OPIS ZAŁOŻEŃ PROJEKTU INFORMATYCZNEGO

|  |  |  |  |
| --- | --- | --- | --- |
| Tytuł projektu | Centrum Reputacyjne Komunikacji Elektronicznej (CRKE) | | |
| Wnioskodawca | Minister Cyfryzacji | | |
| Beneficjent | Urząd Komunikacji Elektronicznej | | |
| Partnerzy | Nie dotyczy | | |
| Źródło finansowania | 84,63% dofinansowanie UE (II oś POPC E-administracja i otwarty rząd; Działanie 2.1 Wysoka dostępność i jakość usług publicznych); 15,37% dofinansowanie z budżetu Państwa - część budżetowa nr 76 (dysponent: Prezes UKE). | | |
| Całkowity koszt projektu | Netto 22 007 821,14 zł Brutto 27 069 620,00 zł | | |
| Planowany okres realizacji projektu | 07-2021 do 06-2023 | | |
| Osoba kontaktowa | Daniel  Kraszewski | Daniel.Kraszewski@uke.gov. pl | 532540226 |

1. POWODY PODJĘCIA PROJEKTU

1.1. Identyfikacja problemu i potrzeb

CRKE stanowi odpowiedź na potrzebę wzmocnienia kompetencji i podniesienia jakości, dostępności i bezpieczeństwa usług dostarczanych przez Przedsiębiorców Telekomunikacyjnych (PT) oraz formalnej współpracy z innymi podmiotami. CRKE będzie wspierać procesy oraz wzmocni kompetencje pozwalające na identyfikacje zdarzeń lub incydentów, wpływających na reputację komunikacji elektronicznej, a w efekcie na konsumenta. Dzięki analizie „post-mortem”, będzie możliwość potwierdzenia incydentu zgłoszonego przez Klienta, a w przypadku braku zgłoszenia, Prezes UKE będzie mógł przekazać i/lub wydać rekomendacje.

Bazując na badaniu świadomości zagrożenia incydentami w sieci pracowników polskich firm oraz urzędów przeprowadzonych w 2020 r.[[1]](#footnote-2), wynika, że 46% ankietowanych potwierdza, iż ich pracodawca zetknął się z incydentami w zakresie bezpieczeństwa sieci (wynik o 6% wyższy niż w badaniu z 2019 r.). Jednocześnie również 46% respondentów wskazało, że ich pracodawca nie zatrudnia specjalisty w zakresie bezpieczeństwa sieci. Dodatkowo aż 78% ankietowanych potwierdza, że wykorzystuje służbowy sprzęt do celów prywatnych. Aż 65% respondentów przyznaje, że ma trudności z określeniem zakresu naruszeń bezpieczeństwa, ograniczaniem ich wpływu, a także zapobieganiem im w przyszłości. Powyższe ilustruje jak ważne jest budowanie świadomości, bazy wiedzy i wymiany dobrych praktyk w zakresie zachowania bezpieczeństwa w celu redukcji potencjalnych incydentów w sieci.

CRKE będzie działać w oparciu o koncepcje sektorowego Information Sharing and Analysis Center (ISAC) i pozwoli na udostępnienie narzędzi do budowy kompetencji i dzielenie się wiedzą z PT, umożliwi współpracę PT z CSIRT poziomu krajowego, w zakresie wymiany informacji. Będzie ona realizowana z wykorzystaniem systemów teleinformatycznych, w oparciu o zasady ustalone w przepisach Ustawy o Krajowym Systemie Cyberbezpieczeństwa (Ustawa KSC).

PT to przedsiębiorstwa na różnym poziomie dojrzałości, a incydenty teleinformatyczne rzadko dotyczą tylko jednej instytucji. Współpraca i właściwa, dobrowolna wymiana wiedzy powinna znacznie podnieść poziom bezpieczeństwa usług i minimalizować wpływ niekorzystnego oddziaływania na konsumenta.

CRKE stanowi odpowiedź na potrzebę dostępu do wiedzy, standardów oraz bieżących informacji od podmiotów w innych sektorach gospodarki. Poprzez interakcje podmioty obszaru Telco, a w szczególności PT z sektora MŚP, zyskają większą świadomość na temat ryzyka, zagrożeń i incydentów. CRKE będzie współtworzyć i dystrybuować zarówno standardy i rekomendacje sektorowe dla Telco współpracując z CSIRT Telco, jak i regulacje, które przyczyniają się do poprawy bezpieczeństwa. Ponadto odczuwalne obecnie skutki niedoboru specjalistów ds. bezpieczeństwa sieci, będą ograniczane przez efektywne dzielenie się wiedzą. Szkolenia, warsztaty, informacje analityczne pozwolą na usprawnienie procesu reklamacyjnego i podniesienie poziomu obsługi skarg i postępowania ADR.

Przedstawione założenia projektu wpisują się w realizację zadań UKE wskazanych w ustawie prawo telekomunikacyjne (par. 192 ust. 1 pkt. 19).

| Interesariusz | Zidentyfikowany problem | Szacowana wielkość grupy |
| --- | --- | --- |
| Przedsiębiorcy telekomunikacyjni (w szczególności z sektora MŚP) | 1. Brak możliwości bezpiecznej wymiany doświadczeń, dzielenia się wiedzą o incydentach między Przedsiębiorcami Telekomunikacyjnymi (PT). 2. Potrzeba wymiany doświadczeń i wniosków, dotyczących narzędzi i taktyk pozwalających na wczesną detekcję i blokowanie incydentów związanych z bezpieczeństwem sieci i unikanie incydentów w sieciach telekomunikacyjnych. 3. Brak możliwości efektywnego przeprowadzenia diagnozy poziomu bezpieczeństwa, identyfikacji słabości w bezpieczeństwie oraz skutecznego wdrażania, rekomendacji przez PT w ich sieciach. 4. Zróżnicowany poziom świadomości bieżących zagrożeń w zależności od potencjału PT. 5. Zróżnicowany poziom dojrzałości organizacji w obszarze bezpieczeństwa sieci. 6. Znaczna ilość podatności mogących wpływać na bezpieczeństwo sieci i usług dostarczanych przez PT 7. Brak zaufania i niski poziom współpracy oraz wymiany informacji pomiędzy konkurującymi między sobą PT | 4 124 przedsiębiorców telekomunikacyjnych[[2]](#footnote-3) |
| Klienci (indywidualni oraz instytucjonalni) przedsiębiorców telekomunikacyjnych | 1. Brak informacji o reputacji i stanie sieci, poziomie dostępności, ciągłości usług telekomunikacyjnych. 2. Zakłócenia / incydenty w zakresie bezpieczeństwa, prywatności i/lub integralności mające miejsce, lub pochodzące ze słabo zabezpieczonych sieci teleinformatycznych o niskiej reputacji mogą mieć negatywny wpływ na jakość / ciągłość usług oferowanych klientom indywidualnym oraz finalnie na reputacje usług telekomunikacyjnych. | 16,2 mln  użytkowników sieci Internet; liczba aktywnych kart SIM -52,2 mln szt 3,5 mln abonentów telefonii stacjonarnej; 2,5 mln abonentów / użytkowników VoIP |
| Stowarzyszenia zrzeszające przedsiębiorców telekomunikacyjnych | Brak możliwości bezpiecznego transferu wiedzy i informacji na temat poziomu nieautoryzowanego ruchu w sieci, oraz narzędzi do weryfikacji sporów między przedsiębiorcami co do rozliczeń usług w sieciach. | 4 |

1.2. Opis stanu obecnego

W 2020 r. UKE odnotował 96 poważnych naruszeń bezpieczeństwa i integralności sieci i usług(w2019 r. odnotowano 95 tego typu naruszeń, a w 2018 r. - 198[[3]](#footnote-4)). Natomiast w 2019 r. CERT Polska obsłużył łącznie 22 343 zgłoszenia, Na podstawie 10 489 zgłoszeń zarejestrowano 6 484 incydenty zagrażające cyberbezpieczeństwu (dla porównania w 2018 r. - 3 739 incydentów). W porównaniu do danych za 2018 r. CERT Polska zarejestrował rekordowy wzrost liczby obsługiwanych incydentów na poziomie 73%. Najczęściej występującym incydentem był atak typu phising, kolejne miejsca zajmują ataki związane z użyciem złośliwego oprogramowania oraz incydenty dotyczące obraźliwych i nielegalnych treści, w tym spam. W zeszłym roku w ramach ustawy o Krajowym Systemie Cyberbezpieczeństwa Zespół CERT Polska obsłużył 9 incydentów, które zaklasyfikowano jako poważne, czyli takie, których wystąpienie ma istotny skutek zakłócający świadczenie usługi kluczowej. W podziale na sektory gospodarki dotknięte incydentami sieci należy odnotować, że udział incydentów związanych z sektorami infrastruktury cyfrowej oraz poczty oraz usług kurierskich wynosił 9,3%.[[4]](#footnote-5)

Aktualnie nie ma narzędzia pozwalającego na automatyczne przekazywanie oraz gromadzenie i przetwarzanie tych zgłoszeń. Dlatego w rzeczywistości powyższe dane obrazujące zgłoszenia zaraportowane do UKE czy CERT Polska mogą nie obejmować wszystkich naruszeń przez co skala i skutki incydentów w sektorze Telco mogą być znacząco większe. Ponadto z dużym prawdopodobieństwem można założyć, że zjawiska te będą się nasilać, uwzględniając postępującą rozbudowę sieci i rozwój usług.

Realne wskaźniki mogą być bardziej niepokojące, niż zaprezentowane poniżej, ze względu na brak ich raportowania przez konsumentów. Z tego względu należy też zwrócić uwagę na pośrednie sygnały świadczące o skali wyzwań stojących przez sektorem Telco w obszarze bezpieczeństwa.

Średni czas pomiędzy wykryciem obecności hakera a momentem, w którym przejął on kontrolę nad infrastrukturą firmy, wciąż przekracza aż pół roku[[5]](#footnote-6).

Przedsiębiorcy telekomunikacyjni identyfikują naruszenia bezpieczeństwa oraz integralności sieci lub usług na podstawie kryteriów uznania zakłócenia za naruszenie mające istotny wpływ na funkcjonowanie sieci lub usług telekomunikacyjnych. Obowiązek zgłaszania incydentów dotyczy naruszeń, które dotknęły co najmniej 10 000 użytkowników przez określony czas. Czas braku dostępności lub ograniczenia usługi, jaki podlega zgłoszeniu zależy tego, ilu użytkowników danej usługi dotknęło dane naruszenia. Zgłoszeniu podlegają również naruszenia skutkujące niedostępnością telefonów alarmowych (np. 112).

Ponadto pojawia się wiele niepokojących informacji o różnego rodzaju aktywnościach z wykorzystaniem połączeń telefonicznych oraz SMS, mogących prowadzić do strat finansowych u konsumentów (nakłanianie do instalacji szkodliwych aplikacji, powodujących kradzież danych oraz środków finansowych, czy wiadomości SMS zachęcające do zapoznania się z „ofertą”, a w efekcie aktywujące niechciane płatne usługi bez wiedzy konsumenta)

Szerokie grono PT nie ma możliwości gromadzenia wiedzy na temat aktualnych zagrożeń i ryzyka, oraz wykorzystania doświadczeń specjalistów, którzy znają specyfikę sektora i mają najbardziej aktualne informacje na temat zagrożeń. Brak jest obecnie platformy współpracy i wymiany informacji między PT, a operatorami usług kluczowych.

Zasadnym jest udostępnienie dla PT (zwłaszcza pochodzącym z grupy MŚP) kompleksowej e-usługi w obszarze CRKE opartej o założenia modelu ISAC, obejmującej następujące procesy:

1. gromadzenie i analizowanie danych dot. zdarzeń bezpieczeństwa w infrastrukturze ICT (PT),
2. udostępnianie wyników analizy incydentów w infrastrukturach PT oraz przedstawianie rekomendacji w zakresie przeciwdziałania ponownym incydentom zgodnie z wytycznymi CSIRT Poziomu Krajowego dla branży Telco[[6]](#footnote-7),
3. raportowania incydentów bezpieczeństwa zgodnie z obowiązkami PT,
4. modelowania, agregowania danych niezbędnych do prowadzenia analiz, przygotowanie wytycznych implementacyjnych.

Istotnym elementem CRKE jest platforma edukacyjna pozwalająca na prowadzenie szkoleń on-line, uzupełniona o system pozwalający na prowadzenie certyfikowanych egzaminów w formie on-line. Szkolenia będą adresowane do szerokiego grona konsumentów oraz PT, a formuła pozwoli na dostęp w dogodnym dla nich czasie.

Dotychczas UKE nie uruchomił procesu, który realizuje funkcje zbliżone do ISAC. W związku z tym proces gromadzenia wiedzy na temat zagrożeń i ryzyka ma charakter rozproszony i niesystematyczny. Proces ten obecnie cechuje się również niewielkim przepływem informacji między interesariuszami. Dzięki skutecznej kwalifikacji informacji, istotna ich część może zostać upubliczniona szerokiemu gronu odbiorców. Planowane systemy pozwolą na prowadzenie bezpiecznej komunikacji w ramach członków ISAC, co pozwoli na efektywną wymianę informacji.

Gromadzone i udostępniane informacje o reputacji sieci i usług pozwolą na budowanie wyższego poziomu świadomości konsumenckiej oraz promowanie bezpiecznych zachowań w zakresie użytkowania sieci.

1. EFEKTY PROJEKTU
   1. Cele i korzyści wynikające z projektu

|  |  |
| --- | --- |
| Cel - 1 | Wypracowanie, przetestowanie oraz wdrożenie technicznych narzędzi wspierających CRKE oraz zbudowanie relacji między profesjonalistami z wykorzystaniem organizacyjno-proceduralnych rozwiązań skutecznej wymiany informacji o podatnościach, zagrożeniach, rekomendacjach i standardach pozwalających na osiągnięcie wysokiego poziomu bezpieczeństwa sieci oraz konsumentów, dzięki udostępnieniu istotnych informacji oraz szkoleń na platformie on-line w obszarze komunikacji elektronicznej w sektorze telekomunikacyjnym w okresie 07.2021-06.2023 |
| Cel strategiczny | Przedmiotowy projekt wpisuje się w następujące dokumenty strategiczne:   1. Program Zintegrowanej Informatyzacji Państwa,   cel główny: modernizacja administracji publicznej i usprawnienie funkcjonowania państwa przy wykorzystaniu technologii cyfrowych cel szczegółowy: Zwiększenie jakości oraz zakresu komunikacji między obywatelami i innymi interesariuszami a państwem (o którym mowa w pkt 4.2.1 Programu)   1. Program Operacyjny Polska Cyfrowa   cel szczegółowy nr 2 „Wysoka dostępność i jakość e-usług publicznych” w ramach Osi priorytetowej II. „E-administracja i otwarty rząd” PO PC.   1. Strategia na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.)   Obszar: E-państwo / Kierunek Interwencji: Budowa i rozwój e-administracji – orientacja administracji państwa na usługi cyfrowe   1. Strategia „Sprawne i Nowoczesne Państwo 2030” (projekt) cel szczegółowy III. Podniesienie sprawności realizacji zadań państwa poprzez wykorzystanie technologii cyfrowych i zmianę sposobu działania stosownie do możliwości, jakie stwarza technologia 2. „Strategiczne kierunki działań Prezesa UKE w latach 2017-2021”. Kierunek: podnoszenie jakości usług telekomunikacyjnych, w tym zapewnienie ich bezpieczeństwa, m.in. poprzez promowanie rekomendacji i standardów ENISA (European Union Agency for Cybersecurity) oraz wdrażanie dobrych praktyk w zakresie cyberbezpieczeństwa przez regulatorów UE. 3. „Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024”. Cel szczegółowy 1 – rozwój krajowego systemu cyberbezpieczeństwa |
| Korzyść: | Główne korzyści wynikające z realizacji projektu:  1/ Umożliwienie bezpiecznej wymiany informacji między profesjonalistami z PT. Dzielenie się specjalistyczną wiedzą oraz budowa kompetencji z obszaru bezpieczeństwa sieci i usług oferowanych przez PT,  2/ Podniesienie poziomu bezpieczeństwa informatycznego w sektorze Telco,  3/ Wypracowanie i propagacja rekomendacji w zakresie bezpieczeństwa usług telekomunikacyjnych w oparciu o rekomendacje CSIRT Poziomu Krajowego, rekomendacje dla Telco oraz analogicznych źródeł,  4/ Poprawa jakości i niezawodności cyfrowych usług publicznych oraz możliwość świadczenia ich bardziej zaawansowanych form,  5/ Łatwiejsze, sprawniejsze i niezakłócone korzystanie z szeregu dostępnych dla przedsiębiorców telekomunikacyjnych cyfrowych usług publicznych w kontaktach z e-administracją,  6/ Minimalizacja kosztów związanych z skutkami i obsługą incydentów bezpieczeństwa zarówno w odniesienie do klienta indywidualnego jak i podmiotów administracji państwowej,  7/ Zacieśnienie współpracy pomiędzy specjalistami ds. bezpieczeństwa PT, a innymi podmiotami o podobnych funkcjach,  8/ Zwiększenie zaufania do usług zarządzanych i udostępnianych przez administrację państwową. |
| KPI: | KPI nr 1: Liczba usług publicznych udostępnionych on-line o stopniu dojrzałości co najmniej 4 – transakcja  KPI nr 2: Liczba załatwionych spraw poprzez udostępnioną on-line usługę publiczną  KPI nr 3: Liczba uruchomionych systemów teleinformatycznych w podmiotach wykonujących zadania publiczne  KPI nr 4: Liczba pracowników podmiotów wykonujących zadania publiczne niebędących pracownikami IT, objętych wsparciem szkoleniowym - ogółem  KPI nr 5. Liczba pracowników podmiotów wykonujących zadania publiczne nie będących pracownikami IT, objętych wsparciem szkoleniowym – kobiety  KPI nr 6. Liczba pracowników podmiotów wykonujących zadania publiczne nie będących pracownikami IT, objętych wsparciem szkoleniowym – mężczyźni |
| Wartość aktualna i docelowa KPI: | wartość bazowa KPI nr 1: 0  wartość bazowa KPI nr 2: 0  wartość bazowa KPI nr 3: 0  wartość bazowa KPI nr 4: 0  wartość bazowa KPI nr 5: 0  wartość bazowa KPI nr 6: 0  wartość docelowa KPI nr 1: 1  wartość docelowa KPI nr 2: 250 konsultacji oraz rekomendacji w obszarze incydentów bezpieczeństwa rocznie  wartość docelowa KPI nr 3: 1  wartość docelowa KPI nr 4: 32  wartość docelowa KPI nr 5: 16  wartość docelowa KPI nr 6: 16 |
| Metoda pomiaru KPI | Metoda, źródło danych i częstotliwość pomiaru KPI nr 1: testy wdrożeniowe i akceptacyjne systemu  Metoda i częstotliwość pomiaru KPI nr 2: raporty miesięczne podsumowujące konsultacje / rekomendacje w obszarze incydentów i reakcje na nie oraz raporty z przeprowadzonych usług skanowania podatności infrastruktury przedsiębiorców telekomunikacyjnych  Metoda i częstotliwość pomiaru KPI nr 3: testy wdrożeniowe i akceptacyjne systemu  Metoda i częstotliwość pomiaru KPI nr 4,5,6: dokumentacja szkoleniowa (m.in. materiały szkoleniowe, listy obecności, wyniki testów wiedzy i umiejętności po szkoleniu) |

* 1. Udostępnione e-usługi

| Lp. | Nazwa e-usługi | Typ | Zakres  oddziaływania | Poziom dojrzałości e-usługi |
| --- | --- | --- | --- | --- |
| 1 | E-usługa obejmująca:  Platformę bezpiecznej wymiany informacji między PT (na zasadzie dobrowolności) | A2B A2C | Przedsiębiorcy telekomunikacyjni (w szczególności z  sektora MŚP)  Klienci (indywidualni oraz instytucjonalni) przedsiębiorców telekomunikacyjnych Stowarzyszenia zrzeszające przedsiębiorców telekomunikacyjnych (rocznie ok 3000 transakcji) Podmioty wymieniające informacje na podstawie przyjętych zasad. | Personalizacja |
| 2 | E-usługa obejmująca:  Bazę wiedzy |  | W zależności od klasyfikacji informacji.  Przedsiębiorcy telekomunikacyjni (w szczególności z sektora  MŚP)  Stowarzyszenia zrzeszające przedsiębiorców telekomunikacyjnych (rocznie ok 3000 transakcji) | Personalizacja |
| 3 | E-usługa obejmująca:  Platformę do realizacji szkoleń on-line |  | Przedsiębiorcy telekomunikacyjni (w szczególności z sektora  MŚP)  Stowarzyszenia zrzeszające przedsiębiorców telekomunikacyjnych (rocznie ok 3000 transakcji).  Konsumenci | Personalizacja |
| 4 | E-usługa obejmująca:  Platformę do realizacji certyfikowanych egzaminów on-line |  | Podmioty i osoby zgodnie z opracowanym programem. | Personalizacja |
| 5 | E-usługa prezentowania informacji o reputacji dla sektora Telko |  | W zależności od klasyfikacji informacji.  Przedsiębiorcy telekomunikacyjni (w  szczególności z sektora  MŚP)  Stowarzyszenia zrzeszające przedsiębiorców telekomunikacyjnych (rocznie ok 3000 transakcji) | Personalizacja |
| 6 | E-usługa raportowania incydentów przez konsumenta |  | Konsumenci | Personalizacja |

* 1. Udostępnione informacje sektora publicznego i zdigitalizowane zasoby

|  |  |  |
| --- | --- | --- |
| Rodzaj informacji/zasobów | Planowana data udostępnienia | Szacowana liczba obiektów objętych digitalizacją  (udostępnianiem informacji) |
| informacje statystyczne dotyczące incydentów bezpieczeństwa | 31-05-2023 | 1 |
| branżowa baza wiedzy o zagrożeniach w sektorze telekomunikacyjnym | 31-05-2023 | 1 |
| dokumentacja API integracyjna | 28-02-2023 | 4 |

Czy wszystkie zdigitalizowane zasoby objęte projektem będą udostępniane bezpłatnie?

TAK/~~NIE~~

* 1. Produkty końcowe projektu

|  |  |
| --- | --- |
| Nazwa produktu | Planowana data wdrożenia |
| Sprzęt i oprogramowanie standardowe – zgodnie ze specyfikacją. Montaż fizyczny urządzeń oraz wstępne uruchomienie. Implementacja platformy sprzętowej w infrastrukturze Data Center UKE. Przeprowadzenie testów poprawności działania. | 10-2021 |
| Dokumentacja projektowa – W ramach realizacji projektu zostanie przygotowana dokumentacja analityczna i projektowa obejmująca projekty techniczne, dokumentacje procedur instalacyjnych i uruchomieniowych. | 11-2021 |
| Konfiguracja Systemu – Konfiguracja komponentów systemu. | 12-2021 |
| Koncepcja organizacyjna CRKE – Opracowanie dokumentacji dotyczącej budowy organizacji CRKE wraz z zaprojektowaniem procesów zgodnie z  międzynarodowymi standardami. | 12-2021 |
| Implementacja i organizacja systemu teleinformatycznego CRKE | 10-2022 |
| Opracowanie oraz implementacja podstawowych szkoleń | 04-2023 |
| Opracowanie oraz implementacja wybranych testów w systemie on-line | 04-2023 |
| Baza wiedzy zawierająca informacje na temat typów incydentów i sposobów ich rozwiązania | 04-2023 |
| Raport z testów systemu – zostaną przeprowadzone testy całego systemu na podstawie dostarczonych planów testów oraz scenariuszy testowych. Proces weryfikacji i walidacji dla zapewnienia oczekiwanej jakości produktów projektu będzie realizowany na przestrzeni całego cyklu życia projektu | 05-2023 |
| Szkolenia – Zostaną przygotowane i przeprowadzone cykle szkoleń dla wybranych grup pracowników obejmujące: obsługę systemu, administrację systemem oraz realizację procesów biznesowych. | 06-2023 |

1. KAMIENIE MILOWE

|  |  |
| --- | --- |
| Kamienie milowe | Planowany termin osiągnięcia |
| Opracowanie specyfikacji docelowego rozwiązania systemu CRKE | 2021-08-31 |
| Dostawa platformy sprzętowej oraz oprogramowania wraz z instalacją fizyczną | 2021-09-30 |
| Prototyp platformy narzędziowej dla CRKE | 2022-02-28 |
| Konfiguracja laboratorium systemu szkoleń on-line | 2022-06-30 |
| Konfiguracja systemu VM wraz z integracją | 2022-06-30 |
| Wykonanie dokumentacji do przygotowywania szkoleń on-line. | 2022-10-31 |
| Wykonanie dokumentacji do przygotowywania egzaminów on-line. | 2022-10-31 |
| Gotowość organizacyjna systemu CRKE | 2022-10-31 |
| Rozwój systemu CRKE - wdrożenie scenariuszy analitycznych dla grupy | 2023-02-28 |
| Kamienie milowe | Planowany termin osiągnięcia |
| Rozwój systemu CRKE – wdrożenie kompletu scenariuszy analitycznych | 2023-03-31 |
| Testy systemu – zostaną przeprowadzone testy całego systemu na podstawie dostarczonych planów testów oraz scenariuszy testowych. Proces weryfikacji i walidacji dla zapewnienia oczekiwanej jakości produktów projektu będzie realizowany na przestrzeni całego cyklu życia projektu | 2023-05-31 |
| Uruchomienie branżowej bazy wiedzy o zagrożeniach w sektorze Telekomunikacyjnym | 2023-05-31 |
| Udostępnienie informacji statystycznych dotyczących incydentów bezpieczeństwa | 2023-05-31 |
| Odbiór końcowy Systemu CRKE przez Zamawiającego (komponentów sprzętowych, komponentów programowych, dokumentacji API , dokumentacji powykonawczej, kodów źródłowych, bibliotek, praw autorskich, licencji standardowego oprogramowania). Przekazanie  Zamawiającemu dokumentu gwarancji – protokół odbioru końcowego. | 2023-05-31 |
| Podpisanie Umowy Gwarancyjnej na System CRKE (2-lata) i realizacja działań Wykonawcy w okresie gwarancyjnym. | 2023-06-30 |
| Szkolenia – Zostaną przygotowane i przeprowadzone cykle szkoleń dla wybranych grup pracowników obejmujące: obsługę systemu CRKE, administrację systemem oraz realizację procesów biznesowych. | 2023-06-30 |
| Zakończenie projektu systemu CRKE | 2023-06-30 |

1. KOSZTY
   1. Koszty ogólne projektu wraz ze sposobem finansowania

|  |  |  |
| --- | --- | --- |
| Całkowity koszt projektu (netto oraz brutto), w tym | Netto 22 007 821,14 zł Brutto 27 069 620,00 zł | |
| Procent dofinansowania ze środków UE (brutto) | 84,63% | |
| Procent środków z budżetu państwa (brutto) | 15,37% | |
| Podział całkowitego kosztu projektu na poszczególna lata (netto oraz brutto) | 2021 | Netto 8 376 861,79 zł  Brutto 10 303 540 zł |
| 2022 | Netto 7 619 544,72 zł  Brutto 9 372 040,00 zł |
| 2023 | Netto 6 011 414,63 zł  Brutto 7 394 040,00 zł |

* 1. Wykaz poszczególnych pozycji kosztowych

| Nazwa pozycji kosztowej | | Przewidywany koszt brutto | Uzasadnienie pozycji kosztowej (przeznaczenie) |
| --- | --- | --- | --- |
| Oprogramowanie | Oprogramowanie obejmuje niezbędne narzędzia i oprogramowanie zabezpieczające działanie e-usług. | 8 110 000,00 zł | Oprogramowanie to jeden z niezbędnych elementów to funkcjonowania CRKE (w szczególności w postaci e-usług). |
| Infrastruktura | Infrastruktura techniczna niezbędna do implementacji rozwiązania | 1 000 000,00 zł | Infrastruktura techniczna niezbędna do implementacji rozwiązania oraz narzędzia wspierające administrowanie systemem, w tym narzędzia do zarządzania użytkownikami uprzywilejowanymi. |
| Koszty UX i grafiki | Zapewnienie przyjaznego oraz ergonomicznego interfejsu z punktu widzenia użytkowników systemu. | 2 000 000,00 zł | W celu zapewnienia odpowiedniej ergonomii użytkowania, intuicyjnego GUI w architekturze klient-serwer i wsparcia różnych OS (Windows, Android, IOS), w tym aplikacje wizualizacji wyników i aktywny dashboard. |
| Bezpieczeństwo | opracowanie / zakup elementów gwarantujących bezpieczeństwo systemu | 1 828 800,00 zł | opracowanie / zakup elementów gwarantujących bezpieczeństwo systemu |
| Wydajność rozwiązań | Koszt obejmuje realizację głównych procesów jakie mają doprowadzić do docelowego rozwiązania | 2 400 000,00 zł | Przygotowanie koncepcji CRKE, obejmuje projekt techniczny, funkcjonalny i organizacyjny oraz opracowanie prototypu platformy.  Implementacja rozwiązania wraz ze wszystkimi komponentami technologicznymi, aplikacyjnymi oraz elementami bezpieczeństwa. W ramach platformy, zostanie wytworzony autorski system |
| Szkolenia | Szkolenia skierowane zarówno do administratorów i przygotowania zespołów, jak i szkolenia dla użytkowników | 5 000 000,00 zł | Szkolenia osób zaangażowanych w obsługę systemu są niezbędne do efektywnego wdrożenia rezultatów projektu. |
| Działania informacyjnopromocyjne | content marketing, konferencja, publikacje w czasopismach i na portalach branżowych | 3 200 000,00 zł | Są to działania niezbędne do tego aby poinformować o projekcie i zachęcić do skorzystania z rezultatów projektu poszczególne grupy interesariuszy, w szczególności przedsiębiorstw telekomunikacyjnych. |
| Koszty zarządzania i wsparcia (w tym wynagrodzenia personelu wspomagającego) | wynagrodzenia osób  zaangażowanych w realizację projektu | 3 530 712,00 zł | wynagrodzenia osób zaangażowanych w realizację projektu brutto-brutto (obejmujące także składki ubezpieczeniowe opłacane przez pracodawcę); koszty nie przekraczają 15% całkowitej wartości projektu. |

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

|  |  |  |  |
| --- | --- | --- | --- |
| Całkowity koszt utrzymania trwałości projektu (brutto) | 2 637 800,00 zł | | Źródło finansowania |
| Podział całkowitego kosztu utrzymania trwałości projektu na poszczególna lata (netto oraz brutto) | 2023 | 239 800,00 zł (brutto)  (194 959, 35 zł netto) | krajowe środki  publiczne - budżet  państwa |
| 2024 | 479 600,00 zł (brutto)  (389 918,70 zł netto) | krajowe środki  publiczne - budżet  państwa |
| 2025 | 479 600,00 zł (brutto)  (389 918,70 zł netto) | krajowe środki  publiczne - budżet  państwa |
| 2026 | 479 600,00 zł (brutto)  (389 918,70 zł netto) | krajowe środki  publiczne - budżet  państwa |
| 2027 | 479 600,00 zł (brutto)  (389 918,70 zł netto) | krajowe środki  publiczne - budżet  państwa |
| 2028 | 479 600,00 zł (brutto)  (389 918,70 zł netto) | krajowe środki  publiczne - budżet  państwa |

* 1. 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~~

1. GŁÓWNE RYZYKA
   1. Ryzyka wpływające na realizację projektu

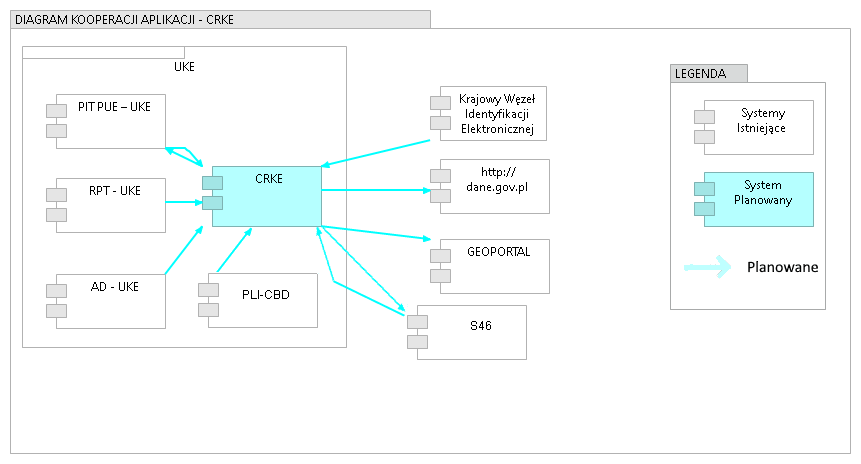
| Nazwa ryzyka | Siła  oddziaływania | Prawdopo- dobieństwo  wystąpienia ryzyka | Sposób zarzadzania ryzykiem |
| --- | --- | --- | --- |
| Brak możliwości wykrywania incydentów na wczesnym etapie | Średnia | Średnie | Budowa zespołu, szkoleni i warsztaty. Opracowanie optymalnych procedur działania. |
| Błędne dobranie czynników ryzyka identyfikujących ataki / Błędna identyfikacja czynników ryzyka, które będą uwzględnione podczas oceny bezpieczeństwa a w efekcie brak możliwości poprawnego wykrywania zagrożeń. | Duża | Średnie | Do identyfikacji czynników zostaną wykorzystane zróżnicowane źródła wiedzy o bezpieczeństwie systemu, w tym aktualne zbiory charakterystyk ataków teleinformatycznych pochodzące m.in. od przedsiębiorstw telekomunikacyjnych.  Weryfikacja informacji dotyczących czynników ryzyka identyfikujących ataki na platformach: Mitrie Attack i OWASP. Konsultacja czynników w ramach sieci ISAC. |
| Ryzyko nieodpowiedniego zabezpieczenia przetwarzanych danych / ryzyko nieodpowiedniego zabezpieczenia danych wykorzystywanych w pracach nad budową i rozwojem  systemu - gdy przechowywane dane będą nieodpowiednio zabezpieczone lub dostęp do nich zostanie umożliwiony nieodpowiednim osobom. | Duża | Niskie | Opracowanie wytycznych (zaleceń) w zakresie bezpiecznego przetwarzania danych (anonimizacja danych, kontrola dostępu).  Przeszkolenie zaangażowanego personelu w zakresie bezpieczeństwa danych.  Stosowanie pseudonimizacji danych testowych.  Użycie generatorów danych do zastosowania podczas testów. Cykliczne monitorowanie środowiska bezpieczeństwa. |
| Rotacja członków zespołu projektowego / Wystąpienie rotacji członków zespołu projektowego może doprowadzić do zachwiania efektywnego gromadzenia i zarządzania wiedzą w ramach prac projektowych. | Średnia | Średnie | Prowadzenie repozytorium projektowego, w którym umieszczane będą wszelkie informacje o stanie poszczególnych zadań oraz dokumenty związane z nimi. Wykorzystywanie systemu motywowania w celu utrzymania stałego zespołu.  Monitorowanie nastrojów zespołu w celu aktywnego oddziaływania. Bieżące rozwiązywanie problemów projektowych i wewnątrz-zespołowych. |

* 1. Ryzyka wpływające na utrzymanie efektów

| Nazwa ryzyka | Siła  oddziaływania | Prawdopodobieństwo  wystąpienia ryzyka | Sposób zarzadzania ryzykiem |
| --- | --- | --- | --- |
| Niekonkurencyjność w miarę upływu czasu | Duża | Niskie | W pracach nad rozwiązaniem konieczne  będzie uwzględnienie w analizie zagrożeń różnych modeli: działanie ludzi, urządzeń czy sieci. Elementem wpływającym na zmniejszenie tego typu ryzyka jest również analiza danych ze  wszystkich dostępnych źródeł oraz ciągłe uczenie się i porównania do normalnie działającej sieci, korelacja wszelkich anomalii. Monitorowanie metod dostępnych w istniejących rozwiązaniach. Monitorowanie wskaźników . Konsultacja metod w ramach sieci ISAC. |
| Zaproponowane metody będą w miarę upływu czasu  niekonkurencyjne wobec istniejących rozwiązań. | Duża | Wysokie | Ze względu na charakter problemu wykrywania anomalii należy zakładać, iż istotną rolę dla jakości końcowej diagnozy bezpieczeństwa odgrywa skuteczna komunikacja i relacje oparte na zaufaniu. |
| Zmiany legislacyjne warunkujące zmiany w działaniu Centrum CRKE | Średnia | Średnie | Bieżący monitoring zmian prawnych oraz dostosowywanie organizacyjnotechniczne CRKE uwzględniające nowe regulacje prawne. Wymiana informacji w ramach sieci ISAC. |
| Ryzyko niewystarczającej ilości Klientów (przedsiębiorstw telekomunikacyjnych) zainteresowanych skorzystaniem z eusług | Średnia | Średnie | Przygotowanie kampanii informacyjnej dotyczącej branżowych zagadnień związanych z potrzebą monitorowania infrastruktury IT. Kontakty bezpośrednie z przedsiębiorcami telekomunikacyjnymi zaangażowanymi w projekt dla informowania innych podmiotów w ramach kontaktów branżowych. |

1. OTOCZENIE PRAWNE

| Lp. | Tytuł aktu prawnego | Czy wymaga zmian | Opis zmian  (jeśli  dotyczy) | Etap prac legislacyjnych  (jeśli dotyczy) |
| --- | --- | --- | --- | --- |
| 1 | Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. 2004 nr 171 poz. 1800, ze zmianami) | ~~TAK~~/NIE |  |  |
| 2 | Ustawa z dnia … wprowadzająca ustawę – Prawo komunikacji elektronicznej – Projekt z dnia 29 lipca 2020 r. https://legislacja.gov.pl/ projekt/12336501 | ~~TAK~~/NIE |  |  |
| 3 | Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560) | ~~TAK~~/NIE |  |  |
| 4 | Ustawa z dnia … 2020 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych - Projekt z 7 września 2020 r. https:// mc.bip.gov.pl/articles/view/361169/projektustawy-o-zmianie-ustawy-o-krajowym-systemiecyberbezpieczenstwa-oraz-ustawy-prawozamowien-publicznych.html/year:2020/ month:09/day:08 | ~~TAK~~/NIE |  |  |
| 5 | Rozporządzenie Ministra Cyfryzacji z dnia 22 czerwca 2020 r. w sprawie minimalnych środków technicznych i organizacyjnych oraz metod, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług. (Dz. U. 2020 poz. 1130.) | ~~TAK~~/NIE |  |  |
| 6 | Rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie wzoru formularza do przekazywania informacji o naruszeniu bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych, które miało istotny wpływ na funkcjonowanie sieci lub usług. (Dz.  U. 2018 poz. 1831) | ~~TAK~~/NIE |  |  |
| 7 | Rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie kryteriów uznania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług (Dz. U. 2018 poz. 1830) | ~~TAK~~/NIE |  |  |
| 8 | Rozporządzenie Rady Ministrów z dnia 19 sierpnia 2020 r. w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń. (Dz. U.  2020 poz. 1464) | ~~TAK~~/NIE |  |  |
| 9 | ROZPORZĄDZENIE PARLAMENTU  EUROPEJSKIEGO I RADY (UE) 2015/2120 z dnia 25 listopada 2015 r. ustanawiające środki dotyczące dostępu do otwartego internetu oraz zmieniające dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, a także rozporządzenie (UE) nr 531/2012 w sprawie 26.11.2015 | PL |  Dziennik Urzędowy Unii Europejskiej | L 310/1) | ~~TAK~~/NIE |  |  |
| 10 | DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2018/1972 z dnia 11 grudnia 2018 r.  ustanawiająca Europejski kodeks łączności elektronicznej (17.12.2018 | PL | Dziennik  Urzędowy Unii Europejskiej | L 321/36) | ~~TAK~~/NIE |  |  |
| 11 | DYREKTYWA 2007/2/WE PARLAMENTU  EUROPEJSKIEGO I RADY z dnia 14 marca 2007 r. ustanawiająca infrastrukturę informacji przestrzennej we Wspólnocie Europejskiej (INSPIRE) (25.4.2007| PL | Dziennik Urzędowy  Unii Europejskiej | L 108/1) | ~~TAK~~/NIE |  |  |
| 12 | Komunikat KE łączności dla konkurencyjnego jednolitego rynku cyfrowego „W kierunku społeczeństwa gigabitowego”- cele do 2025 r. https://www.gov.pl/web/cyfryzacja/komunikatkomisji-europejskiej-w-kierunku-europejskiegospoleczenstwa-gigabitowego | ~~TAK~~/NIE |  |  |
| 13 | Europejska Agenda Cyfrowa https:// www.europarl.europa.eu/factsheets/pl/ sheet/64/digital-agenda-for-europe | ~~TAK~~/NIE |  |  |
| 14 | BEREC Opinion for the evaluation of the application of Regulation (EU) 2015/2120 and  the BEREC Net Neutrality Guidelines, BOR(18)244, 6.12.2018 https://berec.europa.eu/eng/document\_register/ subject\_matter/berec/opinions/8317%20berec-opinion-for-the-evaluation-of-theapplication-of-regulation-eu-20152120-and-theberec-netneutrality-guidelines | ~~TAK~~/NIE |  |  |
| 15 | ROZPORZĄDZENIE RADY MINISTRÓW z dnia  12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci  elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych  http://isap.sejm.gov.pl/isap.nsf/download.xsp/  WDU20170002247/  O/D20172247.pdf | ~~TAK~~/NIE |  |  |
| 16 | Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne z późn. zm. | ~~TAK~~/NIE |  |  |

1. ARCHITEKTURA
   1. Widok kooperacji aplikacji
   2. Lista systemów wykorzystywanych w projekcie

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
| --- | --- | --- | --- | --- | --- |
| 1 | CRKE | Regulator -  UKE | System zawierający planowaną e-usługę | Planowany |  |
| 2 | Krajowy Węzeł  Identyfikacji  Elektronicznej | KPRM | Dostęp do usług przez Węzeł Krajowy pozwala używać uniwersalnego loginu i bezpiecznego hasła oraz korzystać z różnych środków identyfikacji elektronicznej. | Istniejący |  |
| 3 | Dane.gov.pl | KPRM | Portal Centralnego  Repozytorium Informacji  Publicznej, wskazanego w Ustawie o dostępie do informacji publicznej (Dz. U. Nr 112, poz. 1198, z późn. zm.) jako jeden z  trybów dostępu i ponownego wykorzystywania informacji publicznej. | Istniejący |  |
| 4 | Active  Directory (AD) | Regulator -  UKE | System podstawowej  rejestracji i logowania klientów UKE. | Istniejący |  |
| 5 | Rejestr  Przedsiębiorc ów  Telekomunikac  yjnych  – RPT | Regulator -  UKE | Dane o Przedsiębiorcach Telekomunikacyjnych w kraju wraz z zakresem i parametrach  świadczonych przez nich usług | Istniejący |  |
| 6 | GEOPORTAL / Dane centralnego zasobu geodezyjnego i  kartograficzne  go | GUGIK | Dane centralnego zasobu geodezyjnego i kartograficznego: Osnowy geodezyjne, grawimetryczne i  magnetyczne  Państwowy rejestr granic i jednostek podziałów  terytorialnych kraju  Ortofotomapa  Mapy topograficzne  Państwowy Rejestr Nazw  Geograficznych  Dane pomiarowe  Numeryczny model terenu  Numeryczny model pokrycia terenu  Mapy tematyczne  Baza Danych Obiektów  Ogólnogeograficznych Zintegrowane kopie baz danych obiektów  topograficznych BDOT10k Zobrazowania lotnicze | Istniejący |  |

Lista przepływów

| Lp. | System źródłowy | System docelowy | Zakres wymienianych danych | Sposób wymiany danych | Typ modyfikacji | Typ interfejsu |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | PIT PUE UKE | CRKE | Komunikacja z interesariuszam i. Zgłoszenia incydentów, zdarzeń bezpieczeństw  a. | Dla wszystkich systemów wewnętrznych UKE i zewnętrznych:  - przez Tryb odwołań bezpośrednich  (§13 ust. 2)  KRI | Tryb odwołań bezpośrednich  (§13 ust. 2)  KRI | Dla wszystkich systemów wewnętrznych  UKE i  zewnętrznych  – standard  HTTPS |
| 2 | CRKE | PIT PUE UKE | Diagnoza poziomu bezpieczeństwa , informacje o identyfikacji słabości w bezpieczeństw ie testowanej infrastruktury i aplikacji, zalecenia , wytyczne, informacje o ruchu w sieci PT. Informacje o  zakłóceniach incydentach w zakresie bezpieczeństw  a i/lub integralności, informacje o reputacji sieci teleinformatycznych | Dla wszystkich systemów wewnętrznych UKE i zewnętrznych:  - przez Tryb odwołań bezpośrednich  (§13 ust. 2)  KRI | Tryb odwołań bezpośrednich  (§13 ust. 2)  KRI | Dla wszystkich systemów wewnętrznych UKE i  zewnętrznych  – standard  HTTPS |
| 3 | RPT | CRKE | Dane o Przedsiębiorcach  Telekomunikacyjnych w kraju wraz z zakresem i parametrach świadczonych przez nich usług | Dla wszystkich systemów wewnętrznych UKE i zewnętrznych:  - przez Tryb odwołań bezpośrednich  (§13 ust. 2)  KRI | Tryb odwołań bezpośrednich  (§13 ust. 2)  KRI | Dla wszystkich systemów wewnętrznych UKE i  zewnętrznych  –standard  HTTPS |
| 4 | AD-UKE | CRKE | Udostępnienie tożsamości AD pozwalającej na logowanie do systemu wszystkich użytkowników  wewnętrznych  UKE | Inicjowany przez pracownika UKE za pomocą klienta AD | Tryb odwołań bezpośrednich  (§13 ust. 2)  KRI | Dla wszystkich systemów wewnętrznych UKE – standard  HTTPS |
| 5 | Krajowy  Węzeł  Identyfikacj  i  Elektronicz nej | CRKE | Dane związane z tożsamością użytkownika systemu (Nazwisko, Imię, Data urodzenia, NIP, PESEL, Data urodzenia) | Inicjowany przez podmiot zewnętrzny  posiadający  PZ | Tryb odwołań bezpośrednich  (§13 ust. 2)  KRI | Dla wszystkich systemów wewnętrznych UKE – standard  HTTPS, SOAP |
| 6 | CRKE | http:// dane.gov.p  l | Prezentacja raportów z e-usług cyfrowych | Automatyczny  dla raportów okresowych lub inicjowany przez pracownika UKE z wykorzystanie m  udostępnionych  mechanizmów  (API) Tryb odwołań bezpośrednich  (§13 ust. 2)  KRI | Tryb odwołań bezpośrednich  (§13 ust. 2)  KRI | Dla wszystkich systemów wewnętrznych UKE i  zewnętrznych  – standard  HTTPS |
| 7 | CRKE | GEOPORTA L | Prezentacja obiektów i informacji systemowych na mapach | Dla wszystkich systemów wewnętrznych UKE i zewnętrznych:  przez Tryb odwołań bezpośrednich  (§13 ust. 2)  KRI | Tryb odwołań bezpośrednich  (§13 ust. 2)  KRI | Dla wszystkich systemów  wewnętrznych    UKE i zewnętrznych  – standard  HTTPS |
| 8 | CRKE | S46 | Informacje bieżące , Informacje pozyskane z sieci, MISP, | Dla wszystkich systemów wewnętrznych UKE i zewnętrznych:  przez Tryb odwołań bezpośrednich  (§13 ust. 2)  KRI | Tryb odwołań bezpośrednich  (§13 ust. 2)  KRI | Dla wszystkich systemów Wewnętrznych UKE i  zewnętrznych -standard  HTTPS, JSON,  MISP |
| 9 | S46 | CRKE | Informacje bieżące, podatności, dobre praktyki, rekomendacje , informacje o  incydentach,  MISP | Dla wszystkich systemów wewnętrznych UKE i zewnętrznych:  przez Tryb odwołań bezpośrednich  (§13 ust. 2)  KRI | Tryb odwołań bezpośrednich  (§13 ust. 2)  KRI | Dla wszystkich systemów wewnętrznych UKE i  zewnętrznych -standard  HTTPS, JSON,  MISP |
| 10 | PLI-CBD | CRKE | Informacje o usterkach zgłaszanych przez operatorów uczestniczących w procesie przenoszenia numerów,  Informacje od „małych operatorów” dot, przekazywania oraz kontroli wymaganych danych. |  |  |  |

* 1. Kluczowe komponenty architektury rozwiązania

Diagram

Description automatically generated

* 1. Przyjęte założenia technologiczne

|  |  |  |
| --- | --- | --- |
| Lp. | Obszar | Założenie technologiczne |
| 1. | Infrastruktura | Infrastruktura oparta o istniejące technologie serwerowe, bazodanowe i macierzowe |
| 2. | Sieć i bezpieczeństwo | Sieć gigabit ethernet, FC, protokoły wymiany danych zgodne z TLS v.1.3 lub odpowiednie, system klasy WAF, system Firewall z funkcją IDS/IPS |
| 3. | Standardy wymiany danych | Sieć IP z zapewnieniem odpowiedniego szyfrowania |
| 4. | Systemy operacyjne serwerowe | Głównie systemy z rodziny Linux |
| 5. | Bazy danych | MySQL, natywne systemy bazodanowe dla rozwiązań bezpieczeństwa, indeksy ElasticSearch, Hadoop |
| 6. | Serwery aplikacji | Apache |
| 7. | Portale |  |
| 8. | Inne |  |

* 1. 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

* 1. 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~~
* dodatkowe zabezpieczenia powyżej wymogów KRI: należy wskazać uzasadnienie

Projektowana struktura CRKE będzie poprzez rozwiązania architektoniczne spełniała wysokie standardy m.in. jeśli chodzi o zapewnienie ciągłości działania, jako dostawca szeregu usług oferowanych w reżimie 24/7, oraz standardy bezpieczeństwa i ochrony informacji, które w momencie uruchomienia na koniec projektu potwierdzone zostaną pozyskaniem certyfikatów:

PN-ISO/IEC 22301 - z zakresie systemu zarządzania ciągłością działania w zakresie świadczenia usług związanych z sieciami teleinformatycznymi i cyberbezpieczeństwa,

PN-ISO/IEC 24762 - w zakresie systemu i procesu odtwarzania zasobów IT po katastrofie w ramach odtwarzania komponentów niezbędnych do zapewnienia ciągłości działania. ISO 27001 - w zakresie systemu zarządzania bezpieczeństwem informacji w zakresie świadczenia usług związanych z sieciami teleinformatycznymi i cyberbezpieczeństwem.

Całość platformy teleinformatycznej zbudowanej dla potrzeby CRKE, będzie spełniać wysokie standardy procesów utrzymania komponentów IT w działaniu, obejmujące takie cykliczne procesy jak:

* bieżące aktualizacje komponentów oprogramowania, pod kątem podatności, aktualności wersji, polityki uwierzytelniania tworzenia i zmiany haseł, kontroli i hierarchii dostępu, bezpieczeństwa i archiwizacji przechowywania danych.
* kontrola efektywności i kompleksowości mechanizmów redundancji, dostępu do oprogramowania systemowego, aktualizacje oprogramowania systemowego pod kątem usuwania luk i aktualizacji jego wersji, zapewnienia pełnej kontroli na fizycznym dostępem do fizycznych komponentów architektury.

1. Raport z badań spółki VECTO „Cyberbezpieczeństwo w polskich firmach 2020” - https://vecto.pl/doc/Vecto-Cyberbezpieczenstwo-polskich-firm-2020.pdf [↑](#footnote-ref-2)
2. Na podstawie Rejestru przedsiębiorców telekomunikacyjnych, prowadzonego przez Urząd Komunikacji Elektronicznej pod adresem: https://bip.uke.gov.pl/rpt/rejestr-przedsiebiorcow-telekomunikacyjnych, dostęp w dniu 20 maja 2021 r. [↑](#footnote-ref-3)
3. Dane pochodzą ze Sprawozdania z działalności Prezesa UKE z kolejnych lat (za 2018 r., 2019 r., 2020 r.). Sprawozdania dostępne na stronie: https://bip.uke.gov.pl/rpt/rejestr-przedsiebiorcow-telekomunikacyjnych [↑](#footnote-ref-4)
4. „Krajobraz bezpieczeństwa polskiego internetu Raport roczny 2019 z działalności CERT Polska” [↑](#footnote-ref-5)
5. https://home.kpmg/pl/pl/home/insights/2018/06/przygotowanie-firmy-na-cyberatak.html [↑](#footnote-ref-6)
6. Zgodnie z założeniami projektu nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa w zakresie funkcjonowania ISAC (Rozd.5a art.25a) [↑](#footnote-ref-7)