MINISTERSTWO OBRONY NARODOWEJ
SEKRETARZ STANU

#SZCZEPIMYSIĘ

Warszawa, dn. 9 listopada 2021 r.

MINISTERSTWO OBRONY NARODOWEJ
WYDZIAŁ KANCELARII JAWNYCH
Nr. 2061/NS
09 LIS. 2021

Pani Wioletta ZWARA

SEKRETARZ KOMITETU RADY MINISTRÓW DS. CYFRYZACJI

KANCELARIA PREZESA RADY MINISTRÓW
e-PUAP

Dotyczy: *projektu informatycznego CROID.*

Szanowna Pani,

w nawiązaniu do wcześniejszej korespondencji uprzejmie informuję, że w dołączonym opisie założeń projektu informatycznego CROID uwzględniono uwagi zgłoszone przez Ministerstwo Cyfryzacji oraz Ministerstwo Funduszy i Polityki Regionalnej.
Jednocześnie proszę o przyjęcie wyjaśnień Rektora-Komendanta Akademii Marynarki Wojennej odnoszących się do uwagi Ministerstwa Finansów dotyczącej konieczności przeprowadzenia konsultacji projektu ze stroną samorządową, tj. Komisją Wspólną Rządu i Samorządu Terytorialnego (KWRiST).
W myśl zapisów ustawy z dnia 6 maja 2005 roku o Komisji Wspólnej Rządu i Samorządu Terytorialnego oraz o przedstawicielach Rzeczypospolitej Polskiej w Komitecie Regionów Unii Europejskiej (Dz.U. Nr 90, poz. 759) przedmiotowy projekt nie stanowi projektu aktu normatywnego ani programu, czy dokumentu rządowego dotyczącego problematyki samorządu terytorialnego, nie powoduje również skutków finansowych dla samorządu terytorialnego. Dlatego też nie ma konieczności przeprowadzenia konsultacji projektu ze stroną samorządową KWRiST.
Jest to projekt szkoleniowy dedykowany dla ekspertów, podnoszący świadomość kierownictwa jednostek samorządu terytorialnego oraz podnoszący wiedzę i umiejętności w zakresie cyberbezpieczeństwa. Przedmiotowy projekt to realizacja Strategii Cyberbezpieczeństwa, a dokładnie zapisu z celu nr 4 - Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa, która była wcześniej konsultowana z KWRiST.

Załącznik: 1 na 16 str. – Opis Założeń Projektu Informatycznego_CROIOD.pdf

Z poważaniem
Wojciech Skurkiewicz
Wojciech SKURKIEWICZ

Wyk. Beata Jałtuszyk, tel. 261-846-832
2021-11-08
T. 007

OPIS ZAŁOŻEŃ PROJEKTU INFORMATYCZNEGO

Tytuł projektu	Obsługa CyberIncydentu CROIOD (Cyber-Ratownik, Obsługa Incydentu i Odtwarzanie Działania)		
Wnioskodawca	Minister Obrony Narodowej		
Beneficjent	Akademia Marynarki Wojennej w Gdyni		
Partnerzy			
Źródło finansowania	REACT-EU - Program Operacyjny Polska Cyfrowa, Oś priorytetowa V „Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU"		
Całkowity koszt projektu	19 313 301,00 zł		
Planowany okres realizacji projektu	12-2021 do 06-2023		
Osoba kontaktowa	Jerzy Kosiński	j.kosinski@amw.gdynia.pl	533223993

1. POWODY PODJĘCIA PROJEKTU

1.1. Identyfikacja problemu i potrzeb

Od 2019 roku można zaobserwować znaczący wzrost infekcji ransomware w sektorze medycznym oraz administracji państwowej i samorządowej. Z roku na rok widać też wyraźmy wzrost wartości okupów żądanych przez przestępców. Wg danych firmy Palo Alto o ponad 170 proc. wzrosła średnia wartość okupu, którą zapłacili w 2020 r. ofiary cyberprzestępców (z 115 tys. USD w 2019 r. do 312 tys. USD w 2020 r.). Wzrastają także kwoty największych okupów - w porównaniu do 2019 r. wartość ta podwoiła się (z 5 mln USD do 10 mln USD). W 2020 r. odnotowano także największy – upubliczniony – jednorazowy zapłacony okup (30 mln USD). Zmienia się także model biznesowy przestępców - coraz częściej domagają się okupu nie tylko za odszyfrowanie danych, ale także za ich nieujawnianie, niekiedy dodatkowo "motywują" swoje ofiary przeprowadzanymi atakami DDoS lub też wykorzystują klientów swoich ofiar do wywierania presji na zaatakowanego przedsiębiorcę.
Cyberprzestepcy coraz częściej atakują przy pomocy ransomware jednostki samorządu terytorialnego oraz placówki ochrony zdrowia. Wystarczy wspomnieć o m.in. o fali skoordynowanych ataków na szpitale w Rumunii w 2019 r., we Francji w 2021 r. Kluczowe są coraz liczniejsze przykłady z Polski. Na początku 2020 r. szpital w Białymstoku został zaatakowany przy pomocy złośliwego oprogramowania typu ransomware. Podobny atak miał miejsce, m.in. na Klinikę Budzik, czy szpital wojewódzki w Skierniewicach (2021 r.).
Celem projektu jest utworzenie systemowego rozwiązania mającego na celu wsparcie podmiotów , w tym JST, w zakresie obsługi incydentu (incident handling) oraz odzyskiwania danych, sprawności systemu po ataku (recovery). Jest to zatem działanie ex post – po wystąpieniu incydentu. Ta część procesu obsługi incydentów , szczególnie recovery, jest krytyczna w kontekście działania danego urzędu, np. realizacji świadczeń społecznych, czy zbierania podatków. Projekt nie przewiduje powstania aktywnych systemów IT chroniących przed incydentami.

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
Instytucje	a. brak osób w instytucjach samorządowych,	min.200 osób -

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
samorządowe	które miałyby doświadczenie w reagowaniu na cyberincydenty, b. niewystarczające wsparcie instytucjonalne dla administratorów zaatakowanych systemów c. brak wsparcia sprzętowego w procesie powstrzymania oraz likwidacji skutków incydentu (16 województw+Warszawa+ 1 laboratorium wyposażone w 2 zestawy) d. brak wsparcia sprzętowego i programowego w przywracaniu organizacji do dalszego działania (16 województw +Warszawa+ 1 laboratorium wyposażone w 2 zestawy) e. niewystarczająca wiedza w zakresie możliwości ograniczania prawdopodobieństwa i skutków ataków typu ransomware	przedstawicieli służb IT z instytucji samorządowych (20 szkoleń x 10 os.) min.600 osób - kampania prewencyjna skierowana do prezydentów miast, burmistrzów, wójtów i sekretarzy oraz osób od IT
Policja	a. brak wiedzy o prawidłowej reakcji na uzyskaną informacje o zaistnieniu cyberincydentu b. brak wsparcia sprzętowego i programowego w procesie powstrzymania oraz likwidacji skutków incydentu realizowanego przez Wydziały dw. z cyberprzestępczością (17) c. brak wiedzy w zakresie gromadzenia oraz zabezpieczania śladów elektronicznych	min.600 osób – służb dyżurnych i wydziałów dw. z cyberprzestępczością

1.2. Opis stanu obecnego

Cyberataki mogą mieć różny charakter i skutki, począwszy od trywialnych oszustw na kilkadziesiąt złotych, po tragiczne, powodujące śmierć ludzi ataki ransomware na szpitale i placówki opieki medycznej. CSIRT NASK zarejestrował w 2020 r. 10 420 incydentów cyberbezpieczeństwa. Jest to zdecydowany wzrost liczby incydentów w stosunku do roku 2019 – aż o 61 proc. Na przestrzeni ostatnich 3 lat doszło w Polsce do wielu ataków typu ransomware na urzędy administracji publicznej m.in. w Kościerzynie, Lututowie, Małopolskim Urzędzie Marszałkowskim w Krakowie. Ataki te doprowadziły do paraliżu tych urzędów. Zmienia się także model biznesowy przestępców - coraz częściej domagają się okupu nie tylko za odszyfrowanie danych, ale także za ich nieujawnianie. W ten sposób podmiotom, które utraciły w ten sposób kontrolne nad przechowywanymi informacjami, w tym danymi osobowymi, grożą konsekwencje wynikające z niedopełnienia obowiązków z RODO.
Niestety zaatakowani, w większości przypadków, nie są przygotowani do odpowiedniej reakcji na wykryte zagrożenia bezpieczeństwa systemu IT.
W większości sytuacji, podstawową reakcją na zaistniałe zagrożenie jest próba odtworzenia środowiska systemu IT. Wykonywana nieumiejętnie prowadzi ona jednak często do trwałego zniszczenia istniejących śladów, których analiza mogłaby doprowadzić do powstrzymania oraz likwidacji skutków incydentu, a także przywrócenia organizacji do dalszego działania. Takie działanie w większości przypadków nie jest skuteczne.

Zaatakowane organizacje, ale także organa ścigania, nie dysponują narzędziami (hardware i software) oraz procedurami umożliwiającymi pozyskanie i zabezpieczenie niezbędnych do analizy danych - posiłkują się wsparciem udzielanym bezpłatnie lub komercyjnie przez firmy prywatne.
Sytuację dodatkowo komplikują procedury finansowo-księgowe, które znacznie utrudniają i opóźniają zarówno możliwość skorzystania ze wsparcia zewnętrznych ekspertów.

2. EFEKTY PROJEKTU

2.1. Cele i korzysci wynikające z projektu

Cel - 1	Stworzenie środowiska edukacyjnego reakcji na cyberincydent, w szczególności na zagrożenia ransomware
Cel strategiczny	Przedmiotowy projekt wpisuje się w: 1. Cele Programu Zintegrowanej Informatyzacji Państwa (PZIP) w odniesieniu do celu 4.2.2. Wzmocnienie dojrzałości organizacyjnej jednostek administracji publicznej oraz usprawnienie zaplecza elektronicznej administracji (back office) oraz 4.2.3. Podniesienie poziomu kompetencji cyfrowych obywateli, specjalistów TIK oraz pracowników administracji publicznej 2. Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, w szczególności celu szczegółowego nr 2 - Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty 3. Cele Programu Operacyjnego Polska Cyfrowa - Oś priorytetowa V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU.
Korzyść:	Wsparcie administracji samorządowej w odpowiedniej reakcji na cyberincydent, w szczególności na zagrożenia typu ransomware, m.in. za pomocą laboratorium szkoleniowego, portal wiedzy i portalu wspomagania obsługi incydentu Zwiększenie zaufania do usług zarządzanych i udostępnianych przez administrację samorządową. Poprawa jakości i niezawodności cyfrowych usług publicznych. Obniżenie kosztów związanych z występowaniem i obsługą incydentów naruszenia cyberbezpieczeństwa zarówno w odniesieniu do klienta indywidualnego, jak i podmiotów administracji samorządowej. Podniesienie poziomu cyberbezpieczeństwa poprzez promocję najlepszych praktyk.
KPI:	1. Liczba utworzonych laboratoriów szkoleniowych, z portalem wiedzy i wspomagania obsługi incydentu 2. Wartość sprzętu IT oraz oprogramowania/licencji finansowanych w odpowiedzi na COVID-19 - inne obszary 3. Wartość sprzętu IT oraz oprogramowania/licencji finansowanych w odpowiedzi na COVID-19 (CV 4) 4. Wartość wydatków kwalifikowalnych przeznaczonych na działania związane z pandemią COVID-19
Wartość aktualna i docelowa KPI:	KPI nr 1: 0 KPI nr 2: 0 KPI nr 3: 0 KPI nr 4: 0 KPI nr 1: 1

	KPI nr 2: 2 242 740,00 zł KPI nr 3: 2 242 740,00 zł KPI nr 4: 2 242 740,00 zł
Metoda pomiaru KPI	Metoda pomiaru KPI nr 1: dokumentacja odbioru laboratorium, protokół walidacji; jednokrotny Metoda pomiaru KPI nr 2,3,4: faktury zakupu; jednokrotny
Cel - 2	Przeszkolenie osób odpowiedzialnych za reakcję na cyberincydent, w szczególności zagrożenia typu ransomware
Cel strategiczny	1. Cele Programu Zintegrowanej Informatyzacji Państwa (PZIP) w odniesieniu do celu 4.2.2. Wzmocnienie dojrzałości organizacyjnej jednostek administracji publicznej oraz usprawnienie zaplecza elektronicznej administracji (back office) oraz 4.2.3. Podniesienie poziomu kompetencji cyfrowych obywateli, specjalistów TIK oraz pracowników administracji publicznej 2. Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, w szczególności celu szczegółowego nr 2 - Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty 3. Cele Programu Operacyjnego Polska Cyfrowa - Oś priorytetowa V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU.
Korzyść:	Wsparcie administracji samorządowej w odpowiedniej reakcji na cyberincydent, w szczególności na zagrożenia typu ransomware. Zwiększenie zaufania do usług zarządzanych i udostępnianych przez administrację samorządową. Poprawa jakości i niezawodności cyfrowych usług publicznych. Obniżenie kosztów związanych z występowaniem i obsługą incydentów naruszenia cyberbezpieczeństwa zarówno w odniesieniu do klienta indywidualnego, jak i podmiotów administracji samorządowej. Podniesienie poziomu cyberbezpieczeństwa poprzez promocję najlepszych praktyk.
KPI:	1. Liczba pracowników objętych szkoleniami w zakresie umiejętności cyfrowych 2. Liczba przeszkolonych przedstawicieli służb IT odbiorców projektu 3. Liczba przeszkolonych osób decyzyjnych odbiorców projektu 4. Liczba przeszkolonych funkcjonariuszy służb dyżurnych i wydziałów dw. z cyberprzestępczością Policji 5. Liczba pracowników objętych szkoleniami w zakresie umiejętności cyfrowych - kobiety 6. Liczba pracowników objętych szkoleniami w zakresie umiejętności cyfrowych - mężczyźni 7. Liczba osób objętych wsparciem w zakresie zwalczania lub przeciwdziałania skutkom pandemii COVID-19
Wartość aktualna i docelowa KPI:	KPI nr 1: wartość bazowa 0 KPI nr 2: wartość bazowa 0 KPI nr 3: wartość bazowa 0 KPI nr 4: wartość bazowa 0 KPI nr 5: wartość bazowa 0 KPI nr 6: wartość bazowa 0 KPI nr 7: wartość bazowa 0 KPI nr 1: min.1400 osób KPI nr 2: min.200 osób (20 szkoleń x 10 os.)

	KPI nr 3: min.600 osób KPI nr 4.: min.600 osób KPI nr 5.: min.140 osób KPI nr 6.: min.1260 osób KPI nr 7: min.1400 osób
Metoda pomiaru KPI	Metoda pomiaru KPI nr 1,5,6,7: dokumentacja szkoleniowa (m.in. materiały szkoleniowe, listy obecności, ocena szkolenia, wyniki testów wiedzy i umiejętności po szkoleniu); 36 pomiarów Metoda pomiaru KPI nr 2: dokumentacja szkoleniowa (m.in. materiały szkoleniowe, listy obecności, wyniki testów wiedzy i umiejętności po szkoleniu); 20 pomiarów Metoda pomiaru KPI nr 3, 4: dokumentacja szkoleniowa (m.in. materiały szkoleniowe, listy obecności, ocena szkolenia); min.16 pomiarów
Cel - 3	Wsparcie sprzętowo-programowe odpowiedniej reakcji na cyberincydent, w szczególności zagrożenia typu ransomware
Cel strategiczny	1. Cele Programu Zintegrowanej Informatyzacji Państwa (PZIP) w odniesieniu do celu 4.2.2. Wzmocnienie dojrzałości organizacyjnej jednostek administracji publicznej oraz usprawnienie zaplecza elektronicznej administracji (back office) oraz 4.2.3. Podniesienie poziomu kompetencji cyfrowych obywateli, specjalistów TIK oraz pracowników administracji publicznej 2. Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, w szczególności celu szczegółowego nr 2 - Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty 3. Cele Programu Operacyjnego Polska Cyfrowa - Oś priorytetowa V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU.
Korzyść:	Wsparcie administracji samorządowej w odpowiedniej reakcji na cyberincydent, w szczególności na zagrożenia typu ransomware. Zwiększenie zaufania do usług zarządzanych i udostępnianych przez administrację samorządową. Poprawa jakości i niezawodności cyfrowych usług publicznych. Obniżenie kosztów związanych z występowaniem i obsługą incydentów naruszenia cyberbezpieczeństwa zarówno w odniesieniu do klienta indywidualnego, jak i podmiotów administracji samorządowej. Podniesienie poziomu cyberbezpieczeństwa poprzez promocję najlepszych praktyk.
KPI:	1. Liczba JST, które zwiększyły swój potencjał cyfrowy (Liczba wyposażonych środowisk do zabezpieczania i odtwarzania danych) 2. Liczba wyposażonych we wsparcie sprzętowe i programowe jednostek Policji gotowych do realizacji procesów powstrzymania oraz likwidacji skutków incydentu 3. Liczba podmiotów objętych wsparciem w zakresie zwalczania lub przeciwdziałania skutkom pandemii COVID-19 4. Wartość sprzętu IT oraz oprogramowania/licencji finansowanych w odpowiedzi na COVID-19 - inne obszary 5. Wartość sprzętu IT oraz oprogramowania/licencji finansowanych w odpowiedzi na COVID-19 (CV 4) 6. Wartość wydatków kwalifikowalnych przeznaczonych na działania związane z pandemią COVID-19 7. Liczba wdrożonych systemów IT w obszarze cyberbezpieczeństwa

Wartość aktualna i docelowa KPI:	KPI nr 1: 0 KPI nr 2: 0 KPI nr 3: 0 KPI nr 4: 0 KPI nr 5: 0 KPI nr 6: 0 KPI nr 7: 0 KPI nr 1: 18 KPI nr 2: 17 KPI nr 3: 35 KPI nr 4: 10 771 760,00 zł KPI nr 5: 10 771 760,00 zł KPI nr 6: 16 261 441,00 zł KPI nr 7: 2
Metoda pomiaru KPI	Metoda pomiaru KPI nr 1: dokumentacja odbioru; 18 odbiorów (16 UMarsz. + UM Warszawa + laboratorium) Metoda pomiaru KPI nr 2: dokumentacja odbioru; 17 odbiorów (16 KWP+KSP) Metoda pomiaru KPI nr 3: dokumentacja odbioru; 35 odbiorów (18 z KPI nr1 i 17 z KPI nr2) Metoda pomiaru KPI nr 4,5,6: faktury zakupu; jednokrotny Metoda pomiaru KPI nr 7: dokumentacja odbioru systemów; jednokrotny

2.2. Udostępnione e-usługi

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

2.3. Udostępnione informacje sektora publicznego i zdigitalizowane zasoby

Nie dotyczy

2.4. Produkty końcowe projektu

Nazwa produktu	Planowana data wdrożenia
Metodyka reagowania (zabezpieczania) na cyberincydenty typu ransomware	01-2022
Metodyka odtwarzania danych w przypadku ataku typu ransomware	01-2022
Materiały szkoleniowe dla służb IT odbiorców projektu	01-2022
Laboratorium szkoleniowe	02-2022
Wyposażenie 19 środowisk do zabezpieczania danych w 18 lokalizacjach	03-2022
Wyposażenie 19 środowisk do odtwarzania danych w 18 lokalizacjach	03-2022
Wyposażenie 17 Wydziałów dw. z cyberprzestępczością Policji w „apteczki”	04-2022

Nazwa produktu	Planowana data wdrożenia
Materiały szkoleniowe dla osób decyzyjnych odbiorców projektu	06-2022
Portal Wiedzy	12-2022
Portal Wspomagania Obsługi Incydentu	12-2022
Filmy szkoleniowe	12-2022
Koncepcja chmurowego wsparcia odtworzenia	06-2023
Koncepcja przedłużenia i rozwoju usług dla odbiorców projektu na lata 2024-2026	06-2023
Podręcznik w zakresie ochrony jednostek administracji samorządowej przed atakami typu ransomware, materiały promocyjne	06-2023

3. KAMIENIE MILOWE

Kamienie milowe	Planowany termin osiągnięcia
Opracowana koncepcja systemu i szkoleń	2021-12-31
Rozstrzygnięcie postępowania przetargowego na środowisko reakcyjne i odtworzeniowe dla urzędów marszałkowskich	2022-01-31
Odebrane pracownia i środowisko szkoleniowe	2022-03-31
Skompletowane środowiska reakcyjne i odtworzeniowe	2022-03-31
Odebrany raport ewaluacyjny programów szkolenia, scenariuszy	2022-03-31
Uruchomione Portal wiedzy i Portal wspomagania obsługi incydentów	2022-12-01
Przekazane środowiska odtworzeniowe dla urzędów marszałkowskich	2022-12-01
Odebrany raport ewaluacyjny środowiska szkoleniowego	2023-06-30

4. KOSZTY

4.1. Koszty ogólne projektu wraz ze sposobem finansowania

Całkowity koszt projektu (netto oraz brutto), w tym	Netto 15 701 870,73 zł Brutto 19 313 301,00 zł	
Procent dofinansowania ze środków UE (brutto)	100%	
Procent środków z budżetu państwa (brutto)	0%	
Podział całkowitego kosztu projektu na poszczególna lata (netto oraz brutto)	2021	Netto 69 333,33 zł Brutto 85 280,00 zł
	2022	Netto 7 246 732,52 zł Brutto 8 913 481,00 zł
	2023	Netto 8 385 804,88 zł Brutto 10 314 540,00 zł

4.2. Wykaz poszczególnych pozycji kosztowych

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
Oprogramowanie	Oprogramowanie	3 877 720,00 zł	Utworzenie środowisk zabezpieczania i odtwarzania oraz apteczki wymaga wykorzystania niezbędnego oprogramowania. Do opracowania i eksploatacji portali wiedzy i obsługi incydentów niezbędny będzie zakup oprogramowania.
Infrastruktura	Sprzęt, wyposażenie	9 514 296,00 zł	Obejmuje utworzenie środowiska edukacyjnego oraz środowisk reakcyjno/odtworzeniowych. W pozycji ujęto koszty: „Bezpieczeństwo" i „Wydajność rozwiązań", które są elementami integralnie związanymi z realizowanymi działaniami w projekcie, a nie dokładanymi do nich – nie można zatem ich wyszczególnić".
Koszty UX i grafiki	badanie wymagań użytkowników projektowanych portali	200 000,00 zł	Opracowanie funkcjonalnych i ergonomicznych portali wymaga zbadania UX i opracowania odpowiedniej grafiki
Bezpieczeństwo			
Wydajność rozwiązań			

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
Szkolenia	przygotowanie i realizacja szkoleń	5 112 165,00 zł	Obejmuje ogólny koszt szkoleń (wraz z przygotowaniem, wyposażeniem, ewaluacją) zarówno ekspertów (5 078 795 zł, jak i szkoleń prewencyjnych (33 370 zł)
Działania informacyjno-promocyjne	Opracowanie i przekazanie informacji o produktach projektu	60 000,00 zł	Informacja o produktach projektu musi być rozpowszechniona szerzej, niż tylko wśród bezpośrednich interesariuszy projektu
Koszty zarządzania i wsparcia (w tym wynagrodzenia personelu wspomagającego)	Koszt zarządzanie projektem (1/2 etatu) i obsługi (1/2 etatu)	549 120,00 zł	Tak duży projekt wymaga profesjonalnego zarządzania i wsparcia w obsłudze

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

Całkowity koszt utrzymania trwałości projektu (brutto)	7 045 613,00 zł		Źródło finansowania
Podział całkowitego kosztu utrzymania trwałości projektu na poszczególna lata (netto oraz brutto)	2023	200 000,00 zł (brutto) (162 601,63 zł netto)	krajowe środki publiczne - budżet państwa
	2024	1 857 761,00 zł (brutto) (1 510 374,80 zł netto)	krajowe środki publiczne - budżet państwa
	2025	794 245,00 zł (brutto) (645 727,64 zł netto)	krajowe środki publiczne - budżet państwa
	2026	1 699 681,00 zł (brutto) (1 381 854,47 zł netto)	krajowe środki publiczne - budżet państwa
	2027	794 245,00 zł (brutto) (645 727,64 zł netto)	krajowe środki publiczne - budżet państwa
	2028	1 699 681,00 zł (brutto) (1 381 854,47 zł netto)	krajowe środki publiczne - budżet państwa

4.4. Planowane koszty ogólne realizacji (w przypadku projektu

współfinansowanego – wkład krajowy z budżetu państwa) oraz koszty utrzymania projektu:

- 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 projektu

Nazwa ryzyka	Siła oddziaływania	Prawdopo-dobieństwo wystąpienia ryzyka	Sposób zarzadzania ryzykiem
Ryzyko zewnętrzne związane ze zmianą uwarunkowań prawnych	Duża	Niskie	1. bieżący monitoring i analizę zmian prawnych 2. podjęcie działań zmierzających do dostosowania do nowych regulacji pod względem organizacyjno-technicznym 3. udział w opracowywaniu zmian prawnych na wczesnym etapie ich określania
Ryzyko zewnętrzne związane z ograniczeniami wynikającymi z pandemii COVID-19	Duża	Średnie	1. dostosowanie trybu realizacji prac do obowiązujących obostrzeń epidemicznych
Ryzyko związane z pozyskaniem ekspertów	Duża	Niskie	1. zaoferowanie rynkowych wynagrodzeń dla ekspertów realizujących projekt
Ryzyko związane z niewykonaniem zadań	Duża	Niskie	1. bieżąca weryfikacja realizacji zadań i okresowe odbiory wyników w ramach zarządzania projektem 2. integracja zespołów realizujących projekt do wspólnego rozwiązywania pojawiających się problemów 3. ścisła współpraca z JST i Policją w zakresie rekrutacji uczestników
Ryzyko związane z przedłużającymi się procedurami zakupowymi, które uniemożliwią realizację zadań	Duża	Niskie	1. przygotowanie dokumentacji zakupowej przez osoby posiadające doświadczenie w zakresie zamówień publicznych
Ryzyko związane z niedoszacowaniem	Duża	Niskie	1. oszacowanie budżetu z należytą starannością

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarzadzania ryzykiem
budżetu projektu			2. bieżący monitoring harmonogramu zaplanowanych wydatków oraz całkowitych kosztów projektu 3. podejmowanie działań ad hoc mających na celu redukowanie ryzyka
Ryzyko związane z niedotrzymaniem terminowości realizacji projektu	Duża	Niskie	1. wdrożenie i wykorzystywanie metod zarządzania projektem. 2. bieżące monitorowanie harmonogramu realizacji projektu, w tym jego postępu, uwzględniające opracowanie i wdrożenie planu naprawczego
Ryzyko związane z nieprawidłową komunikacją w ramach zespołu realizującego projekt	Duża	Niskie	1. opracowanie i wdrożenie strategii i planów komunikacji 2. utworzenie repozytorium, w którym będą składowane dokumenty projektowe
Ryzyko związane z niską przydatnością praktyczną opracowanych rozwiązań	Duża	Niskie	1. bieżąca weryfikacja założeń technicznych opracowywanych rozwiązań
Ryzyko związane z brakiem pełnej wiedzy o proponowanych rozwiązaniach	Duża	Niskie	1. analiza i identyfikacja możliwych problemów i wymagań biznesowych 2. wdrożenie odpowiednich procedur
Ryzyko związane z dużą rotacją kadr po stronie administracji samorządowej	Duża	Średnie	1. ścisła współpraca z JST w zakresie doboru uczestników szkoleń 2. budowa portalu wiedzy i portalu wspomagania obsługi incydentu 3. egzekwowanie opracowanych procedur

5.2. Ryzyka wpływające na utrzymanie efektów

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarzadzania ryzykiem
Ryzyko związane ze zmianą	Duża	Niskie	1. bieżąca analiza zmian prawnych 2. podjęcie działań dostosowujących

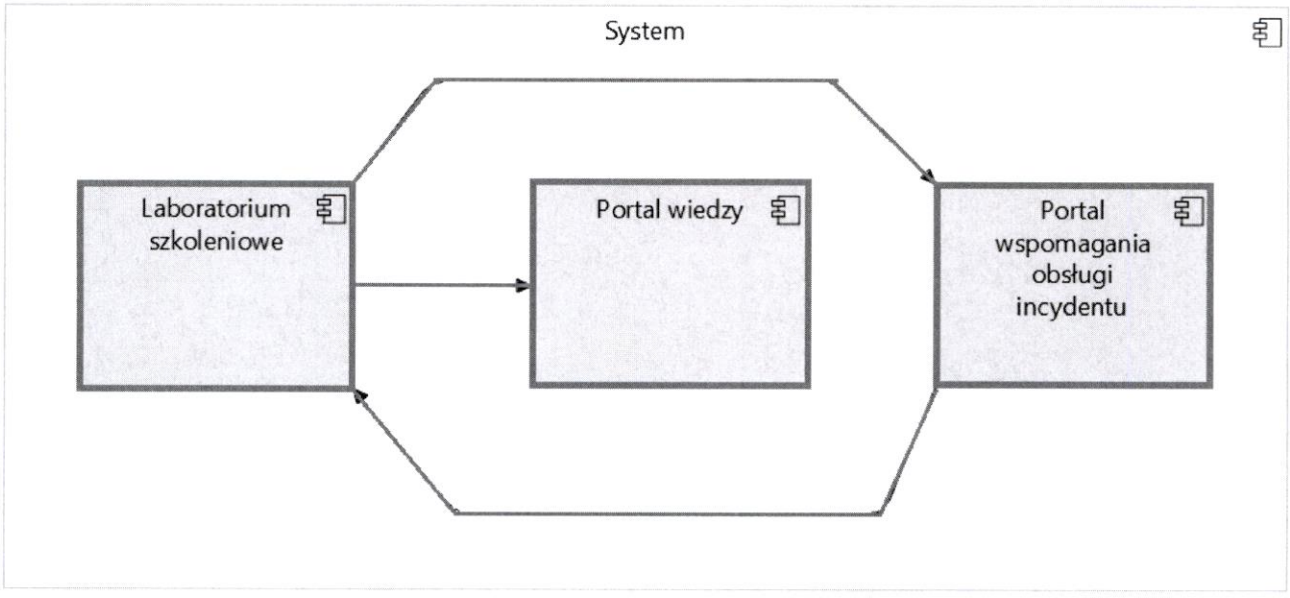
Nazwa ryzyka	Siła oddziaływania	Prawdopo-dobieństwo wystąpienia ryzyka	Sposób zarzadzania ryzykiem
przepisów			efekty do nowych uwarunkowań prawnych
Ryzyko związane ze starzeniem się rozwiązań zastosowanych w projekcie	Duża	Średnie	1. zastosowanie najnowszych technologii na etapie opracowywania projektu 2. wykorzystanie rozwiązań generycznych
Ryzyko związane z dużą rotacją kadr po stronie samorządów lokalnych	Duża	Średnie	1. stworzenie portali oraz podręczników pozwoli na minimalizację skutków dużej rotacji kadr 2. monitorowanie wykorzystania przez JST przeszkolonych w ramach projektu kadr

6. OTOCZENIE PRAWNE

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
1	Ustawa o krajowym systemie cyberbezpieczeństwa	~~TAK~~/NIE		
2	Rozporządzenie o Krajowych Ramach Interoperacyjności	~~TAK~~/NIE		

7. ARCHITEKTURA

7.1. Widok kooperacji aplikacji



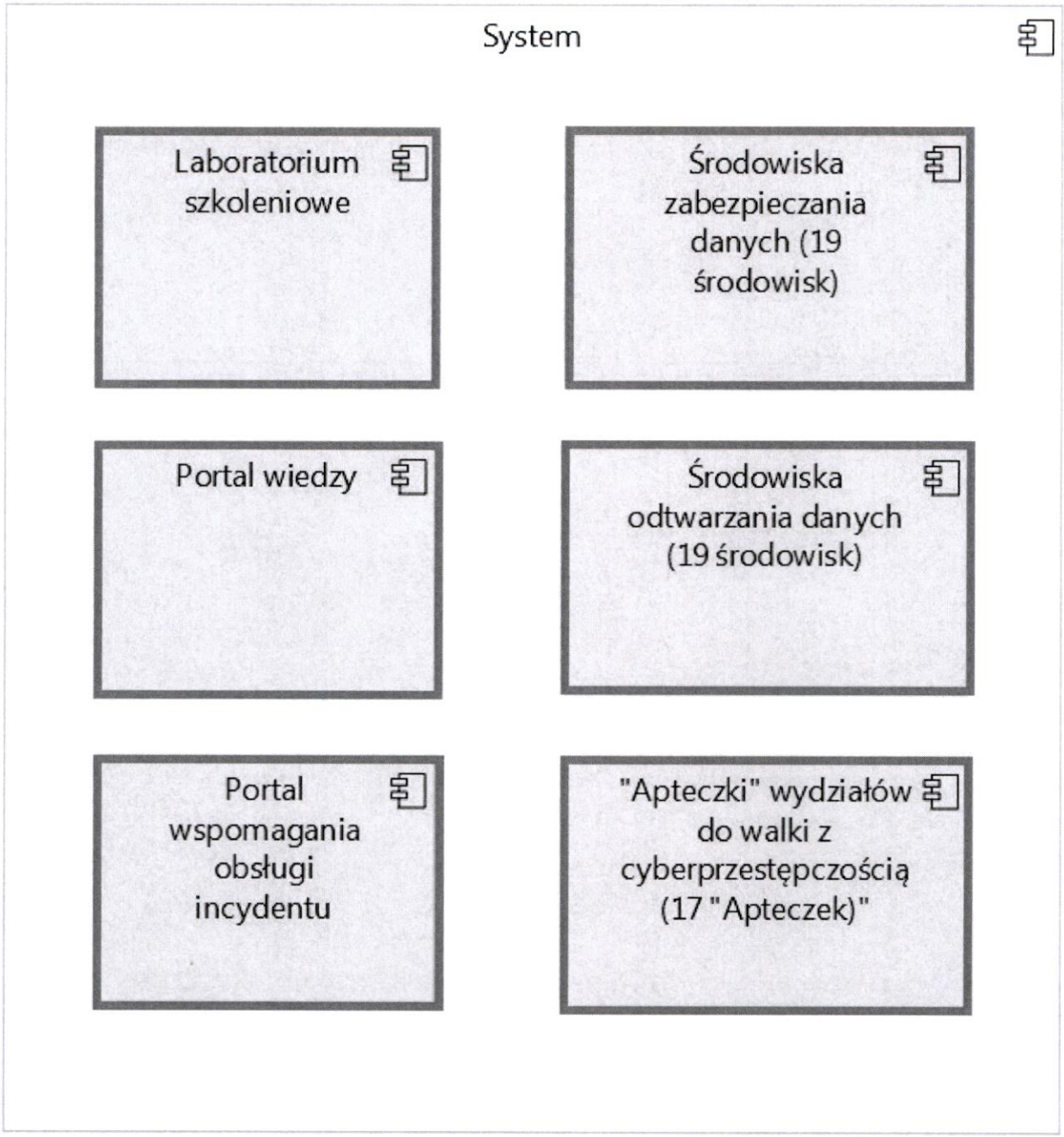
Lista systemów wykorzystywanych w projekcie

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
1	Laboratorium szkoleniowe	AMW	Środowisko edukacyjne w zakresie technicznego reagowania na cyberincydenty.	Planowany	
2	Portal wiedzy	AMW	Miejsce, zawierające materiały metodyczne wspierające odbiorców projektu we właściwej prewencji, reakcji oraz odtwarzaniu. System jest hermetyczny i nie wpływa na AIP.	Planowany	
3	Portal wspomagania obsługi incydentu	AMW	Miejsce, które będzie wspierać „first responders", administratorów IT, w reagowaniu na cyberincydenty. Umożliwi zgłaszanie incydentu i uzyskanie szybkiego wsparcia prawno-proceduralnego oraz technicznego. System jest hermetyczny i nie wpływa na AIP.	Planowany	

Lista przepływów

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
1	Laboratorium szkoleniowe	Portal wiedzy	Wiedza o incydentach (prewencja, reakcja oraz odtwarzanie)	Odwołania bezpośrednie lub kopiowanie danych	Aktualizacja z wykorzystaniem protokołów komunikacyjnych i szyfrujących	Elektronicznie w formacie zgodnym z zał.2 i 4 KRI, struktura zostanie zostanie opracowana w ramach projektu
2	Laboratorium szkoleniowe	Portal wspomagania obsługi incydentu	Metodyki, procedury	Odwołania bezpośrednie lub kopiowanie danych	Aktualizacja z wykorzystaniem protokołów komunikacyjnych i szyfrujących	Elektronicznie w formacie zgodnym z zał.2 i 4 KRI, struktura zostanie zostanie opracowana w ramach projektu
3	Portal wspomagania obsługi incydentu	Portal wspomagania obsługi incydentu	Wiedza o zaistniałych incydentach i ich obsłudze	Odwołania bezpośrednie lub kopiowanie danych	Aktualizacja z wykorzystaniem protokołów komunikacyjnych i szyfrujących	Elektronicznie w formacie zgodnym z zał.2 i 4 KRI, , struktura zostanie zostanie opracowana w ramach projektu

7.2. Kluczowe komponenty architektury rozwiązania



7.3. Przyjęte założenia technologiczne

Lp.	Obszar	Założenie technologiczne
1.	Infrastruktura	
2.	Sieć i bezpieczeństwo	
3.	Standardy wymiany danych	
4.	Systemy operacyjne serwerowe	
5.	Bazy danych	
6.	Serwery aplikacji	

Lp.	Obszar	Założenie technologiczne
7.	Portale	
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

7.5. Bezpieczeństwo

Planowany poziom zapewnienia bezpieczeństwa (w rozumieniu przepisów §20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności [...] (Dz. U. 2012, poz. 526 z późn. zm.) 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

ISO/IEC 27001, ISO/IEC 27037, ISO/IEC 27043

~~- dodatkowe zabezpieczenia powyżej wymogów KRI: należy wskazać uzasadnienie~~