projektu (np. rozwój portalu, systemów) Źródło danych: dane własne, raporty z realizacji działań rozwojowych, protokoły odbioru produktów/usług. Częstotliwość pomiaru: kwartalnie i na zakończenie przy rozliczeniu projektu
Cel - 4	Zwiększenie poziomu cyberbezpieczeństwa państwa poprzez wzmocnienie koordynacji reagowania na incydenty, rozwój centralnych zdolności analitycznych oraz podniesienie odporności infrastruktury teleinformatycznej podmiotów krajowego systemu cyberbezpieczeństwa, w szczególności poprzez rozwój i integrację systemów wspierających PCOC, S46 oraz

	wdrażanie rozwiązań ochronnych i monitorujących bezpieczeństwo danych.
Cel strategiczny	Projekt wpisuje się w realizację: 1. Strategii Cyberbezpieczeństwa RP w zakresie a) celu szczegółowego 1 – Rozwój krajowego systemu cyberbezpieczeństwa oraz b) celu szczegółowego 3 - Podniesienie poziomu odporności systemów informacyjnych w sferze publicznej (w tym militarnej) oraz prywatnej. 2. Strategii Cyfryzacji Państwa
Korzyść:	- zwiększenie zdolności instytucji publicznych do projektowania i wdrażania rozwiązań cyfrowych - zmniejszenie liczby skutecznych incydentów cyberbezpieczeństwa - zwiększenie dostępności usług cyfrowych dla interesariuszy - poprawa zdolności wykrywania i analizy zagrożeń i poprawa ochrony przed nimi
KPI:	KPI 4 - Liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji
Wartość aktualna i docelowa KPI:	3
Metoda pomiaru KPI	Metoda i sposób pomiaru: zliczanie liczby wdrożonych lub rozbudowanych systemów spełniających funkcję poprawy cyberbezpieczeństwa, uwzględnienie systemów osiągających pełną funkcjonalność operacyjną (produkcyjne uruchomienie), potwierdzenie poprzez odbiory techniczne i dokumentację wdrożeniową. Źródło danych: dokumentacja wdrożeniowa systemów (CTI, S46, AntyDDoS), protokoły odbioru i uruchomienia systemów, raporty techniczne projektu. Częstotliwość pomiaru: w dniu zakończenia realizacji projektu
Cel - 5	Zwiększenie poziomu cyberbezpieczeństwa państwa poprzez wzmocnienie koordynacji reagowania na incydenty, rozwój centralnych zdolności analitycznych oraz podniesienie odporności infrastruktury teleinformatycznej podmiotów krajowego systemu cyberbezpieczeństwa, w szczególności poprzez rozwój i integrację systemów wspierających PCOC, S46 oraz wdrażanie rozwiązań ochronnych i monitorujących bezpieczeństwo danych.
Cel strategiczny	Projekt wpisuje się w realizację: 1. Strategii Cyberbezpieczeństwa RP w zakresie a) celu szczegółowego 1 – Rozwój krajowego systemu cyberbezpieczeństwa oraz b) celu szczegółowego 3 - Podniesienie poziomu odporności systemów informacyjnych w sferze publicznej (w tym militarnej) oraz prywatnej. 2. Strategii Cyfryzacji Państwa
Korzyść:	- zwiększenie zdolności instytucji publicznych do projektowania i wdrażania rozwiązań cyfrowych - zmniejszenie liczby skutecznych incydentów cyberbezpieczeństwa - zwiększenie dostępności usług cyfrowych dla interesariuszy - poprawa zdolności wykrywania i analizy zagrożeń i poprawa ochrony przed nimi
KPI:	KPI 5 - Poziom dojrzałości zintegrowanego reagowania i monitorowania cyberbezpieczeństwa podmiotów KSC

Wartość aktualna i docelowa KPI:	2 4
Metoda pomiaru KPI	Metoda i sposób pomiaru: Ocena jakościowa w pięciostopniowej skali dojrzałości, przeprowadzana na podstawie analizy stopnia koordynacji reagowania na incydenty, integracji systemów wspierających PCOC i S46, wykorzystania centralnych zdolności analitycznych, wdrożenia rozwiązań ochronnych i monitorujących oraz realizacji działań doskonalących po incydentach, audytach i ćwiczeniach. Ocena końcowa ustalana jest na podstawie kryteriów cząstkowych oraz dowodów operacyjnych i dokumentacyjnych. Źródło danych: Raporty z działań PCOC i systemu S46, rejestry incydentów, raporty z integracji systemów, dokumentacja wdrożeniowa, wyniki audytów i testów bezpieczeństwa, raporty z ćwiczeń cyberbezpieczeństwa, dokumentacja procedur reagowania oraz informacje przekazywane przez podmioty KSC. Częstotliwość pomiaru: końcowo na zakończenie projektu
Cel - 6	Zwiększenie poziomu cyberbezpieczeństwa państwa poprzez wzmocnienie koordynacji reagowania na incydenty, rozwój centralnych zdolności analitycznych oraz podniesienie odporności infrastruktury teleinformatycznej podmiotów krajowego systemu cyberbezpieczeństwa, w szczególności poprzez rozwój i integrację systemów wspierających PCOC, S46 oraz wdrażanie rozwiązań ochronnych i monitorujących bezpieczeństwo danych.
Cel strategiczny	Projekt wpisuje się w realizację: - Strategii Cyberbezpieczeństwa RP w zakresie - celu szczegółowego 1 – Rozwój krajowego systemu cyberbezpieczeństwa oraz - celu szczegółowego 3 - Podniesienie poziomu odporności systemów informacyjnych w sferze publicznej (w tym militarnej) oraz prywatnej. - Strategii Cyfryzacji Państwa
Korzyść:	- zwiększenie zdolności instytucji publicznych do projektowania i wdrażania rozwiązań cyfrowych - zmniejszenie liczby skutecznych incydentów cyberbezpieczeństwa - zwiększenie dostępności usług cyfrowych dla interesariuszy - poprawa zdolności wykrywania i analizy zagrożeń i poprawa ochrony przed nimi
KPI:	KPI 6 - Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych
Wartość aktualna i docelowa KPI:	55000 85000
Metoda pomiaru KPI	Metoda i sposób pomiaru: zliczanie liczby podmiotów korzystających z wdrożonych rozwiązań (np. AntyDDoS, S46, CTI), identyfikacja podmiotów przyłączonych do systemów lub objętych ochroną/usługą, Źródło danych: logi i rejestry systemów (S46, CTI, AntyDDoS), bazy podmiotów objętych wsparciem w ramach KSC, raporty operacyjne i statystyki wykorzystania systemów. Częstotliwość pomiaru: kwartalnie i na zakończenie projektu

2.2. Udostępnione e-usługi

Lp.	Nazwa e-usługi	Typ	Zakres oddziaływania	Poziom dojrzałości e-usługi

2.3. Udostępnione informacje sektora publicznego i zdigitalizowane zasoby

Rodzaj informacji/zasobów	Planowana data udostępnienia	Szacowana liczba obiektów objętych digitalizacją (udostępnianiem informacji)
Udostępnione raporty i sprawozdania dotyczące cyberzagrożeń	30-06-2030	100

Czy wszystkie zdigitalizowane zasoby objęte przedsięwzięciem będą udostępniane bezpłatnie?
TAK/NIE

2.4. Produkty końcowe przedsięwzięcia

Nazwa produktu	Planowana data wdrożenia
Raport z inicjalnych testów prywatności	10-2026
Raport z testów bezpieczeństwa	06-2027
Materiały promocyjne	06-2027
Materiały edukacyjne	06-2027
Narzędzie CTI	12-2027
Raport z testów wydajności	06-2029
Roczny raport z wykorzystania AntyDDoS	12-2029
Modyfikacja systemu S46 w zakresie portalu cyber.gov.pl, systemu centrum S46, systemu komunikacji S46, modułu dostawca usług (SP), wykazu podmiotów kluczowych i ważnych	12-2029
Modyfikacja AntyDDoS	12-2029
Interfejsy API systemu S46	12-2029
Infrastruktura systemu S46 (serwery, urządzenia sieciowe, urządzenia końcowe developerskie, oprogramowanie specjalistyczne)	12-2029

3. KAMIENIE MIŁOWE

Kamienie milowe	Planowany termin osiągnięcia
Zaakceptowana wizja projektu	2026-08-30
Podpisane porozumienie o dofinansowanie realizacji projektu w ramach FERC	2026-09-30
Rozbudowany moduł Wykazu podmiotów kluczowych i podmiotów ważnych o obsługę zarządzania podmiotami krytycznymi	2027-06-30
Rozbudowany moduł Portalu cyber.gov.pl o funkcje pozwalające na tworzenie dedykowanych podstron tematycznych	2027-12-31
Rozbudowany moduł Systemu Centrum S46 o obsługę zarządzania podmiotami krytycznymi	2027-12-31
Zmodyfikowany moduł Systemu Komunikacji S46 polegająca na przebudowie mechanizmów komunikacyjnych i dostosowanie ich do potrzeb użytkowników S46.	2027-12-31
Rozbudowany moduł Systemu Centrum S46 o dedykowane funkcje do zarządzania wieloma podmiotami	2028-06-30
Rozbudowany moduł Portalu cyber.gov.pl o funkcje redakcyjne pozwalające na dynamiczne zarządzanie treścią	2028-06-30
Rozbudowany moduł Systemu Centrum S46 o możliwość integracji systemów użytkowników z S46	2028-12-31
Rozbudowany moduł Systemu Centrum S46 dodająca możliwość zgłaszania posiadanych narzędzi i oprogramowania	2029-06-30
Rozbudowany moduł Systemu Centrum S46 dodająca przesyłania podatności i ostrzeżeń w oparciu o dane wprowadzone przez Podmioty KSC	2029-12-31
Zmodyfikowany moduł Systemu Centrum S46 mająca na celu przebudowie i optymalizacji funkcji systemu dostępnych z poziomu GUI i optymalizacja UX	2030-06-30
Poprawiona operacyjność kluczowych systemów.	2030-06-30

4. KOSZTY

4.1. Koszty ogólne przedsięwzięcia wraz ze sposobem finansowania

Całkowity koszt przedsięwzięcia (netto oraz brutto), w tym	Netto 104 100 757,14 zł Brutto 230 000 000,00 zł	
Procent dofinansowania ze środków UE (brutto)	89,93%	
Procent dofinansowania ze środków z innych źródeł zagranicznych (brutto)	0%	
Procent środków z budżetu państwa (brutto)	10,07%	
Podział całkowitego kosztu przedsięwzięcia na poszczególne lata (netto oraz brutto)	2026	Netto 6 745 951,22 zł Brutto 9 409 066,40 zł
	2027	Netto 22 810 731,71 zł Brutto 38 436 925,20 zł
	2028	Netto 38 765,00 zł Brutto 63 043 822,20 zł
	2029	Netto 46 876 910,00 zł Brutto 75 224 359,80 zł
	2030	Netto 27 628 399,21 zł Brutto 43 885 826,40 zł

4.2. Wykaz poszczególnych pozycji kosztowych

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
Oprogramowanie	1. Personel: Zespół ds. obsługi PCOC – eksperci ds. cyberbezpieczeństwa, Zespół i eksperci ds. zagrożeń w cyberprzestrzeni, Zespół zaangażowany w obsługę zdarzeń związanych z działaniem ochrony ADDoS (monitorowanie, reagowanie,	47 258 720,00 zł	Koszty obejmują wynagrodzenia zespołów obsługujących narzędzia/systemy

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
	kontakty z chronionymi podmiotami itp.) - pierwsza linia wsparcia NOC / SOC (Network Operation Center/ Security Operation Center) i CC (Call Center), Personel rozwiązujący trudne problemy, administrujący usługami oraz zapewniający obejmowanie ochroną oraz wdrażanie podmiotów (w tym konsultowanie stosowanych rozwiązań i pomoc w rozwiązywaniu problemów) - druga linia wsparcia, Zespół rozbudowujący i modyfikujący usługę zgodnie z aktualnymi zagrożeniami i zapotrzebowaniem instytucji obejmowanych ochroną, Osoby kierujące projektem i zespołami roboczymi, osoby realizujące zadania obsługi formalnej, organizacyjnej i prawnej relacji z podmiotami objętymi ochroną oraz z instytucjami wskazującymi na konieczność prac na rzecz podmiotów obejmowanych ochroną, Zespół		

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
	Dev - zespół programistów odpowiedzialny za wytworzenie oprogramowania związane z rozwojem i utrzymaniem aplikacji., Zespół DevOps - zespół odpowiedzialny za automatyzację procesów wytwórczych i zarządzanie infrastrukturą, prowadzący prace wspierające wytwarzanie oprogramowania i wdrażanie zmian na środowiska produkcyjne, Zespół Utrzymania - zespół odpowiedzialny za utrzymanie infrastruktury i sieci niezbędnej do utrzymania aplikacji, Zespół Wsparcia technicznego - zespół odpowiedzialny za wsparcie klienta końcowego i obsługę zgłoszeń helpdesk, Zespół wsparcia i obsługi procesów - zespół obsługujący procesy wewnątrz i poza aplikacją, które wymagają specyficznej wiedzy domenowej i kompetencji w obszarach wykraczających poza rozwój i		

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
	utrzymanie aplikacji 2. licencje i oprogramowania do każdego z zadań		
Infrastruktura	1. Zakup środków trwałych/dostawy: a) Dostawy sprzętu sieciowego i serwerowego, sprzętu towarzyszącego na potrzeby usług AntyDDoS; b) Modernizacja infrastruktury i sieci systemu S46; c) Modernizacja systemu zabezpieczeń systemu S46; d) Narzędzia i stacje specjalistyczne systemu S46; e) Narzędzia i stacje specjalistyczne do zapewnienia funkcjonalności strony cyber.gov; 2. Zakup usług.: a) narzędzia CTI strategicznego; b) Na potrzeby systemu AntyDDoS: Zapewnienie łączności i kolokacji dla wewnętrznego systemu ochrony FLDX użytkowanego w projekcie oraz objęcie serwisem pogwarancyjnym używanych w projekcie	103 957 731,03 zł	Zapewnienie ciągłości działania, bezpieczeństwa oraz rozwoju infrastruktury teleinformatycznej, w tym systemów AntyDDoS, S46 oraz portalu cyber.gov.pl. Zakup licencji na potrzeby PCOC oraz systemu S46 zapewni ciągły dostęp do aktualizacji, wsparcia technicznego i zgodności z wymaganiami bezpieczeństwa. Oprogramowanie AntyDDoS - przekierowywania i zarządzania ruchem usług AntyDDoS, symulacji ataków i realizacji testów, oprogramowania narzędzi pomiarowych oraz oprogramowania bezpieczeństwa koniecznych do rozbudowy własnych systemów ochrony. Licencja dla strony cyber.gov gwarantuje jej stabilne, bezpieczne działanie oraz możliwość dalszego rozwoju zgodnie z obowiązującymi standardami.

Nazwa pozycji kosztowej	Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
systemów; c) Na potrzeby systemu S46: utrzymanie infrastruktury i sieci - odnowienie wsparcia / gwarancji na serwery, macierze dyskowe, urządzenia sieciowe niezbędnych do zapewnienia ciągłości działania i utrzymania środowiska produkcyjnego (z uwzględnieniem obecnych trzech centrów danych), preprodukcyjnego, środowisk wytwórczych oraz środowisk testowych i szkoleniowych zapewniających utrzymanie i rozwój. Kolokacja oraz utrzymanie sieci l3vpn. Usługi chmurowe - Zapewnienie dostępu do usług chmurowych na potrzeby Systemu S46 dla zapewnienia ciągłości działania Systemu. d) Zapewnienie dostępu do usług chmurowych na potrzeby utrzymania ciągłości działania portalu cyber.gov.pl. 3. Dostawy inne		

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
	niż środki trwałe.: a) Zakup materiałów niezbędnych do utrzymania i zapewnienia ciągłości działania systemu AntyDDoS b) Zakup materiałów niezbędnych do utrzymania i zapewnienia ciągłości działania Systemu S46. 4. Oprogramowanie systemowe i narzędziowe związane z infrastrukturą teleinformatyczną: a) licencji w formie subskrypcji na potrzeby PCOC; b) oprogramowania systemowego i symulacyjnego do obsługi AntyDDoS; c) licencji oprogramowania na potrzeby systemu S46 d) licencji oprogramowania na potrzeby strony cyber.gov.		
Koszty UX i grafiki	Nie dotyczy	0,00 zł	W projekcie nie wyodrębniono odrębnej kategorii kosztów UX. Działania związane z analizą potrzeb użytkowników, projektowaniem doświadczeń użytkownika (UX), testowaniem użyteczności, projektowaniem interfejsów oraz doskonaleniem funkcjonalności systemów będą realizowane w ramach bieżących zadań zespołu projektowego oraz

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
			wykonawców zaangażowanych w rozwój produktów projektu. Zakres prac UX będzie uzależniony od potrzeb identyfikowanych na poszczególnych etapach realizacji projektu, w szczególności podczas rozwoju systemu S46 oraz portalu Cyber.gov.pl. Ze względu na niemożność precyzyjnego określenia na etapie planowania projektu udziału czasowego poszczególnych specjalistów w realizacji prac UX, nie przewidziano odrębnych stanowisk ani osobnej kategorii kosztów dedykowanej wyłącznie tym zadaniom. Koszty związane z realizacją działań UX zostały uwzględnione odpowiednio w kosztach personelu projektu oraz kosztach usług zewnętrznych związanych z projektowaniem, rozwojem i utrzymaniem produktów cyfrowych. Materiały wypracowane w ramach projektu zostaną przygotowane w sposób dostępny cyfrowo i będą spełniać standard WCAG 2.2 na poziomie A i AA.
Bezpieczeństwo	1. Zapewnienie usług ochrony przed atakami DDoS przez dostawcę zewnętrznego (podstawowego) 2. Zapewnienie usług ochrony przed atakami DDoS przez dostawcę zewnętrznego (dodatkowego). 3. Utrzymanie systemów zabezpieczeń -	58 776 000,00 zł	Niezbędne do zapewnienia poufności, integralności i dostępności systemów S46 oraz cyber.gov.pl. Platforma ADDOS zapewnia ochronę przed atakami na dostępność usług przez nią ochraniających.

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
	Odnowienie wsparcia / gwarancji na systemy zabezpieczeń wzmacniających odporność Systemu S46 na naruszenia dostępności, poufności i integralności danych.		
Wydajność rozwiązań	Sprawdzenie czy system jest wydajny dla aktualnej liczby użytkowników	0,00 zł	Bezkosztowo
Szkolenia	Szkolenia personelu projektu	2 277 528,97 zł	Szkolenia są niezbędne do podnoszenia kompetencji w obszarze cyberbezpieczeństwa.
Działania informacyjno-promocyjne	Działania informacyjno-promocyjne na potrzeby zadań w projekcie	4 713 520,00 zł	Działania związane z promocją projektu, promocją PCOC, promocją systemów S46 i AntyDDoS, oraz z promocją strony cyber.gov.
Koszty zarządzania i wsparcia (w tym wynagrodzenia personelu wspomagającego)	1. Koszty personelu obsługowego w ramach kosztów pośrednich 2. Pozostałe koszty pośrednie	13 016 500,00 zł	Koszty pośrednie to koszty wynagrodzenia kierownika projektu i koordynatorów merytorycznych – wszystkie osoby niezbędne są, aby zarządzać i spajać zadania w projekcie. Pozostałe koszty pośrednie to koszty administracyjne.

4.3. Koszty ogólne utrzymania wraz ze sposobem finansowania (okres 5 lat)

Całkowity koszt utrzymania trwałości przedsięwzięcia (brutto)	699 165 250,00 zł		Źródło finansowania
Podział całkowitego kosztu utrzymania	2030	62 345 275,00 zł (brutto) (31 368 455,28 zł netto)	krajowe środki publiczne - budżet

trwałości przedsięwzięcia na poszczególne lata (netto oraz brutto)			państwa
	2031	122 488 525,00 zł (brutto) (57 125 121,95 zł netto)	krajowe środki publiczne - budżet państwa
	2032	131 150 225,00 zł (brutto) (58 492 357,72 zł netto)	krajowe środki publiczne - budżet państwa
	2033	140 759 100,00 zł (brutto) (59 678 211,38 zł netto)	krajowe środki publiczne - budżet państwa
	2034	158 044 650,00 zł (brutto) (65 082 926,82 zł netto)	krajowe środki publiczne - budżet państwa
	2035	84 377 475,00 zł (brutto) (34 160 813,00 zł netto)	krajowe środki publiczne - budżet państwa

4.4. Planowane koszty ogólne realizacji (w przypadku przedsięwzięcia współfinansowanego – wkład krajowy z budżetu państwa) oraz koszty utrzymania przedsięwzięcia:

- zostaną pokryte w ramach budżetów odpowiednich dysponentów części budżetowych bez konieczności występowania o dodatkowe środki z budżetu państwa
- ~~- będą powodować konieczność przyznania dodatkowych kwot~~

5. GŁÓWNE RYZYKA

5.1. Ryzyka wpływające na realizację przedsięwzięcia

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Brak skutecznej integracji istniejących systemów i portalu (S46, cyber.gov.pl)	Duża	Średnie	Zaprojektowanie architektury docelowej na poziomie centralnym, wdrożenie standardów interoperacyjności, etapowe testy integracyjne
Opóźnienia w formalizacji i rozwoju PCOC	Duża	Średnie	Zapewnienie powiązania projektu z procesem legislacyjnym (KSC/NIS2), ustanowienie jasnego modelu zarządzania i kompetencji
Brak wystarczających zasobów	Duża	Wysokie	Automatyzacja procesów, centralizacja kompetencji, wykorzystanie wsparcia partnera (NASK), rozwój kompetencji

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
kadrowych do realizacji projektu			wewnętrznych
Wzrost liczby i złożoności incydentów przekraczający zdolności wdrażanych rozwiązań	Duża	Wysokie	Projektowanie systemów skalowalnych, wprowadzenie mechanizmów elastycznej rozbudowy infrastruktury i mocy obliczeniowej
Problemy z objęciem wszystkich podmiotów KSC	Duża	Średnie	Stopniowe wdrażanie, priorytetyzacja kluczowych sektorów, zapewnienie wsparcia dla nowych uczestników systemu
Trudności w standaryzacji procesów między instytucjami	Średnia	Średnie	Opracowanie jednolitych procedur, wytycznych oraz modeli operacyjnych, koordynacja przez PCOC
Opóźnienia w realizacji wdrożeń technologicznych	Średnia	Średnie	Zarządzanie projektowe (harmonogramy, kamienie milowe), podział na etapy, mechanizmy kontroli postępu
Ograniczona adopcja rozwiązań przez użytkowników systemu	Średnia	Niskie	Szkolenia, wsparcie wdrożeniowe, budowanie świadomości i obowiązków regulacyjnych
Ryzyka technologiczne (bezpieczeństwo, kompatybilność, awarie)	Duża	Średnie	Stosowanie standardów bezpieczeństwa, testy, redundancja systemów, ciągłe monitorowanie
Zmiany regulacyjne i legislacyjne (NIS2, KSC) wpływające na zakres projektu	Średnia	Średnie	Elastyczne zarządzanie zakresem projektu, bieżąca współpraca z zespołami legislacyjnymi
Przekroczenie harmonogramu realizacji projektu	Średnia	Niskie	Monitorowanie kamieni milowych, wprowadzenie buforów czasowych, bieżąca kontrola postępu, szybkie działania korygujące
Niezrealizowanie zamówień publicznych i zakupów w planowanym terminie	Średnia	Średnie	Wczesne przygotowanie dokumentacji przetargowej, ścisła współpraca z działem zamówień, harmonogram postępowań, stosowanie trybów przyspieszonych

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Brak wystarczających środków na realizację projektu	Średnia	Średnie	Kontrola budżetu, tworzenie rezerw finansowych, etapowanie wydatków, poszukiwanie alternatywnych źródeł finansowania
Brak możliwości zatrudnienia osób o odpowiednich kompetencjach	Mała	Niskie	Planowanie zasobów z wyprzedzeniem, wykorzystanie outsourcingu, szkolenia pracowników, elastyczne formy zatrudnienia
Nieosiągnięcie wskaźników produktu/celu oraz celu projektu	Duża	Średnie	Bieżący monitoring wskaźników, działania korygujące, doprecyzowanie KPI, regularne przeglądy postępów
Niepełne zidentyfikowanie zależności z innymi projektami	Mała	Niskie	Analiza powiązań projektowych, regularna komunikacja między zespołami, uczestnictwo w zarządzaniu portfelem projektów

5.2. Ryzyka wpływające na utrzymanie efektów

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Brak zapewnienia finansowania utrzymania systemów cyberbezpieczeństwa	Duża	Średnie	Zapewnienie finansowania utrzymania i rozwoju systemów i utrzymania platform i portalu informacyjnego (S46, CTI, AntyDDoS, cyber.gov.pl) w budżecie państwa oraz planach wieloletnich; monitorowanie kosztów infrastruktury, licencji i usług ICT.
Niewystarczające zasoby kadrowe i kompetencyjne	Duża	Średnie	Zapewnienie wykwalifikowanej kadry poprzez szkolenia, rozwój kompetencji oraz współpracę z NASK-PIB; utrzymanie zespołów eksperckich ds. cyberbezpieczeństwa.
Dezaktualizacja technologiczna systemów	Duża	Wysokie	Stosowanie skalowalnej i modułowej architektury systemów oraz ich regularna aktualizacja; ciągłe dostosowanie do zmieniających się zagrożeń cybernetycznych.
Niski poziom integracji i współpracy podmiotów KSC	Duża	Średnie	Wdrożenie jednolitych standardów współpracy, wykorzystanie systemu S46 jako podstawowego narzędzia wymiany informacji oraz rozwój mechanizmów

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
			koordynacji w ramach PCOC.
Naruszenia bezpieczeństwa lub nieskuteczność mechanizmów ochrony	Duża	Średnie	Stały monitoring zagrożeń, audyty bezpieczeństwa oraz wdrażanie procedur reagowania na incydenty.
Uzależnienie od dostawców technologii	Duża	Średnie	Stosowanie otwartych standardów, zapewnienie interoperacyjności systemów.
Niewystarczające wykorzystanie systemów przez użytkowników	Średnia	Średnie	Prowadzenie działań szkoleniowych i informacyjnych oraz rozwój portalu cyber.gov.pl jako centralnego punktu dostępu do usług cyberbezpieczeństwa.
Zmiany regulacyjne wpływające na system	Średnia	Średnie	Monitorowanie zmian legislacyjnych i zapewnienie elastyczności systemów umożliwiającej szybkie dostosowanie do nowych wymagań prawnych.
Przerwy w działaniu infrastruktury krytycznej	Duża	Średnie	Zapewnienie redundancji, backupów, planów ciągłości działania oraz wysokiej dostępności systemów.
Brak dalszego rozwoju systemów	Duża	Średnie	Zaplanowanie ciągłego rozwoju systemów zgodnie ze Strategią Cyberbezpieczeństwa RP oraz zapewnienie finansowania na modernizację w kolejnych latach.

6. OTOCZENIE PRAWNE

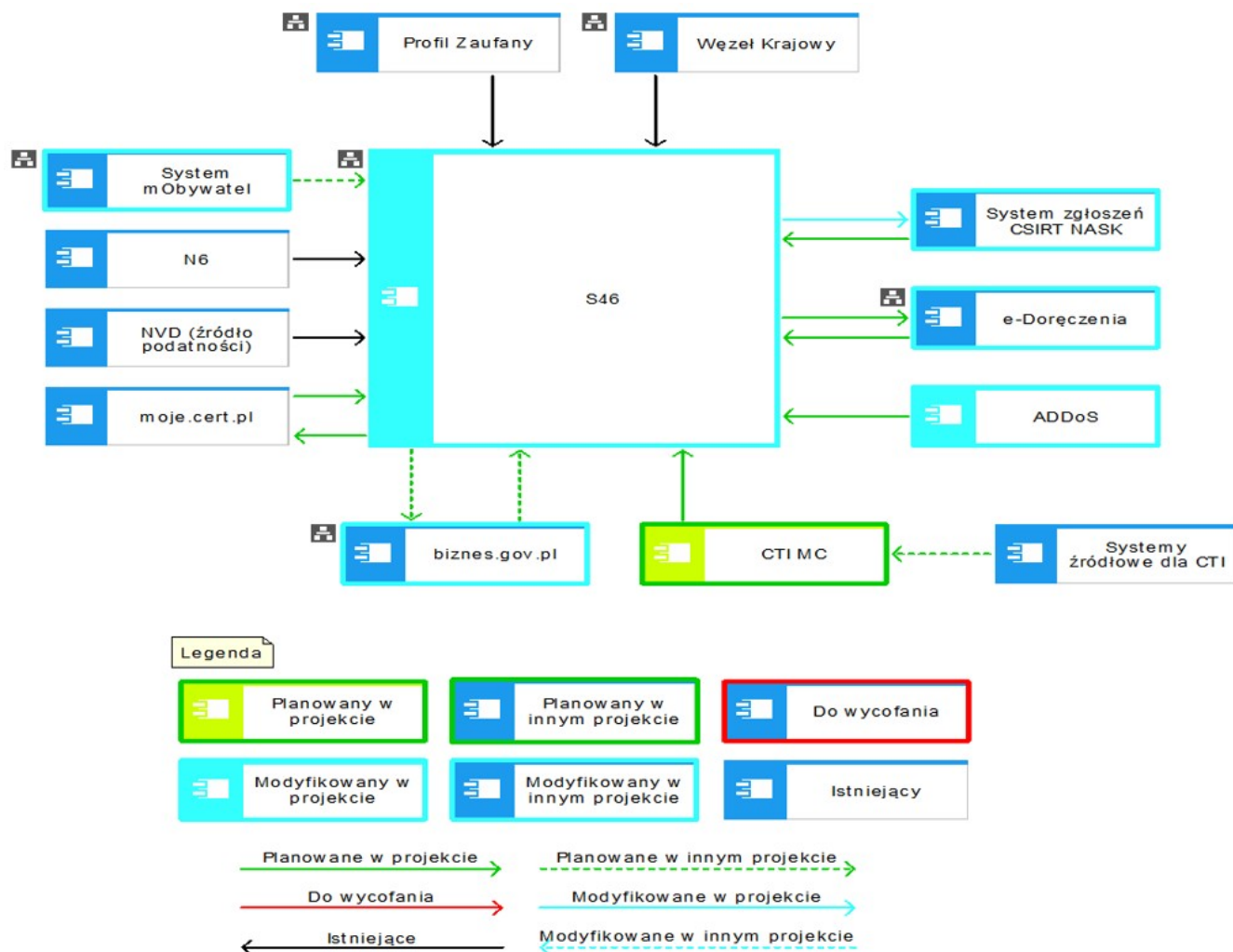
Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
1	Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2026 r. poz. 20 z późn. zm.)	TAK/NIE		
2	Uchwała nr 125 Rady Ministrów z dnia 23 marca 2026 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej (M.P. 2026 poz. 309)	TAK/NIE		
3	Ustawa z dnia 17 lutego 2005 r. o	TAK/NIE		

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
	informatyzacji działalności podmiotów realizujących zadania publicznej (Dz.U. z 2025 r. poz. 1703 z późn. zm.)			
4	Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów informatycznych (Dz.U. z 2024 r. poz. 773)	TAK/NIE		
5	Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi (Akt w sprawie zarządzania danymi) (Dz.U. z 2022 r. poz. 868)	TAK/NIE		
6	Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (Akt w sprawie danych) (Dz.U. z 2023 r. poz. 2854)	TAK/NIE		
7	Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz.U. z 2024 r. poz. 1769)	TAK/NIE		
8	Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U. z 2023 r. poz. 1440)	TAK/NIE		
9	Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2024 r. poz. 1725)	TAK/NIE		
10	Rozporządzenie z dnia 29 czerwca 2020 r. Ministra Cyfryzacji w sprawie profilu zaufanego i podpisu zaufanego (Dz.U. z 2023 r. poz. 2551)	TAK/NIE		
11	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),	TAK/NIE		
12	Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa	TAK/NIE		

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
	teleinformatycznego (Dz.U. Nr 159, poz. 948)			
13	Ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz.U. z 2023 r. poz. 1524)	TAK/NIE		
14	Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz.U. z 2026 r. poz. 3)	TAK/NIE		
15	Rozporządzenie Prezesa Rady Ministrów z dnia 8 maja 2014 r. w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (Dz.U. z 2014 r. poz. 590)	TAK/NIE		
16	Rozporządzenie Ministra Cyfryzacji z dnia 10 marca 2020 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników (Dz.U. z 2020 r. poz. 399)	TAK/NIE		
17	Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U. z 2020 r. poz. 164)	TAK/NIE		

7. ARCHITEKTURA

7.1. Widok kooperacji aplikacji



Lista systemów wykorzystywanych w przedsięwzięciu

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
1	ADDoS	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Advanced Distributed Denial of Service - to system wspierający ochronę infrastruktury teleinformatycznej oraz usług aplikacyjnych przed atakami typu Distributed Denial of Service. Celem systemu jest zapewnienie ciągłości działania usług cyfrowych poprzez wykrywanie i neutralizację ataków wolumetrycznych, protokolowych i aplikacyjnych.	Modyfikowany	Zmiana modułu zarządzania użytkownikami w zakresie ilości podmiotów, dla których świadczona jest usługa.

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			System nie prowadzi rejestrów publicznych. Główne funkcjonalności: - ochrona warstwy infrastrukturalnej (L3/L4) – detekcja i filtrowanie ruchu, - ochrona warstwy aplikacyjnej (L7) – WAF, zarządzanie botami, - analiza behawioralna ruchu, - automatyczne mechanizmy mitigacji (scrubbing, rate limiting). Całość działa automatycznie, minimalizując wpływ na legalny ruch oraz zapewniając ciągłość działania usług. Integracje: System integruje się z krajowymi systemami cyberbezpieczeństwa, w tym systemem S46, w zakresie przekazywania informacji o zagrożeniach i incydentach.		
2	biznes.gov.pl	Ministerstwo Rozwoju i Technologii	Biznes.gov.pl to serwis przeznaczony dla osób zamierzających rozpocząć i prowadzących działalność gospodarczą. Celem portalu jest pomoc w realizacji spraw związanych z zakładaniem i prowadzeniem i zamykaniem działalności oraz udostępnienie narzędzi upraszczających formalny proces założenia i prowadzenia firmy. W serwisie dostępne są opisy usług publicznych oraz formularze	Modyfikowany	

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			pozwalające na ich realizację w sposób zdalny. Za pomocą serwisu, osoby prowadzące firmę mogą składać wnioski do instytucji państwowych drogą elektroniczną, a także załatwiać swoje biznesowe sprawy przez internet. Serwis łączy w sobie wiele usług i funkcji nie tylko dla przedsiębiorców, ale także dla administracji państwowej. Przedsiębiorcy znajdują tutaj szczegółowe informacje o obowiązujących przepisach prawa, wymaganych procedurach i formalnościach związanych z zakładaniem i prowadzeniem działalności gospodarczej w Polsce oraz odniesienie do analogicznych informacji dotyczących pozostałych krajów Unii Europejskiej. Serwis spełnia też rolę wyszukiwarki danych kontaktowych wszystkich instytucji obsługujących przedsiębiorców. Daje praktyczne instrukcje, jak sobie radzić w biznesie i umożliwia realizację spraw administracyjnych drogą elektroniczną.		
3	e-Doręczenia	Ministerstwo Cyfryzacji	Krajowy System Doręczeń Elektronicznych (e-Doręczenia) to system wspierający bezpieczne doręczanie dokumentów elektronicznych pomiędzy podmiotami sektora	Modyfikowany	

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			publicznego, obywatelami i przedsiębiorcami. System zapewnia doręczenie elektroniczne o skutku prawnym równoważnym przesyłce poleconej za potwierdzeniem odbioru, zgodnie z obowiązującymi przepisami krajowymi oraz dyrektywami Unii Europejskiej. W systemie prowadzony jest rejestr publiczny Baza adresów elektronicznych, zawierający dane umożliwiające realizację doręczeń. Główne funkcjonalności systemu obejmują: • Wysyłanie dokumentów elektronicznych z potwierdzeniem doręczenia • Odbieranie dokumentów przez adresatów • Bezpieczne przechowywanie dokumentów w dedykowanej skrzynce doręczeń System jest zintegrowany z krajowymi systemami teleinformatycznymi		
4	moje.cert.pl	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Platforma usługowa moje.cert.pl to platforma usługowa udostępniana przez CSIRT NASK. To system wspierający przekazywanie informacji o zagrożeniach cyberbezpieczeństwa do użytkowników końcowych, instytucji oraz operatorów sieci. Celem systemu jest umożliwienie monitorowania bezpieczeństwa zasobów	Istniejący	

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			użytkowników i dostarczanie informacji o incydentach. System nie prowadzi rejestrów publicznych. System umożliwia odbiorcom dostęp do spersonalizowanych danych o incydentach, takich jak wykryte podatności, infekcje malware czy aktywności złośliwe związane z ich zasobami. Platforma zapewnia bezpieczny portal, w którym użytkownicy mogą monitorować stan bezpieczeństwa swoich systemów, otrzymywać powiadomienia o zagrożeniach oraz pobierać raporty i rekomendacje działań naprawczych. Dane prezentowane w moje.cert.pl pochodzą m.in. z systemu n6 oraz innych źródeł analizy CSIRT NASK. Rozwiązanie wspiera automatyzację reagowania na incydenty i podnosi poziom świadomości cyberzagrożeń, umożliwiając szybkie podejmowanie działań ograniczających ryzyko oraz poprawę ogólnego poziomu bezpieczeństwa organizacji. System integruje się z systemem n6 oraz S46.		
5	N6	Naukowa i Akademicka Sieć Komputerowa –	System n6 to zaawansowana platforma analityczna opracowana przez CSIRT NASK, system wspierający	Istniejący	

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
		Państwowy Instytut Badawczy	gromadzenie, przetwarzanie i analizę informacji o zagrożeniach w cyberprzestrzeni. Celem systemu jest identyfikacja i klasyfikacja incydentów oraz wsparcie reagowania na zagrożenia. System nie prowadzi rejestrów publicznych. Umożliwia zbieranie danych o incydentach bezpieczeństwa z wielu źródeł, takich jak honeypoty, czujniki sieciowe czy zewnętrzne feedy threat intelligence. System automatycznie koreluje i klasyfikuje zdarzenia, identyfikując potencjalne zagrożenia, takie jak infekcje malware, próby skanowania, phishing czy ataki DDoS. Dzięki zastosowaniu mechanizmów analizy behawioralnej i wzorców zagrożeń umożliwia szybkie wykrywanie anomalii i nowych kampanii ataków. n6 wspiera działania operacyjne CSIRT poprzez dostarczanie uporządkowanych informacji o incydentach do odbiorców, takich jak dostawcy usług internetowych, instytucje publiczne i firmy. Umożliwia również automatyczne raportowanie oraz integrację z systemami bezpieczeństwa, wspierając szybkie reagowanie na zagrożenia i podnoszenie poziomu cyberbezpieczeństwa.		

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			System integruje się z systemami krajowymi, w tym S46 i moje.cert.pl.		
6	NVD (źródło podatności)	Podmioty komercyjne , społeczność	National Vulnerability Database (NVD) to system teleinformatyczny prowadzony przez amerykański National Institute of Standards and Technology (NIST), służący do gromadzenia, klasyfikowania i publikowania informacji o podatnościach w produktach informatycznych. Celem systemu jest udostępnianie wiarygodnych i aktualnych danych o podatnościach oraz zagrożeniach dotyczących konkretnych wersji produktów, wspierających zarządzanie ryzykiem i bezpieczeństwem w systemach teleinformatycznych. Zakres danych przetwarzanych w systemie obejmuje: • identyfikację podatnego produktu, • identyfikatory podatności w formacie CVE (Common Vulnerabilities and Exposures), • poziom zagrożenia w formacie CVSS (Common Vulnerability Scoring System), • dodatkowe informacje opisowe dotyczące podatności. System NVD nie prowadzi rejestru publicznego w rozumieniu polskich	Istniejący	

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			przepisów prawa. Główne grupy funkcjonalności systemu obejmują: • publikację danych o podatnościach – w oparciu o standardy CVE i CVSS, • klasyfikację i ocenę ryzyka – dla produktów i komponentów informatycznych, • integrację z systemami zewnętrznymi – system NVD jest zintegrowany z: - o Systemem S46 – w zakresie pozyskiwania danych o podatnościach, - o systemami komercyjnych podmiotów, takimi jak Tenable, Qualys oraz Rapid7. System NVD stanowi jedno z kluczowych źródeł informacji wykorzystywanych w analizie podatności i zarządzaniu ryzykiem cyberbezpieczeństwa w środowiskach administracji publicznej i komercyjnej.		
7	Profil Zaufany	Ministerstwo Cyfryzacji	Profil Zaufany to system wspierający obsługę publicznego systemu identyfikacji elektronicznej, umożliwiający uwierzytelnianie osób fizycznych oraz składanie podpisu zaufanego w kontaktach z administracją publiczną za pośrednictwem usług elektronicznych. Celem systemu jest zapewnienie możliwości identyfikacji i uwierzytelnienia osoby	Istniejący	

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			fizycznej przy użyciu środka identyfikacji elektronicznej – profilu zaufanego – oraz umożliwienie opatrywania dokumentów elektronicznych podpisem zaufanym w procesach realizowanych drogą elektroniczną. Główne grupy funkcjonalności – Wydawanie i zarządzanie profilem zaufanym jako środkiem identyfikacji elektronicznej – Uwierzytelnianie osoby fizycznej przy użyciu profilu zaufanego – Umożliwienie składania podpisu zaufanego na dokumentach elektronicznych – Obsługa procesu potwierdzania, zawieszania i unieważniania profilu zaufanego – Automatyczna aktualizacja danych identyfikacyjnych na potrzeby procesu uwierzytelniania System jest zintegrowany z krajowymi systemami teleinformatycznymi		
8	S46	Ministerstwo Cyfryzacji	System S46 zapewnia obsługę incydentów cyberbezpieczeństwa, wymianę informacji oraz koordynację działań pomiędzy uczestnikami krajowego systemu cyberbezpieczeństwa. W systemie prowadzony jest również publiczny wykaz podmiotów kluczowych i ważnych.	Modyfikowany	1. Rozbudowa modułu Wykaz podmiotów kluczowych i podmiotów ważnych o obsługę zarządzania podmiotami krytycznymi 2.

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			Celem systemu jest zapewnienie narzędzi wspierających realizację zadań krajowego systemu cyberbezpieczeństwa, w szczególności w zakresie obsługi incydentów, wymiany informacji, zarządzania ryzykiem, ostrzegania o zagrożeniach oraz prowadzenia procesów nadzorczych. Główne funkcjonalności: • Obsługa incydentów – umożliwia zgłaszanie, analizę, monitorowanie i koordynację obsługi incydentów cyberbezpieczeństwa. • Wymiana informacji między podmiotami – zapewnia bezpieczne przekazywanie komunikatów, zgłoszeń oraz informacji o zagrożeniach. • Zarządzanie ryzykiem – wspiera identyfikację, ocenę i monitorowanie ryzyk związanych z cyberbezpieczeństwem. • Ostrzeganie o zagrożeniach – umożliwia dystrybucję alertów oraz informacji o nowych zagrożeniach i podatnościach. • Wsparcie procesów nadzorczych – wspomaga realizację działań nadzorczych oraz monitorowanie spełniania obowiązków przez podmioty. • Prowadzenie wykazu podmiotów – umożliwia prowadzenie i aktualizację publicznego rejestru podmiotów		Rozbudowa modułu System Centrum S46: • obsługę zarządzania podmiotami krytycznymi, • dedykowane funkcje do zarządzania wieloma podmiotami • możliwość integracji systemów użytkowników z S46 • przebudowie i optymalizacji funkcji systemu dostępnych z poziomu GUI i optymalizacja UX • dodająca możliwość zgłaszania posiadanych narzędzie i oprogramowanie • dodająca przesyłania podatności i ostrzeżeń w oparciu o dane wprowadzone przez Podmioty KSC 3. Modyfikacja modułu System Komunikacji S46 polegająca na

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			kluczowych i ważnych. Integracje: System integruje się z krajowymi i międzynarodowymi usługami oraz bazami danych, m.in. e-Doręczeniami, Profilem Zaufanym, moje.cert.pl, n6 oraz NVD, zapewniając sprawną wymianę danych i automatyzację procesów.		przebudowie mechanizmów komunikacyjnych i dostosowanie ich do potrzeb użytkowników S46. 4. Rozbudowa modułu Portal cyber.gov.pl: • funkcje redakcyjne pozwalające na dynamiczne zarządzanie treścią • funkcje pozwalające na tworzenie dedykowanych podstron tematycznych 5. Rozbudowa modułu Dostawca Usług: • Dodanie obsługi logowania z zagranicy z użyciem eID
9	System mObywatel	Ministerstwo Cyfryzacji	mObywatel to system teleinformatyczny utworzony w celu umożliwienia obywatelom pobierania i prezentowania dokumentów elektronicznych oraz korzystania z usług cyfrowych przy użyciu aplikacji mobilnej mObywatel. Rozwiązanie to zapewnia wygodny dostęp do danych	Modyfikowany	

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			pochodzących z rejestrów publicznych oraz innych systemów teleinformatycznych podmiotów współpracujących, wspierając cyfrową obsługę spraw urzędowych. W systemie mObywatel prowadzone są rejestry i mechanizmy udostępniania danych obejmujące m.in.: -dokumenty elektroniczne zawierające dane osobowe użytkownika, -dokumenty potwierdzające sytuację prawną lub prawa użytkownika, -dokumenty umożliwiające identyfikację rzeczy powiązanych z użytkownikiem, -elektroniczne odpowiedniki dokumentów urzędowych wydawanych pierwotnie w postaci papierowej. Do głównych funkcjonalności systemu należą: -obsługa aplikacji mobilnej mObywatel, Portalu dla Szkół i Uczelni oraz Portalu Administracyjnego i back endu, - zarządzanie dokumentami i usługami dostępnymi w aplikacji, -prezentacja powiadomień PUSH, -obsługa środka identyfikacji elektronicznej Profil mObywatel, System jest zintegrowany		

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			z krajowymi systemami teleinformatycznymi.		
10	System zgłoszeń CSIRT NASK	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	System zgłoszeń CSIRT NASK to system wspierający rejestrację i obsługę zgłoszeń dotyczących incydentów komputerowych w obszarze określonym w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. System pełni funkcję centralnego narzędzia ticketowego dla CSIRT poziomu krajowego, umożliwiając koordynację i realizację procesu reagowania na incydenty bezpieczeństwa teleinformatycznego. Celem systemu jest zapewnienie sprawnego zarządzania zgłoszeniami incydentów, koordynacja działań analitycznych oraz wsparcie w procesie obsługi incydentów cyberbezpieczeństwa. System nie prowadzi rejestrów publicznych. Główne grupy funkcjonalności: – Rejestracja zgłoszeń incydentów komputerowych – Obsługa procesu reagowania na incydenty – Koordynacja działań CSIRT NASK – Monitorowanie i raportowanie statusu zgłoszeń System jest zintegrowany z krajowymi systemami teleinformatycznymi	Modyfikowany	
11	Węzeł Krajowy	Ministerstwo	Węzeł Krajowy to system wspierający proces	Istniejący	

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
		Cyfryzacji	uwierzytelniania użytkowników korzystających z usług online świadczonych przez podmioty publiczne. System pełni rolę pośrednika pomiędzy systemami identyfikacji elektronicznej a systemami udostępniającymi usługi elektroniczne, umożliwiając bezpieczne przekazywanie potwierdzeń tożsamości. Celem systemu jest zapewnienie jednolitego, bezpiecznego i interoperacyjnego mechanizmu uwierzytelniania użytkowników usług online administracji publicznej poprzez wykorzystanie różnych środków identyfikacji elektronicznej. Główne grupy funkcjonalności – Pośredniczenie w procesie uwierzytelniania użytkowników usług online – Integracja z systemami identyfikacji elektronicznej – Przekazywanie potwierdzeń tożsamości do systemów świadczących usługi elektroniczne – Zapewnienie bezpiecznej wymiany danych identyfikacyjnych Integracje System jest zintegrowany z krajowymi systemami teleinformatycznymi		
12	CTI MC	Ministerst	Cyber Threat Intelligence	Planowany	

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
		wo Cyfryzacji	Ministerstwa Cyfryzacji (CTI MC) to system wspierający zarządzanie informacjami o zagrożeniach cyberbezpieczeństwa dla wybranych podmiotów krajowego systemu cyberbezpieczeństwa. Celem systemu jest pozyskiwanie, agregowanie, przetwarzanie, wzbogacanie, analiza, korelacja oraz prezentacja informacji o zagrożeniach, w tym wskaźników kompromitacji, danych o infrastrukturze wykorzystywanej w atakach, kampaniach cyberzagrożeń oraz technikach, taktykach i procedurach stosowanych przez podmioty atakujące. System nie prowadzi rejestrów publicznych. System obejmuje następujące główne grupy funkcjonalności: Moduł pozyskiwania i agregacji Pobiera surowe dane (IOC, hashe, adresy IP, domeny) z kanałów OSINT, komercyjnych feedów i sieci ISAC Moduł przetwarzania i wzbogacania Normalizuje i deduplikuje pakiety informacji oraz przypisuje kontekst do wskaźników zagrożeń (np. powiązanie z kampaniami grup APT) Silnik analizy i korelacji Klasyfikuje zdarzenia za pomocą modeli AI/NLP oraz mapuje zachowania napastników na macierz MITRE ATT&CK oraz		

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			dokonyuje oceny i priorytetyzacji zagrożeń (scoring) pod kątem realnego ryzyka dla organizacji Moduł wizualizacji i raportowania Generuje grafy powiązań (np. relacje między infrastrukturą a podmiotami atakującymi). System wymienia dane z innymi systemami i źródłami krajowymi oraz zagranicznymi		
13	Systemy źródłowe dla CTI	Dostawca CTI	System wielokrotny Systemy źródłowe dla CTI to systemy wspierające pozyskiwanie, udostępnianie oraz wymianę danych wykorzystywanych przez system CTI. Systemy te stanowią źródło informacji niezbędnych do realizacji procesów biznesowych, operacyjnych i analitycznych obsługiwanych przez CTI. Celem funkcjonowania tej klasy systemów jest zapewnienie dostępu do aktualnych i wiarygodnych danych pochodzących z różnych źródeł, umożliwiających realizację procesów przetwarzania, analizy oraz wymiany informacji w systemie CTI. Główne grupy funkcjonalności – Udostępnianie danych źródłowych na potrzeby systemu CTI – Wymiana informacji pomiędzy systemami współpracującymi	Istniejący	

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			– Aktualizacja i synchronizacja danych wykorzystywanych przez CTI – Wsparcie procesów analitycznych i raportowych – Zapewnienie jakości i spójności danych przekazywanych do systemu CTI Systemy są zintegrowane z krajowymi i zagranicznymi systemami teleinformatycznymi		

Lista przepływów

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
1	S46	biznes.gov.pl	Dane dot. włączenia firmy w skład podmiotów krajowego systemu cyberbezpieczeństwa: • Osoba fizyczna (Użytkownik S46) • Identyfikator osoby fizycznej • Podmiot KSC • NIP • REGON Klasyfikacja podmiotu	Tryb odwołań bezpośrednich, Tryb federacyjny	realizowalny inną metodą	Usługi: SOAP, REST Protokoły: HTTPS, SAML Format danych: XML, JSON
2	biznes.gov.pl	S46	Dane dot. firmy w obszarze podlegania	Tryb odwołań bezpośrednich, Tryb federacyjny	realizowalny inną metodą	Usługi: SOAP, REST Protokoły: HTTPS, SAML

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
			pod NIS2 • Osoba fizyczna • Identyfikator osoby fizycznej • Podmiot KSC • NIP • REGON Klasyfikacja podmiotu			Format danych: XML, JSON
3	S46	e-Doręczenia	Przekazywanie plików i formularza zgłoszenia naruszenia ochrony danych osobowych do UODO • Osoba fizyczna (Użytkownik S46) • Identyfikator osoby fizycznej • Podmiot KSC • NIP • REGON • Adres • Dane kontaktowe Dane administratora danych osobowych	Tryb odwołań bezpośrednich, Tryb federacyjny, Tryb asynchroniczny	krytyczny dla sukcesu projektu	Usługi: SOAP, REST Protokoły: HTTPS, AS4/AS2, SAML Format danych: XML
4	S46	moje.cert.pl	Adresy IP i domeny podmiotów KSC wprowadzone przez podmioty do S46	Tryb odwołań bezpośrednich	krytyczny dla sukcesu projektu	Usługi: REST API Protokoły: HTTPS Format danych: JSON

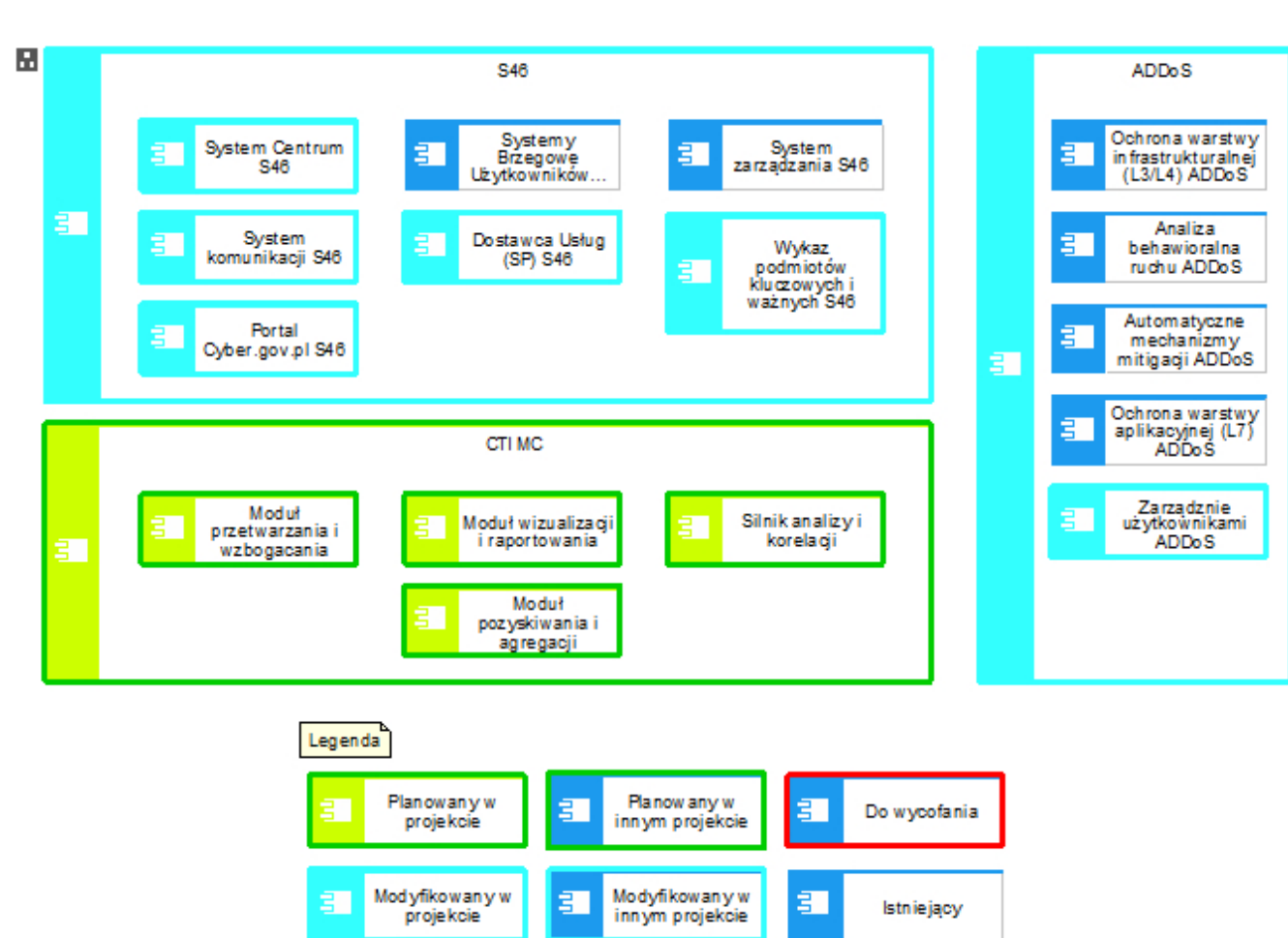
Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
			- Osoba fizyczna (Użytkownik S46) - Podmiot KSC - NIP - REGON - Adres IP Domena			
5	moje.cert.pl	S46	Zweryfikowana lista IP i domen oraz informacje o podatnościach i raporty - Osoba fizyczna (Użytkownik S46) - Podmiot KSC - NIP - REGON - Adres IP Domena	Tryb odwołań bezpośrednich	krytyczny dla sukcesu projektu	Usługi: REST API Protokoły: HTTPS Format danych: JSON
6	N6	S46	Informacje o podatnościach - Adres IP - Domena Podatności	Tryb odwołań bezpośrednich, Tryb wsadowy	krytyczny dla sukcesu projektu	Usługi: REST API, feedy danych Protokoły: HTTPS, SFTP Format danych: JSON, CSV
7	NVD (źródło podatności)	S46	Informacje o podatnościach Podatności	Tryb odwołań bezpośrednich	krytyczny dla sukcesu projektu	Usługi: REST API Protokoły: HTTPS Format danych: JSON
8	Profil Zaufany	S46	Podpisany dokument, plik podpisu - Osoba fizyczna (Użytkownik S46)	Tryb odwołań bezpośrednich, Tryb federacyjny	krytyczny dla sukcesu projektu	Usługi: SOAP, REST Protokoły: HTTPS, SAML Format danych: XML

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
			Identyfikator osoby fizycznej - Podpisany dokument - Plik podpisu			
9	System mObywatel	S46	Dane umożliwiające zgłaszanie zagrożeń z zakresu nielegalnych treści w internecie oraz z zakresu cyberbezpieczeństwa - Osoba fizyczna (Użytkownik S46) - Identyfikator osoby fizycznej - Formularz zgłoszenia incydenty	Tryb odwołań bezpośrednich, Tryb federacyjny	realizowalny inną metodą	Usługi: REST API Protokoły: HTTPS, OAuth2 Format danych: JSON
10	Węzeł Krajowy	S46	Dane uwierzytelnianej osoby - Osoba fizyczna - Identyfikator osoby fizycznej	Tryb federacyjny	krytyczny dla sukcesu projektu	Usługi: SSO (federacyjne) Protokoły: SAML 2.0, OAuth2/OpenID Connect Format danych: XML (SAML), JSON (OIDC)
11	System zgłoszeń CSIRT NASK	S46	Odpowiedzi do podmiotów i zmiany statusu zgłoszonych incydentów Osoba fizyczna (Użytkownik S46)	Tryb odwołań bezpośrednich	krytyczny dla sukcesu projektu	Usługi: REST API Protokoły: HTTPS Format danych: JSON

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
			• Podmiot KSC • Formularz zgłoszenia incydentu • Adres • Dane kontaktowe • Wiadomości do podmiotu • Komentarze			
12	S46	System zgłoszeń CSIRT NASK	Przekazywanie informacji o incydentach • Osoba fizyczna (Użytkownik S46) • Podmiot KSC • NIP • REGON • Adres • Dane kontaktowe • Formularz zgłoszenia incydentu	Tryb odwołań bezpośrednich	krytyczny dla sukcesu projektu	Usługi: REST API Protokoły: HTTPS Format danych: JSON
13	ADDoS	S46	Przekazywanie informacji o trendach, zagrożeniach i statystyki: • Adres IP • Domena • Podatności Dane statystyczne	Tryb odwołań bezpośrednich, Tryb publikacji/subskrypcji, Tryb asynchroniczny	krytyczny dla sukcesu projektu	Usługi: REST API Protokoły: HTTPS TLS Format danych: JSON
14	CTI MC	S46	Komunikaty, ostrzeżenia i raporty analityczne przetworzone ręcznie na podstawie danych z CTI MC	kopiowanie danych	realizowalny inną metodą	Ręczne wprowadzenia informacji do S46 (w formie raportów, komunikatów lub ostrzeżeń)

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
15	Systemy źródłowe dla CTI	CTI MC	Dane dotyczące cyberzagrożeń	kopiowanie danych	realizowalny inną metodą	usługa REST

7.2. Kluczowe komponenty architektury rozwiązania



7.3. Przyjęte założenia technologiczne

Lp.	Obszar	Założenie technologiczne
1.	Infrastruktura	Rozwiązania będą wdrożone w infrastrukturze teleinformatycznej z zapewnieniem odpowiednich mechanizmów skalowalności, dostępności oraz bezpieczeństwa przetwarzanych danych.
2.	Sieć i bezpieczeństwo	Transmisja danych będzie realizowana z wykorzystaniem bezpiecznych protokołów komunikacyjnych oraz mechanizmów uwierzytelniania systemów i kontroli dostępu. Z uwzględnieniem

Lp.	Obszar	Założenie technologiczne
		ochrony infrastruktury sieci przez specjalizowane systemy i zapewnienia bezpieczeństwa mechanizmów chmurowych poprzez uwzględnienie mechanizmów zabezpieczeń dla kupowanych usług.
3.	Standardy wymiany danych	Komunikacja realizowana będzie z wykorzystaniem bezpiecznych usług sieciowych umożliwiających automatyczną wymianę danych Usługi: SOAP, REST, REST API, SSO (federacyjne), feedy danych Protokoły: HTTPS, SAML, SAML 2.0, OAuth2, OpenID Connect (OIDC), AS2, AS4, TLS, SFTP Formaty danych: XML, JSON, CSV
4.	Systemy operacyjne serwerowe	System oparty jest na serwerowych systemach operacyjnych z rodziny Linux, takich jak Red Hat Enterprise Linux, Ubuntu Server lub ich odpowiedniki. Wybór tej platformy wynika z wysokiej stabilności, bezpieczeństwa oraz szerokiego wsparcia dla rozwiązań klasy enterprise.
5.	Bazy danych	W systemie przewidziano wykorzystanie zarówno relacyjnych, jak i nierelacyjnych baz danych, co pozwala na optymalne dopasowanie technologii do charakteru przetwarzanych danych.
6.	Serwery aplikacji	Planowane systemy będą realizowane w architekturze aplikacji webowych, z dostępem poprzez przeglądarkę internetową dla uprawnionych użytkowników
7.	Portale	Dostęp do funkcjonalności systemów realizowany będzie poprzez interfejs webowy dostępny dla uprawnionych użytkowników
8.	Inne	

7.4. Opis zasobów danych przetwarzanych w planowanym rozwiązaniu

Czy nowy system będzie tworzył zasoby danych o charakterze rejestru publicznego?

TAK/NIE

Czy nowy system będzie przetwarzał (używał, zmieniał) zawartość innych rejestrów publicznych?

TAK/NIE

Lp.	Rejestr publiczny	Opis	Zakres przetwarzania
1	Wykaz Podmiotów Kluczowych i Podmiotów Ważnych	Wykaz Podmiotów Kluczowych i Podmiotów Ważnych prowadzony w systemie S46 odpowiada za samorejestrację podmiotów kluczowych i ważnych. Umożliwia podmiotom kluczowym i ważnym obsługę cyklu życia wpisu w Wykazie. W szczególności umożliwia: rejestrację, weryfikację statusu wpisu do Wykazu,	zmiana danych

Lp.	Rejestr publiczny	Opis	Zakres przetwarzania
		wskazanie osób właściwych do spraw cyberbezpieczeństwa, czy aktualizację danych dotyczących podmiotu. Ze strony organów właściwych możliwa jest obsługa wniosków o wpis oraz wpisywanie podmiotów kluczowych lub podmiotów ważnych do wykazu z urzędu przez ministra właściwego do spraw informatyzacji i organy właściwe do spraw cyberbezpieczeństwa, czy wykreślenie z Wykazy podmiotów KCS, jak również raportowanie.	
2	Baza Adresów Elektronicznych	BAE zawiera adresy do doręczeń elektronicznych powiązanych z publiczną usługą rejestrowanego doręczenia elektronicznego albo z kwalifikowaną usługą rejestrowanego doręczenia elektronicznego. Adresy te przydzielane są zgodnie z ustawą o doręczeniach elektronicznych, wszystkim podmiotom publicznym, podmiotom wpisanym do KRS oraz osobom fizycznym wykonującym określone zawody (np. adwokata, doradcy podatkowego) i prowadzącym działalność gospodarczą wpisaną do CEIDG oraz komornikom sądowym. Pozostałe osoby fizyczne mogą wystąpić o wpisanie adresu do doręczeń elektronicznych do bazy adresów elektronicznych, co jest równoznaczne z żądaniem doręczania korespondencji do nich przez podmioty publiczne na ten adres. BAE zawiera także dane podstawowe tych podmiotów i osób fizycznych oraz dane administratorów	użycie danych

Lp.	Rejestr publiczny	Opis	Zakres przetwarzania
		skrzynki doręczeń.	

7.5. Bezpieczeństwo

Planowany poziom zapewnienia bezpieczeństwa (w rozumieniu przepisów § 19 rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773)) w zakresie dot. systemu zarządzania bezpieczeństwem informacji:

- ~~-system nie podlega rygorom KRI – należy wyjaśnić czy istnieją inne normy bezpieczeństwa, które będą spełnione przez system zgodnie z wymogami KRI~~
- ~~-dodatkowe zabezpieczenia powyżej wymogów KRI: należy wskazać uzasadnienie~~