Załącznik 5. Studia przypadków

1. Krajowy schemat oceny i certyfikacji bezpieczeństwa oraz prywatności produktów i systemów IT zgodny z Common Criteria (KSO3C)

Nazwa projektu
Krajowy schemat oceny i certyfikacji bezpieczeństwa oraz prywatności produktów i systemów IT zgodny z Common Criteria (KSO3C)
Cel projektu
Celem projektu było stworzenie metod oraz technik ewaluacji bezpieczeństwa oraz prywatności na wysokim poziomie uzasadnienia pewności, opartych na innowacyjnym podejściu do oceny podatności związanych z tworzeniem zaawansowanych technik ataków, zarówno nieinwazyjnych, takich jak ataki typu side-channel czy inżynieria wsteczna, jak i inwazyjnych, takich jak ataki perturbacyjne.
Podmiot/podmioty zaangażowane w realizację
1. Instytut Łączności - Państwowy Instytut Badawczy – ***Lider konsorcjum*** 2. Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy 3. Instytut Technik Innowacyjnych EMAG
Zgodność z celami Programu CSI i określonymi tematami badawczymi
Projekt zgodny z celem głównym Programu CSI: *Podniesienie poziomu bezpieczeństwa cyberprzestrzeni RP przez zwiększenie dostępności narzędzi sprzętowo-programistycznych do roku 2023*, przyczyniający się do jego realizacji oraz realizacji 2. Celu szczegółowego Programu: *Wdrożenie metod i technik identyfikacji i uwierzytelniania*, obejmujący II temat badawczy - *Technologie i rozwiązania w zakresie tożsamości cyfrowej z uwzględnieniem aspektów prywatności.*
Zrealizowany poziom wskaźników (% osiągnięcia planowanej wartości)
Wskaźniki rezultatu: 1. Liczba wprowadzonych do użytku egzemplarzy produktów, powstałych w wyniku wdrożenia rezultatów Programu - 100%. 2. Liczba sprzedanych usług, powstałych w wyniku wdrożenia rezultatów Programu - 0% (wskaźnik odnosi się do okresu trwałości). 3. Liczba certyfikatów bezpieczeństwa produktów lub usług, wydanych z wykorzystaniem metodyk opracowanych w Programie - 0% (wskaźnik odnosi się do okresu trwałości). 4. Liczba wdrożonych produkcyjnie rozwiązań technologicznych ułatwiających współpracę i koordynację działań między różnymi domenami bezpieczeństwa - 100%.

5. Liczba wdrożeń komponentów mających zastosowanie w systemach - 0% (zostanie osiągnięty po zakończeniu ewaluacji produktu z tego obszaru - przewidywane w 1 roku okresu trwałości).
6. Przychód beneficjentów z wdrożonych rozwiązań technologicznych w zakresie koordynacji działań między domenami cyberbezpieczeństwa - 0% (wskaźnik odnosi się do okresu trwałości).
7. Udział rozwiązań opracowanych w ramach Programu, w zakresie koordynacji działań między domenami cyberbezpieczeństwa generujących przychody w stosunku do liczby wdrożonych rozwiązań - 0% (wskaźnik odnosi się do okresu trwałości).
8. Liczba prac przyjętych do prezentacji na konferencjach z listy stanowiącej załącznik nr 19 do Regulaminu lub liczba publikacji z części A wykazu czasopism naukowych Ministerstwa Nauki i Szkolnictwa Wyższego, związanych tematycznie z programem CyberSecIdent - 33% (wskaźnik odnosi się do okresu trwałości).

Wskaźniki produktu:

1. Metody i techniki weryfikacji bezpieczeństwa dla różnych warstw struktur sprzętowo – programistycznych opartych na międzynarodowych standardach takich jak ISO 15408 oraz opracowanie krajowego schematu certyfikacji – 100%.
2. Metody i techniki weryfikacji bezpieczeństwa modułów kryptograficznych – 100%.
3. Metody i wzorce projektowe security by design dla danych przetwarzanych w systemach teleinformatycznych administracji publicznej – 100%.
4. Metody i wzorce projektowe privacy by design dla danych przetwarzanych w systemach teleinformatycznych administracji publicznej – 50%.

Rezultaty realizacji projektu

Praktyczne rezultaty Projektu KSO3C w zakresie produktów:

- gotowa operacyjnie struktura oceny bezpieczeństwa i prywatności złożona z jednostki certyfikującej i dwóch laboratoriów dokonujących oceny zgodności z Common Criteria oraz europejskimi ramami certyfikacji bezpieczeństwa i prywatności, które były tworzone na moment opracowywania wniosku o dofinansowanie projektu,
- min. 3 autorskie metody i techniki oceny zgodności (w tym ataków i testów penetracyjnych) dla układów scalonych lub podobnych urządzeń kryptograficznych, umożliwiających ocenę bezpieczeństwa na wysokim poziomie uzasadnienia pewności oceny,
- min. 3 autorskie metody testowania modułów lub układów sprzętowo – programowych wyposażonych w tzw. security boxes, na wysokim (powyżej EAL4) poziomie uzasadnienia pewności oceny,
- min. 2 autorskie metody testowania bezpieczeństwa oprogramowania na wysokim (powyżej EAL4) poziomie uzasadnienia pewności oceny.

Rezultaty bezpośrednie charakteryzują się rozpoczęciem operacyjnej działalności opisanej powyżej struktury, bezpośrednio po zakończeniu projektu KSO3C, w tym: wydawaniem certyfikatów (bezpieczeństwa i prywatności), świadczeniem usług komercyjnych, w tym dla sektora obronności i bezpieczeństwa w zakresie opracowywania wymagań bezpieczeństwa oraz testowania produktów ICT, świadczeniem usług w postaci szkoleń, usług doradczych w formułowaniu oraz wdrażaniu wymagań bezpieczeństwa lub prywatności, wspierających zasadę „security by design" i „privacy by design", jak i osiągnięciem potencjału badawczo – rozwojowego dla rozwoju nowych metod i technik oceny bezpieczeństwa lub prywatności produktów lub usług teleinformatycznych.

Praktyczne wykorzystanie wyników projektu

- W wyniku realizacji projektu powstała działająca struktura organizacyjna składająca się z jednostki certyfikującej oraz dwóch laboratoriów, akredytowanych w Polskim Centrum Akredytacji, świadczących usługi na światowym poziomie. Powstały w ramach projektu polski schemat oceny i certyfikacji uzyskał też formalny status autoryzowanego uczestnika międzynarodowych porozumień, który wydaje certyfikaty bezpieczeństwa uznawane przez innych uczestników tych porozumień. Wypracowane rozwiązanie kierowane jest do dużych jednostek. W ramach wdrażania rezultatów projektu w praktyce podjęto już pierwsze komercyjne ewaluacje z wykorzystanie powstałego systemu, m.in. z Polską Grupą Zbrojeniową.

Otwarcie w Instytucie Łączności Laboratorium Oceny Bezpieczeństwa Produktów Teleinformatycznych zgodne z normą Common Criteria

Źródło: https://www.kso3c.pl/pierwsze-w-polsce-laboratorium-oceny-bezpieczenstwa-produktow-teleinformatycznych/

Laboratorium Oceny Bezpieczeństwa Produktów Teleinformatycznych w IŁ-PIB otrzymało certyfikat zgodności z PN-EN ISO/IEC 27001


ISOCERT

CERTYFIKAT

SYSTEMU ZARZĄDZANIA

Instytut Łączności - Państwowy Instytut Badawczy

04-894 Warszawa, ul. Szachowa 1

ISOCERT sp. z o.o. zaświadcza, że certyfikowana organizacja wprowadziła i stosuje System Zarządzania Bezpieczeństwem Informacji zgodny z wymaganiami:

PN-EN ISO/IEC 27001:2017-06

Zakres certyfikacji:
działalność laboratoryjna polegająca na ocenie bezpieczeństwa i testowaniu zgodności, realizowana w Laboratorium Oceny Bezpieczeństwa Produktów Teleinformatycznych (LOB)

Wyłączenia: Załącznik A punkty: A.14.2; A.14.3.

Numer certyfikatu: 570491/CH
Data decyzji certyfikacyjnej: 05.01.2023
Data wydania certyfikatu: 05.01.2023

Certyfikat wystawiony przez ISOCERT sp. z o.o.

Tomasz Wycisk
Dyrektor ds. certyfikacji

ISOCERT sp. z o.o., ul. Rysia 1a, 53-650 Wrocław

Źródło: https://www.kso3c.pl/laboratorium-oceny-bezpieczenstwa-produktow-teleinformatycznych-w-il-pib-otrzymalo-certyfikat-zgodnosci-z-pn-en-iso-iec-27001/

Korzyści społeczne i gospodarcze wdrożonych wyników projektu

Korzyści społeczne:

- wzrost zaufania nie tylko przedsiębiorców, ale także osób fizycznych do usług oferowanych na rynku dzięki pojawieniu się polskiej rozpoznawalnej marki certyfikacji bezpieczeństwa produktów IT i uzyskaniu uprawnienia polskiego schematu oceny i certyfikacji do wydawania certyfikatów uznawanych na całym świecie,
- certyfikacja bezpieczeństwa produktów IT uznawana w skali światowej zwiększająca zaufanie polskich i zagranicznych obywateli do tychże produktów,
- ogólna poprawa społecznego odbioru funkcjonowania rozwiązań teleinformatycznych, zwłaszcza w obszarze ich bezpieczeństwa.

Korzyści gospodarcze:

- zwiększenie konkurencyjność polskich produktów IT na rynkach zagranicznych dzięki certyfikacji w schemacie uznawanym międzynarodowo, zgodnie z regulacjami Unii Europejskiej (Dyrektywa NIS, Rozporządzenie eIDAS, normy europejskie dotyczące certyfikacji komponentów infrastruktury inteligentnego opomiarowania i sterowników przemysłowych), a także Ogólnym Rozporządzeniem dotyczącym Ochrony Danych na mocy, którego organizacje zobowiązane są do przeprowadzania oceny skutków dla prywatności (privacy impact assessment),
- popularyzacja w Polsce marki Common Criteria oraz uświadomienia polskim producentom korzyści rynkowych wynikających z oferowania certyfikowanych produktów IT,
- poszerzenie wiedzy polskich producentów IT, w jaki sposób projektować i wdrażać produkty zgodnie z metodyką Common Criteria,
- możliwość świadczenia odpłatnych usług na rzecz producentów i dostawców z innych krajów (zainteresowane podmioty m.in. z Belgii i Czech) w polskim schemacie oceny i certyfikacji przez powstałe w projekcie kwalifikowane laboratoria,
- możliwość uzyskiwania zleceń w kraju i za granicą na specjalizowane badania niezwiązane z systemem certyfikacji przez ww. laboratoria.

Produkty, usługi lub procesy będące rezultatem realizacji projektu

- Gotowa operacyjnie struktura oceny bezpieczeństwa i prywatności złożona z jednostki certyfikującej i dwóch laboratoriów dokonujących oceny zgodności z Common Criteria oraz europejskimi ramami certyfikacji bezpieczeństwa i prywatności.
- Możliwość komercyjnego świadczenia usług przez polskie kwalifikowane laboratoria w polskim schemacie na rzecz producentów i dostawców z innych krajów, a także usług specjalizowanych badań niezwiązanych z systemem certyfikacji na rzecz krajowych i zagranicznych podmiotów.

Czynniki/uwarunkowania wpływające na przebieg realizacji projektu

- Bezpośrednie zaangażowanie się w nadzór nad projektem Ministerstwa Cyfryzacji/resortu odpowiedzialnego kompetencyjnie za obszar cyberbezpieczeństwa w kraju.
- Uczestnictwo w Komitecie Sterującym Programem CSI kierownictwa podmiotów tworzących konsorcjum projektowe.
- Zagraniczny partner - spółka DEKRA z Hiszpani, która w ramach projektu przekazała konsorcjantom know-how w obszarze testowania i certyfikowania.
- Opóźnienia i utrudnienia w projekcie spowodowane były głównie pandemią COVID-19.

Mocne i słabe strony projektu

Mocne strony:

- projekt o charakterze pionierskim, którego rezultat sprawił, że Polska jest w europejskiej czołówce krajów, posiadających uprawniania do wydawania certyfikatów bezpieczeństwa uznawanych na mocy międzynarodowych porozumień,
- projekt realizowano przez wykwalifikowaną kadrę, która dodatkowo dzięki jego realizacji podnosiła kompetencje w specjalistycznym obszarze.

Słabe strony:

- opóźnienia w działaniach projektowych wynikające z pandemii COVID-19 m.in. pilotowe ewaluacje w polskich przedsiębiorstwach nie mogły odbyć się w zaplanowanych terminach, bo firmy te zmagały się ze skutkami obostrzeń wprowadzonych w związku z pandemią COVID-19,

• przedsiębiorcy nie byli wstanie przygotować produktów do pilotażu w założonych terminach ze względu na złożoność dokumentacji niezbędnej do ewaluacji produktu w schemacie bezpieczeństwa, jaki powstał w projekcie, • brak systemowego wsparcia w obszarach: kadrowym, budżetowym i organizacyjnym przy realizacji zadań związanych z certyfikacją bezpieczeństwa produktu i jego ewaluacji, • brak wiedzy i umiejętności polskich przedsiębiorców w zakresie przygotowania *developmentu* i dokumentowania produktu w specyficzny dla schematu sposób, • odmienne cele w związku z projektem poszczególnych członków konsorcjum.
Opis wpływu na realizację założeń Programu CSI wraz z uwzględnieniem perspektywy długotrwałej
Na chwilę obecną 6 krajów w Europie posiada uprawniania do wydawania certyfikatów uznawanych na mocy międzynarodowych porozumień, w tym Polska dzięki rezultatom projektu KSO3C - polski schemat certyfikacji prywatności i bezpieczeństwa wraz z laboratoriami i jednostką certyfikacyjną. Jest to efekt długoterminowy realizacji projektu.

Źródło: opracowanie własne.

Krajowy schemat oceny i certyfikacji bezpieczeństwa oraz prywatności produktów i systemów IT zgodny z Common Criteria (KSO3C)

Cel główny projektu:
Podniesienie poziomu bezpieczeństwa cyfrowego w sektorze publicznym poprzez przygotowanie i pilotażowe uruchomienie modelowego Regionalnego Centrum Bezpieczeństwa Cybernetycznego (RegSOC) dedykowanego dla podmioów publicznym z możliwością rozszerzenia na podmioty niepubliczne.

Cel szczegółowy 1:
Opracowanie rozwiązania sprzetowo-programowego stosowanego w punkcie klienckim - miejscu przyłączenia wewnętrznej sieci informatycznej podmiotu do sieci publicznej (część kliencka-lokalna).

Cel szczegółowy 2:
Opracowanie systemu organizacyjnego i oprogramowania dla funkcjonowania regionalnych centrów cyberbezpieczeństwa integrujących urządzenia klienckie z danego obszaru (część regionalna).

Cel szczegółowy 3:
Opracowanie integracji centrów tegionalnych RegSOC z Narodową Platformą Cyberbezpieczeństwa (NPC) (część materialna).

Rezultat 1:
Klienckie rozwiązanie sprzętowo-programowe, dedykowane dla instytucji publicznych, funkcjonujące zarówno samodzielnie (autonomicznie), pod lokalnym nadzorem administracyjnym oraz pod nadzorem RegSOC.

Rezultat 2:
Platforma monitorowania bezpieczeństwa cyfrowego na potrzeby RegSOC jako rozwiązanie programowe oraz organizacyjne (model zarządzania i procedury operacyjne), służące także integracji i administracji urządzeń klienckich, z bazą sygnatur i informacji o naruszeniach bezpieczeństwa, udostępnianą w celach zwiększenia potencjału systemów obrony oraz dla umożliwienia dalszego budowania wiedzy przez inne podmioty.

Rezultat 3:
Model integracji centrów regionalnych z NCP, w tym model organizacyjno-proceduralny funkcjonowania regionalnych centrów we współpracy z CSIRT NASK oraz wewnętrzne oprogramowanie integrujące.

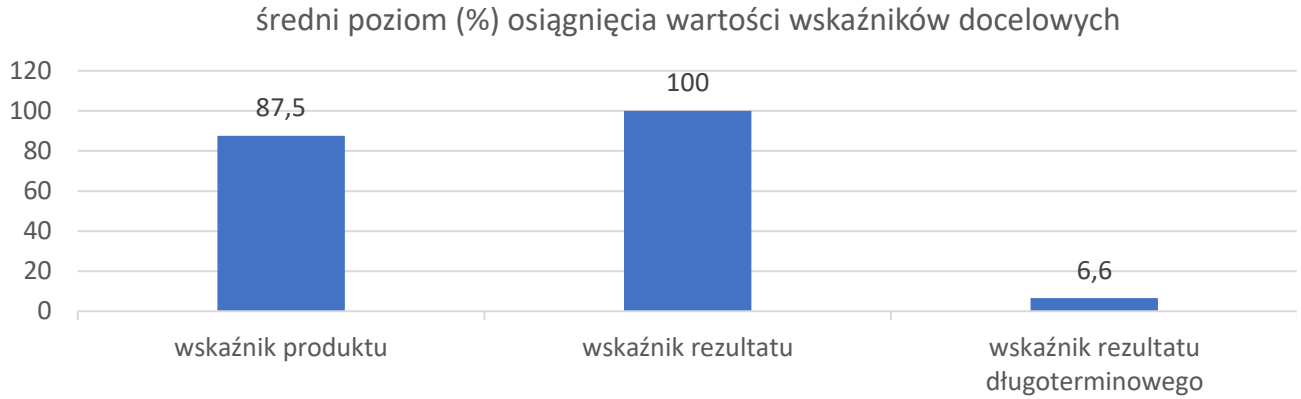
Rezultat 4:
prototypowe RegSOC przy Politechnice Wrocławskiej z komponentami klienckimi wdrożonymi u zainteresowanych podmiotów wspierających projekt.

Wdrażanie efektów w praktyce:

Utworzono polski schemat oceny i certyfikacji (KSO3C) – uruchomiono nowatorskie Laboratorium Oceny Bezpieczeństwa Produktów Informatycznych zgodne z Common Criteria oraz powstał Ośrodek Standaryzacji i Certyfikacji, który ma pełnić funkcję Jednostki Certyfikującej.
Projekt został już zakończony w połowie 2022 roku i aktualnie z powodzeniem przebiega **komercjalizacja jego rezultatów**.
W jego wyniku powstała działająca struktura organizacyjna składająca się z jednostki certyfikującej oraz dwóch laboratoriów, akredytowanych w Polskim Centrum Akredytacji, świadczących usługi na światowym poziomie. Powstały w ramach projektu polski schemat oceny i certyfikacji uzyskał też formalny **status autoryzowanego uczestnika międzynarodowych porozumień, który wydaje certyfikaty bezpieczeństwa** uznawane przez innych uczestników tych porozumień. Wypracowane rozwiązanie kierowane jest do dużych jednostek. W ramach wdrażania rezultatów projektu w praktyce podjęto już pierwsze komercyjne ewaluacje z wykorzystanie powstałego systemu, np. z Polską Grupą Zbrojeniową.

Na chwilę obecną 6 krajów w Europie posiada uprwnienia do wydawania certyfikatów uznawanych na mocy międzynarodowych pozumień, w tym Polska dzięki rezultatom projektu KSO3C.

Krajowy schemat oceny i certyfikacji bezpieczeństwa oraz prywatności produktów i systemów IT zgodny z Common Criteria (KSO3C)



Dobre praktyki

- wsparcie projektu przez Komitet Sterujący Programem CSI,
- zaangażowanie w struktury projektowe dyrektorów wszystkich podmiotów tworzących konsorcjum i nadanie projektowi najwyższej rangi w strukturach konsorcjantów na okres jego realizacji,
- przewidywanie na etapie głównie planowania projektu ryzyk związanych z otoczeniem międzynarodowym i zmiennością międzynarodowych regulacji prawnych,
- udział w grupach opracowujących regulacje prawne dotyczące cyberbezpieczeństwa,
- przygotowanie produktu projektowego i organizacji realizujących projekt do wejścia z nim nie tylko na polski, ale także światowe rynki,
- odpowiedni budżet na promocję rezultatów projektu i kontakty biznesowe, zarówno w kraju, jak i poza jego granicami,
- klarowny, jasny podział zadań i odpowiedzialności za ich rezultaty pomiędzy podmiotami realizującymi projekt w konsorcjum.

Najważniejsze czynniki wpływające na realizację

- ministerialny nadzór nad projektem,
- wysoki priorytet projektu w strukturach konsorcjantów,
- zaangażowanie przedstawicieli ministra odpowiadającego za cyfryzację i kierownictwa konsorcjantów w pracę Komitetu Sterującego Programem CSI,
- środki Programu CSI pozwalające zrealizować projekt w pełnym wymiarze,
- zagraniczny partner przekazujący swoje know-how (DEKRA Hiszpania),
- pandemia COVID-19, jako czynnik powodujący opóźnienia w realizacji projektu.

2. Narodowa Platforma Cyberbezpieczeństwa

Nazwa projektu
Narodowa Platforma Cyberbezpieczeństwa
Cel projektu
Celem projektu było opracowanie kompleksowego, zintegrowanego systemu monitorowania, obrazowania i ostrzegania o zagrożeniach identyfikowanych w czasie zbliżonym do rzeczywistego w cyberprzestrzeni państwa. Wynikiem prac jest prototyp Narodowej Platformy Cyberbezpieczeństwa (NPC) tworzonej przez Centrum Operacyjne i komponenty integrujące z nim uczestników Platformy.
Podmiot/podmioty zaangażowane w realizację
1. Naukowa i Akademicka Sieć Komputerowa NASK – ***Lider konsorcjum*** 2. Politechnika Warszawska 3. Narodowe Centrum Badań Jądrowych 4. Instytut Łączności - Państwowy Instytut Badawczy
Zgodność z celami Programu CSI i określonymi tematami badawczymi
Projekt zgodny z celem głównym Programu CSI: *Podniesienie poziomu bezpieczeństwa cyberprzestrzeni RP przez zwiększenie dostępności narzędzi sprzętowo-programistycznych do roku 2023*, przyczyniający się do jego realizacji oraz realizacji 1. Celu szczegółowego Programu: *wdrożenie rozwiązań technologicznych ułatwiających współpracę i koordynację działań między różnymi domenami bezpieczeństwa cyberprzestrzeni ze szczególnym uwzględnieniem cyfrowej tożsamości*, obejmujący I temat badawczy - *Technologie i rozwiązania w zakresie wykrywania, prezentacji oraz ochrony przed zagrożeniami w cyberprzestrzeni i skutkami ich wystąpienia na poziomie państwa.*
Zrealizowany poziom wskaźników (% osiągnięcia planowanej wartości)
Wskaźniki rezultatu (wpływu długoterminowego): 1. Liczba wprowadzonych do użytku egzemplarzy produktów, powstałych w wyniku wdrożenia rezultatów Programu - 107% 2. Liczba sprzedanych usług, powstałych w wyniku wdrożenia rezultatów Programu - 300% 3. Liczba certyfikatów bezpieczeństwa produktów lub usług, wydanych z wykorzystaniem metodyk opracowanych w Programie - 0% **Wskaźniki rezultatu:** 1. Liczba wdrożonych produkcyjnie rozwiązań technologicznych ułatwiających współpracę i koordynację działań między różnymi domenami bezpieczeństwa – 50%. 2. Przychód beneficjentów z wdrożonych rozwiązań technologicznych w zakresie koordynacji działań między domenami cyberbezpieczeństwa - 310%. 3. Udział rozwiązań opracowanych w ramach Programu, w zakresie koordynacji działań między domenami cyberbezpieczeństwa generujących przychody w stosunku do liczby wdrożonych rozwiązań - 100%. 4. Liczba prac przyjętych do prezentacji na konferencjach z listy stanowiącej załącznik nr 19 do Regulaminu konkursu lub liczba publikacji z części A wykazu czasopism naukowych Ministerstwa Nauki i Szkolnictwa Wyższego, związanych tematycznie z programem CyberSecIdent - 114%

Średni poziom realizacji wskaźników rezultatu – 143,5%

Wskaźniki produktu:

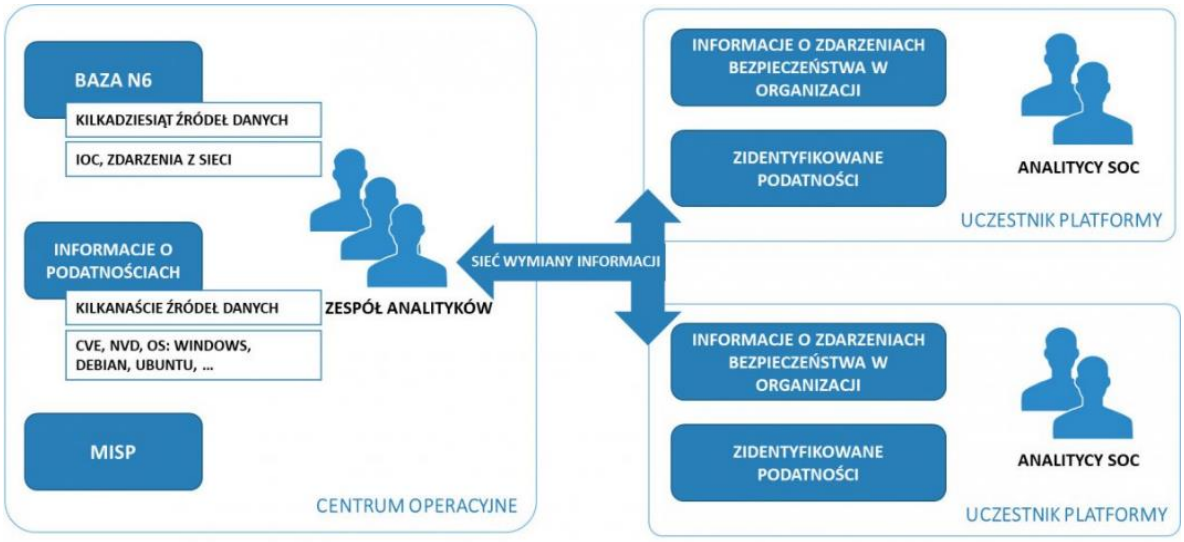
1. Metody skutecznego monitorowania i szybkiej identyfikacji zagrożeń - 150%.
2. Metody i techniki wizualizacji zagrożeń w cyberprzestrzeni - 100%..
3. Metody i techniki obrony przed zmasowanymi atakami z cyberprzestrzeni oraz ochrony prywatności - 100%.
4. Metody i techniki dla postępowania po incydencie - 100%.
5. Dynamiczne i statyczne metodyki szacowania ryzyka - 100%.

Rezultaty realizacji projektu

Praktyczne rezultaty projektu NPC:

- sprawdzony w warunkach operacyjnych prototyp interaktywnego system monitorowania, obrazowania i ostrzegania o zagrożeniach identyfikowanych w czasie zbliżonym do rzeczywistego w cyberprzestrzeni państwa,
- ekspercki system wspierający dobór sektorowych wymagań dla zapewnienia minimalnego poziomu bezpieczeństwa teleinformatycznego w kluczowych sektorach,
- wielomodalny interfejs operatora z wielowymiarowym obrazowaniem zjawisk występujących w przestrzeni cybernetycznej, m.in. uwzględniający różnorodność typów informacji, przynależność sektorową i geograficzną, a także stopień krytyczności prezentowanych zjawisk,
- bazy danych o podatnościach i zagrożeniach bezpieczeństwa w cyberprzestrzeni państwa,
- zbiór innowacyjnych metod, technik i narzędzi detekcji podatności i zagrożeń bezpieczeństwa w sieciach teleinformatycznych, środowisku Internetu Rzeczy i systemach automatyki przemysłowej,
- zbiór innowacyjnych metod i narzędzi korelacji zdarzeń, analizy sytuacyjnej oraz dynamicznej i statycznej analizy ryzyka.

Model współpracy uczestników Narodowej Platformy Bezpieczeństwa



Źródło: https://www.nask.pl/dokumenty/zalaczniki/30/30-2160.jpg

Praktyczne wykorzystanie wyników projektu

- System NCP uzyskał operacyjność z dniem 1 stycznia 2021 r. i jest wykorzystywany w krajowym systemie cyberbezpieczeństwa przez wskazane w Ustawie trzy CSIRT-y poziomu krajowego, Organy Właściwe oraz Operatorów Usług Kluczowych i Dostawców Usług Cyfrowych.
- W infrastrukturze operatorów dołączonych do systemu S46, NASK zainstalował 16 egzemplarzy zintegrowanych urządzeń końcowych (S46-CPE) przeznaczonych do agregacji i wysyłania danych z ich systemów informatycznych do zespołów CSIRT poziomu krajowego.
- W efekcie wdrożenia produkcyjnej wersji systemu NPC, NASK rozpoczął świadczenie 15 usług s46Ehernet VPN oraz s46net na rzecz podmiotów krajowego systemu cyberbezpieczeństwa.
- Metodyka statycznej i dynamicznej analizy ryzyka, będąca autorskim rezultatem projektu, została pozytywnie oceniona przez Departament Cyberbezpieczeństwa b. Ministerstwa Cyfryzacji oraz zalecona do stosowania przez podmioty Krajowego Systemy Cyberbezpieczeństwa w celu określania aktualnego poziomu ryzyka i raportowania jego wartości do Systemu S46.
- Wyniki analiz i badań dotyczących systemów ochrony sieci przed atakami DDoS oraz doświadczenia w tym zakresie pozyskane przez wykonawców projektu zostały wykorzystane przez NASK do wytworzenia nowych usług i produktów cyberbezpieczeństwa. Niektóre z nich, np. FLDX mają już pierwsze wdrożenia (OSE, ABW, KPRM, NASK S.A.).

Korzyści społeczne i gospodarcze wdrożonych wyników projektu

- Podniesienie poziomu cyberbezpieczeństwa RP poprzez wykonanie i wdrożenie kompleksowego, zintegrowanego systemu monitorowania, obrazowania i ostrzegania o zagrożeniach identyfikowanych w czasie zbliżonym do rzeczywistego w cyberprzestrzeni państwa nastąpiło.
- Stworzenie skutecznych i praktycznych mechanizmów ochrony prywatności użytkownika systemu NPC.
- Zapewniono bezpieczne współdzielenie informacji o zagrożeniach w cyberprzestrzeni państwa umożliwiając wczesne ostrzeganie o skali i zasięgu ich oddziaływania, a także podjęcie działań uprzedzających dla ochrony kluczowych podmiotów gospodarczych i obywateli.
- Konsolidacja informacji o zagrożeniach cyberbezpieczeństwa w jednym miejscu, jakim jest system NCP oszczędza czas poświęcany na pozyskiwanie informacji z wielu niezależnych źródeł.
- Wzrost odporności na ataki w obszarze cyberbezpieczeństwa dotyczy wszystkich obywateli, którzy korzystają z usług kluczowych i cyfrowych.

Produkty, usługi lub procesy będące rezultatem realizacji projektu

Produkty:

1. S46/Powered by NPC - kompleksowe rozwiązanie dla zespołów CSIRT Poziomu Krajowego realizujących zadania ustawowe wskazane w UKSC na bazie prototypu systemu NPC, stanowiące innowację na skalę rynku, na którym oferowany jest produkt,
2. S46-CPE - zintegrowane urządzenie końcowe przeznaczone do agregacji i wysyłania danych z systemów informatycznych podmiotów objętych UKSC do zespołów CSIRT poziomu krajowego w zakresie wskazanym w UKSC, stanowiące innowację na skalę jednostki wdrażającej.

Usługi:

1. S46net - usługa polegająca na udostępnianiu zasobów dedykowanej sieci telekomunikacyjnej typu VPN na potrzeby zapewniania komunikacji podmiotów objętych oddziaływaniem UKSC, w szczególności Dostawców Usług Kluczowych i Dostawców Usług Cyfrowych z systemami informatycznymi zespołów CSIRT poziomu krajowego w zakresie wskazanym w UKSC, będąca innowacją na skalę rynku, na którym oferowany jest produkt,
2. S46-EthernetVPN - usługa dedykowanych połączeń telekomunikacyjnych opartych o protokół sieciowy Ethernet na potrzeby organizacji sieci dostępowej do węzłów sieciowych umożliwiających komunikację systemów informacyjnych uczestników KSC z systemami informatycznymi zespołów CSIRT poziomu krajowego w zakresie wskazanym w ustawie, stanowiąca innowację na skalę jednostki wdrażającej.

Czynniki/uwarunkowania wpływające na przebieg realizacji projektu
• Dobrze zdefiniowane założenia projektu. • Ścisły kontakt z Departamentem Cyberbezpieczeństwa - organ państwowy odpowiadający za cyberbezpieczeństwa na bieżąco był informowany, w jakim kierunku zmierzają prace w projekcie, a także wskazywał obszary do korekty. • Prezentowanie rozwiązań projektowych na etapie ich tworzenia kluczowym podmiotom odpowiadającym za bezpieczeństwo państwa - MON, ABW. • Nawiązanie współpracy z podmiotami Krajowego Systemu Cyberbezpieczeństwa – dostawcy i operatorzy cyfrowych usług kluczowych. • Zmiany opiekunów projektu z ramienia NCBR, duża biurokratyzacja, czasochłonność procedur i decyzji po stronie NCBR, brak ogólnodostępnych, gotowych wzorów dokumentacji dotyczącej projektu oraz raportowania jego przebiegu stanowiły główny czynnik utrudniający.
Mocne i słabe strony projektu
Mocne strony: • podmioty, które tworzyły konsorcjum wcześniej ze sobą współpracowały, • wysokie kompetencje zespołu - bogata wiedzę i doświadczenie możliwe do wykorzystania w projekcie, • determinacja w przestrzeganiu harmonogramu pracy, • wzajemne wspieranie się konsorcjantów w przypadku wystąpienia trudności w realizacji zadań/etapów projektu u któregoś z nich. Słabe strony: • konsorcjanci samodzielnie nawiązywali kontakty z dużymi podmiotami Krajowego Systemu Bezpieczeństwa i przekonywali je do włączenia się na własny koszt w działania projektu w celu wykonania demonstratora na bazie rzeczywistych możliwości.
Opis wpływu na realizację założeń Programu CSI wraz z uwzględnieniem perspektywy długotrwałej
Wynik projektu jest operacyjnie wykorzystywany do raportowania stanu bezpieczeństwa cyberprzestrzeni na poziomie państwa. System S46 powstały w ramach NCP na bieżąco przedstawia obraz sytuacji zagrożeń w podmiotach, które do niego dołączyły. Efekt jest długoterminowy, ponieważ rozbudowywany system zmierza do objęcia swoim działaniem wszystkich podmiotów istotnych z punktu widzenia cyfrowego bezpieczeństwa Polski.

Źródło: opracowanie własne.

Narodowa Platforma Cyberbezpieczeństwa

Cel projektu:

Podniesienie poziomu cyberbezpieczeństwa Rzeczypospolitej Polskiej przez opracowanie kompleksowego, zintegrowanego systemu monitorowania, obrazowania i ostrzegania o zagrożeniach identyfikowanych w czasie zbliżonym do rzeczywistego w cyberprzestrzeni państwa.

Rezultat 1:
Sprawdzony w warunkach operacyjnych prototyp interaktywnego systemu monitorowania, obrazowania i ostrzegania o zagrożeniach identyfikowanych w czasie zbliżonym do rzeczywistego w cyberprzestrzeni państwa.

Rezultat 2:
Ekspercki system wspierający dobór sektorowych wymagań dla zapewnienia minimalnego poziomu bezpieczeństwa teleinformatycznego w kluczowych sektorach.

Rezultat 3:
Wielomodalny interfejs operatora z wielowymiarowym obrazowaniem zjawisk występujących w przestrzeni cybernetycznej, m.in. uwzględniający różnorodność typów informacji, przynależność sektorową i geograficzną, a także stopień krytyczności prezentowanych zjawisk.

Rezultat 4:
Bazy danych o podatnościach i zagrożeniach bezpieczeństwa w cyberprzestrzeni państwa.

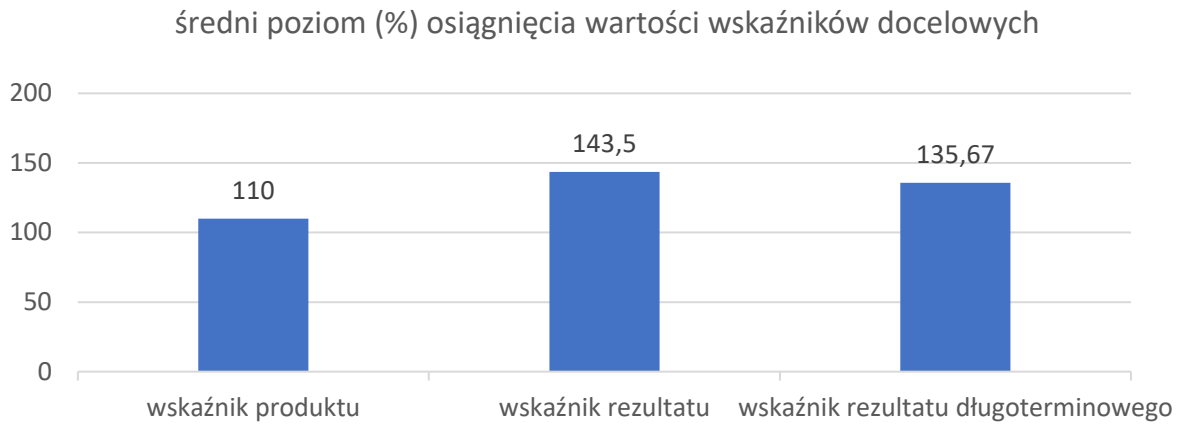
Rezultat 5:
Zbiór innowacyjnych metod, technik i narzędzi detekcji podatności i zagrożeń bezpieczeństwa w sieciach teleinformatycznych, środowisku Internetu Rzeczy i systemach automatyki przemysłowej.

Rezultat 6:
Zbiór innowacyjnych metod i narzędzi korelacji zdarzeń, analizy sytuacyjnej oraz dynamicznej i statycznej analizy ryzyka.

Wdrażanie efektów w praktyce:

Utworzona w projekcie **platforma została istotnym elementem systemu cyberbezpieczeństwa w Polsce.** Została wdrożona przez Ministerstwo Cyfryzacji w Krajowy System Cyberbezpieczeństwa (KSC) i uzyskała operacyjność z dniem 1 stycznia 2021 r. System jest wykorzystywany przez wskazane w ustawie o KSC trzy CSIRT-y poziomu krajowego, organy właściwe oraz operatorów usług kluczowych i cyfrowych. Jego celem jest zapewnienie koordynacji w skali kraju działań służących zapobieganiu, wykrywaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa oraz tworzenie warunków do współdzielenia wiedzy o zagrożeniach z państwami UE.

Narodowa Platforma Cyberbezpieczeństwa



Dobre praktyki

- zbudowanie dobrze współpracującego konsorcjum i kompetentnego zespołu projektowego,
- podzielenie zadań projektowych tak, aby każdy konsorcjant realizował te, w których ma największe kompetencje, doświadczenie i możliwości skutecznej realizacji zakładanych wyników,
- informowanie wszystkich wykonawców projektu o jego bieżącym przebiegu – na jakim etapie jest projekt, jakie wyniki są w nim uzyskiwane, jakie pojawiają się problemy, a także które wyniki projektu należy na dany moment tj. jeszcze przed zakończeniem projektu szczególnie promować,
- dobra współpraca wykonawców – w kulminacyjnym momencie liczba wykonawców wynosiła ponad 100 osób,
- dobra organizacja pracy zespołu i jego determinacja m.in. w przestrzeganiu harmonogramu projketu.

Najważniejsze czynniki wpływające na realizację

- dobrze zdefiniowane założenia projektu,
- ścisły kontakt z Departamentem Cyberbezpieczeństwa - organ państwowy odpowiadający za cyberbezpieczeństwa na bieżąco był informowany, w jakim kierunku zmierzają prace w projekcie, a także wskazywał obszary do korekty,
- prezentowanie rozwiązań projektowych na etapie ich tworzenia kluczowym podmiotom odpowiadającym za bezpieczeństwo państwa - MON, ABW,
- nawiązanie współpracy z podmiotami Krajowego Systemu Cyberbezpieczeństwa – dostawcy ioperatorzy cyfrowych usług kluczowych,
- zmiany opiekunów projektu z ramienia NCBR, duża biurokratyzacja, czasochłonność procedur i decyzji po stronie NCBR, brak ogólnodostępnych, gotowych wzorów dokumentacji dotyczącej projektu oraz raportowania jego przebiegu stanowiły główny czynnik utrudniający.

3. TAMA - skalowalne i wydajne rozwiązanie programistyczne chroniące sieci operatorskie przed atakami typu DDoS (Distributed Denial of Service)

Nazwa projektu
TAMA - skalowalne i wydajne rozwiązanie programistyczne chroniące sieci operatorskie przed atakami typu DDoS (Distributed Denial of Service)
Cel projektu
Celem projektu TAMA było zbudowanie systemu ochrony przed atakami DDoS. System ten został w ramach projektu badawczo-rozwojowego przebadany pod względem technologicznym, zbudowany i przygotowany do wdrożenia pod względem technicznym, biznesowym i prawnym. W okresie trwałości system został wdrożony produkcyjnie w sieci EXATEL i świadczy na rzecz klientów EXATEL usługi anty-DDoS. Uruchomienie usługi we własnej technologii to przełomowy krok w historii EXATEL, dowodzący, że Spółka Skarbu Państwa może być liderem innowacji w obszarze wysokich technologii. Potencjał badawczo-rozwojowy Spółki pozwala na podejmowanie dalszych wyzwań w tym zakresie.
Podmiot/podmioty zaangażowane w realizację
1. Exatel S.A. – ***Lider konsorcjum*** 2. Politechnika Warszawska
Zgodność z celami Programu CSI i określonymi tematami badawczymi
Projekt zgodny z celem głównym Programu CSI: *Podniesienie poziomu bezpieczeństwa cyberprzestrzeni RP przez zwiększenie dostępności narzędzi sprzętowo-programistycznych do roku 2023*, przyczyniający się do jego realizacji oraz realizacji 1. Celu szczegółowego Programu: *Wdrożenie rozwiązań technologicznych ułatwiających współpracę i koordynację działań między różnymi domenami bezpieczeństwa cyberprzestrzeni ze szczególnym uwzględnieniem cyfrowej tożsamości*, obejmujący I temat badawczy - *Technologie i rozwiązania w zakresie wykrywania, prezentacji oraz ochrony przed zagrożeniami w cyberprzestrzeni i skutkami ich wystąpienia na poziomie państwa.*
Zrealizowany poziom wskaźników (% osiągnięcia planowanej wartości)
Wskaźniki rezultatu (wpływu długoterminowego): 1. Liczba wprowadzonych do użytku egzemplarzy produktów, powstałych w wyniku wdrożenia rezultatów Programu – 100%. 2. Liczba sprzedanych usług, powstałych w wyniku wdrożenia rezultatów Programu - 436%. **Wskaźniki rezultatu:** 1. Liczba wdrożeń komponentów mających zastosowanie w systemach teleinformatycznych związanych z cyfrową tożsamością - 100%. 2. Liczba prac przyjętych do prezentacji na konferencjach z listy stanowiącej załącznik nr 19 do Regulaminu konkursu lub liczba publikacji z części A wykazu czasopism naukowych Ministerstwa

Nauki i Szkolnictwa Wyższego, związanych tematycznie z programem CyberSecIdent – 0% (zgodnie z wnioskiem o dofinansowanie projektu wskaźnik zostanie osiągnięty po 3 latach od daty zakończenia realizacji projektu)

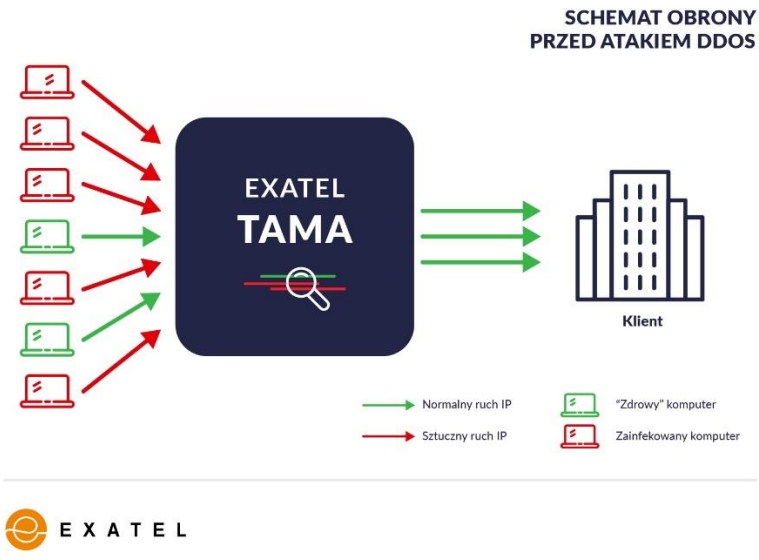
Wskaźniki produktu:

1. Metody skutecznego monitorowania i szybkiej identyfikacji zagrożeń - 100%.
2. Metody i techniki wizualizacji zagrożeń w cyberprzestrzeni - 100%.
3. Metody i techniki obrony przed zmasowanymi atakami z cyberprzestrzeni oraz ochrony prywatności - 100%.

Rezultaty realizacji projektu

- Opracowanie nowego rozwiązania programistycznego chroniącego sieci operatorskie przed atakami DDoS, które może być produkcyjnie wdrażane na przygotowanej platformie sprzętowej i łatwo skalowalne.
- Na bazie ww. rozwiązania świadczone są usługi klientom z sektora publicznego i komercyjnego. Rozwiązanie zalicza się do grupy nowoczesnych technologii i innowacyjnych rozwiązań w zakresie wykrywania, prezentacji oraz ochrony przed zagrożeniami w cyberprzestrzeni i skutkami ich wystąpienia - dzięki posiadaniu autorskich mechanizmów i technik zawierających elementy uczenia maszynowego. W oprogramowaniu zaimplementowano adaptacyjne algorytmy heurystyczne, umożliwiające automatyczne identyfikowanie zagrożeń w sieci oraz ich mitygację bez konieczności ingerencji operatora.
- Dzięki otwartości rozwiązania oprogramowanie można rozszerzać o nowe algorytmy np. wykorzystujące sieci neuronowe lub algorytmy genetyczne. Skalowalność rozwiązania nie wymaga dedykowanych urządzeń producentów a jedynie standardowego sprzętu komputerowego.
- Rozwiązanie, dzięki ekonomicznie skalowalnej wydajności, pozwala na ochronę ruchu o dużej przepustowości, tj. osiągające i przekraczające 100 Gb/s.
- Realizacja projektu we współpracy z Politechniką Warszawską przyczyniła się do wymiany bieżącej wiedzy dziedzinowej, oraz pozwoliła na wykorzystanie infrastruktury badawczej PL-LAB2020 do przeprowadzenia badań i symulacji w kluczowych obszarach badawczych z dziedziny ICT.
- Opracowane w projekcie rozwiązanie otworzyło nowe obszary badawcze dla zainteresowanych jednostek Politechniki Warszawskiej, jak i pobudziło aktywności badawczą w obszarze ICT w ramach Spółki EXATEL.

Schemat obrony przed atakami DDoS zapewnianej przez system TAMA



Źródło: https://biznesalert.pl/exatel-politechnika-warszawska-anty-ddos-cyberbezpieczenstwo/

Praktyczne wykorzystanie wyników projektu

- W wyniku projektu usługa ochrony DDoS, którą otrzymują klienci usług bezpieczeństwa EXATEL, jest w kilkudziesięciu przypadkach świadczona przy użyciu rozwiązania TAMA.
- Pełna specyfikacja zakresu świadczonych usług i objętych nimi podmiotów stanowi dane wrażliwe w EXATEL, ale realizator projektu potwierdza, że są na niej usługi popularne, o dużym wpływie społecznym.
- Usługi DDoS będą oferowane przez EXATEL w ramach pakietu usług bezpieczeństwa, ponieważ klienci rzadko kiedy decydują się tylko na ochronę DDoS, tym bardziej że w przypadku EXATEL usługi bezpieczeństwa i tak najczęściej występują w pakiecie z usługami telekomunikacyjnymi.
- Odbyła się rewizja wszystkich umów klienckich, zostały one przeanalizowane od strony prawnej, pogrupowane, przenegocjowane i aneksowane pod kątem wykorzystania rozwiązania TAMA.
- Projekt TAMA był intensywnie promowany we wszystkich kanałach mediowych EXATEL.

Korzyści społeczne i gospodarcze wdrożonych wyników projektu

Korzyści społeczne:

- usługi ochrony przez atakami DDoS są ważnym czynnikiem obrony cyberprzestrzeni, ponieważ ich skutki, o ile atak się powiedzie, powodują wyłączenie usług, a niedostępność usług informacyjnych, mediów społecznościowych, usług finansowych, bankowych i bezpieczeństwa publicznego (np. OST 112) zwiększa poczucie zagrożenia wśród obywateli.

Korzyści gospodarcze:

- całkowite uzależnienie od zagranicznych technologii ICT wystawiło społeczeństwo polskie na zagrożenia płynące np. z przerwania ciągłości łańcucha dostaw - system TAMA daje w tym względzie autonomię technologiczną,
- zdolność do budowy systemu TAMA stanowi sygnał na skalę globalną świadczący o zdolności Polski do autonomizacji technologicznej.

Produkty, usługi lub procesy będące rezultatem realizacji projektu

Usługa ochrony anty-DDoS TAMA – mająca na celu ochronę infrastruktury klienta przed atakami DDoS (distributed denial of service), które mogą wywołać przeciążenie zasobów sieciowych i serwerowych sieci ICT. Usługa ta stanowi innowację na skalę rynku, na jakim oferowany jest produkt.

Czynniki/uwarunkowania wpływające na przebieg realizacji projektu

- Wykwalifikowane zasoby kadrowe – zarówno te posiadane przez lidera projektu przed rozpoczęciem projektu, jak i pozyskane w trakcie jego realizacji i formowania zespołu projektowego.
- Zasoby techniczne jakim dysponowali konsorcjanci.
- Nawiązanie współpracy z jednostką naukową – Politechnika Warszawska, wspólna realizacja projektu i wymiana doświadczeń w ramach konsorcjum projektowego.

Mocne i słabe strony projektu

Mocne strony:

- sprawna współpraca z konsorcjantem oparta na jasnych zasadach i podziale zadań spisanych w umowie konsorcjum, a także okresowych spotkania konsorcjantów,
- kadra merytoryczna projektu.

Słabe strony:

• zbyt mała elastyczności ze strony NCBR na zmiany, jakich wymagał projekt w trakcie jego realizacji i długi czas udzielania na nie zgód powodujący opóźnienia w harmonogramie.
Opis wpływu na realizację założeń Programu CSI wraz z uwzględnieniem perspektywy długotrwałej
W projekcie stworzono system ochrony przed atakami DDoS (TAMA) – rozwiązanie programistyczne chroniące przed atakami typu DDoS, udostępnione zarówno podmiotom publicznym, jak i prywatnym. Dzięki temu, polskie podmioty nie muszą opłacać zagranicznych licencji. Efekty projektu będą długotrwałe pod warunkiem ich stałego rozwijania pod kątem ciągle rozwijających się metod stosowania/działania ataków DDoS.

Źródło: opracowanie własne.

TAMA - skalowalne i wydajne rozwiązanie programistyczne chroniące sieci operatorskie przed atakami typu DDoS

Cel projektu:

Opracowanie nowego rozwiązania programistycznego chroniącego sieci operatorskie przed atakami DDoS, które będzie mogło być produkcyjnie wdrażane na przygotowanej platformie sprzętowej i łatwo skalowalne. Na jego bazie świadczone będą usługi klientom z sektora publicznego i komercyjnego.

Rezultat 1:
Opracowanie nowego rozwiązania programistycznego chroniącego sieci operatorskie przed atakami DDoS, które może być produkcyjnie wdrażane na przygotowanej platformie sprzętowej i łatwo skalowalne.

Rezultat 2:
Na bazie ww. rozwiązania świadczone są usługi klientom z sektora publicznego i komercyjnego. Rozwiązanie zalicza się do grupy nowoczesnych technologii i innowacyjnych rozwiązań w zakresie wykrywania, prezentacji oraz ochrony przed zagrożeniami w cyberprzestrzeni i skutkami ich wystąpienia - dzięki posiadaniu autorskich mechanizmów i technik zawierających elementy uczenia maszynowego. W oprogramowaniu zaimplementowano adaptacyjne algorytmy heurystyczne, umożliwiające automatyczne identyfikowanie zagrożeń w sieci oraz ich mitygację bez konieczności ingerencji operatora.

Rezultat 3:
Dzięki otwartości rozwiązania oprogramowanie można rozszerzać o nowe algorytmy np. wykorzystujące sieci neuronowe lub algorytmy genetyczne. Skalowalność rozwiązania nie wymaga dedykowanych urządzeń producentów a jedynie standardowego sprzętu komputerowego.

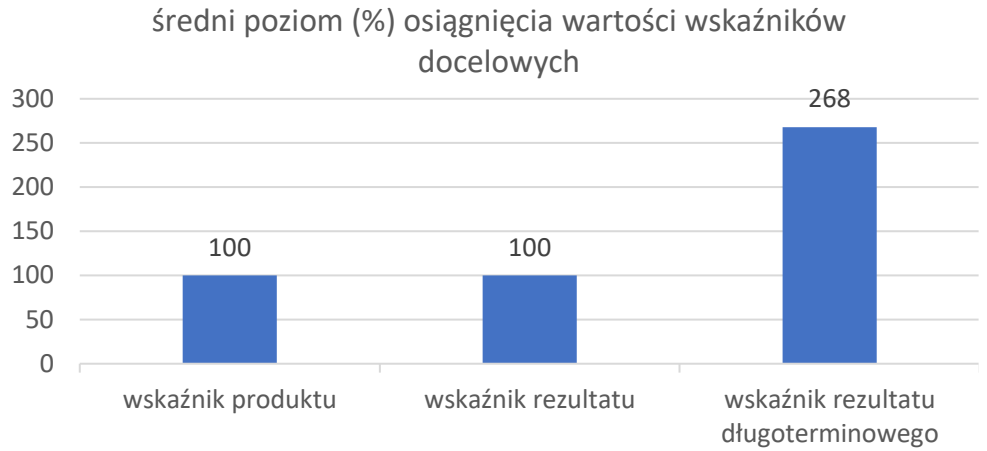
Rezultat 4:
Rozwiązanie, dzięki ekonomicznie skalowalnej wydajności, pozwala na ochronę ruchu o dużej przepustowości, tj. osiągające i przekraczające 100 Gb/s.

Rezultat 5:
Realizacja projektu we współpracy z Politechniką Warszawską przyczyniła się do wymiany bieżącej wiedzy dziedzinowej, oraz pozwoliła na wykorzystanie infrastruktury badawczej PL-LAB2020 do przeprowadzenia badań i symulacji w kluczowych obszarach badawczych z dziedziny ICT.

Wdrażanie efektów w praktyce:

Opracowany system został wdrożony produkcyjnie w sieci EXATEL S.A. i świadczy na rzecz jego klientów **usługi anty-DDoS**. Ustalony plan komercjalizacji powstałego rozwiązania został zrealizowany z sukcesem, co potwierdzają osiągnięte wysokie wartości wskaźników przypisanych do projektu, dotyczące jego wdrażania w praktyce, np. liczba sprzedanych usług, powstałych w rezultacie projektu (436% zakładanej wartości docelowej, według raportu z wdrożenia). Prace nad udoskonaleniem rozwiązania są kontynuowane w ramach innego projektu realizowanego przez EXATEL S.A.

TAMA - skalowalne i wydajne rozwiązanie programistyczne chroniące sieci operatorskie przed atakami typu DDoS



Dobre praktyki

- dobranie odpowiedniego, doświadczonego partnera do projektu,
- właściwy do zakresu i tematyki projektu dobór wykwalifikowanej i doświadocznej kadry naukowej,
- budowa zespołu projektowego przed rozpoczęciem realizacji projektu, tak aby od pierwszych etapów jego realizacji dysponować w pełni kompletnym, kompetentnym zespołem.

Najważniejsze czynniki wpływające na realizację

- wykwalifikowane zasoby kadrowe – zarówno te posiadane przez lidera projektu przed rozpoczęciem projektu, jak i pozyskane w trakcie jego realizacji i formowania zespołu projektowego,
- zasoby techniczne jakim dysponował lider projektu,
- nawiązanie współpracy z jednostką naukową – Politechnika Warszawska, wspólna realizacja projektu i wymiana doświadczeń w ramach konsorcjum projektowego.

4. Regionalne Centrum Bezpieczeństwa Cybernetycznego (RegSOC)

Nazwa projektu

Regionalne Centrum Bezpieczeństwa Cybernetycznego (RegSOC)

Cel projektu

Celem projektu jest przygotowanie i prototypowe uruchomienie w oparciu o wyniki prowadzonych prac B+R modelowego rozwiązania RegSOC na użytek podmiotów publicznych (w tym jednostek administracji rządowej oraz samorządowej) z możliwością rozszerzenia na podmioty niepubliczne.

Podmiot/podmioty zaangażowane w realizację

1. Politechnika Wrocławska – ***Lider konsorcjum***
2. Naukowa i Akademicka Sieć Komputerowa (NASK)
3. Instytut Technik Innowacyjnych EMAG

Zgodność z celami Programu CSI i określonymi tematami badawczymi

Projekt zgodny z celem głównym Programu CSI: *Podniesienie poziomu bezpieczeństwa cyberprzestrzeni RP przez zwiększenie dostępności narzędzi sprzętowo-programistycznych do roku 2023*, przyczyniający się do jego realizacji oraz realizacji 1. Celu szczegółowego Programu: *Wdrożenie rozwiązań technologicznych ułatwiających współpracę i koordynację działań między różnymi domenami bezpieczeństwa cyberprzestrzeni ze szczególnym uwzględnieniem cyfrowej tożsamości*, obejmujący I temat badawczy - *Technologie i rozwiązania w zakresie wykrywania, prezentacji oraz ochrony przed zagrożeniami w cyberprzestrzeni i skutkami ich wystąpienia na poziomie państwa.*

Zrealizowany poziom wskaźników (% osiągnięcia planowanej wartości)

Wskaźniki rezultatu długoterminowego (wpływu):

1. Liczba wprowadzonych do użytku egzemplarzy produktów, powstałych w wyniku wdrożenia rezultatów Programu – 0% (termin osiągnięcia wskaźnika: przed upływem 3 lat od zakończenia projektu; prowadzone są działania zamierzające do osiągnięcia wartości docelowej).

Wskaźniki rezultatu:

1. Liczba wdrożonych produkcyjnie rozwiązań technologicznych i ułatwiających współpracę i koordynację działań między różnymi domenami bezpieczeństwa – 100%.
2. Liczba prac przyjętych do prezentacji na konferencjach z listy stanowiącej załącznik nr 19 do Regulaminu lub liczba publikacji z części A wykazu czasopism naukowych Ministerstwa Nauki i Szkolnictwa Wyższego, związanych tematycznie z programem CyberSecIdent – 83,33% (termin osiągnięcia wskaźnika: przed upływem 3 lat od zakończenia projektu; prowadzone są działania zamierzające do osiągnięcia wartości docelowej).

Wskaźniki produktu:

1. Metody skutecznego monitorowania i szybkiej identyfikacji zagrożeń – 100%.
2. Metody i techniki obrony przed zmasowanymi atakami z cyberprzestrzeni oraz ochrony prywatności – 100%.
3. Metody i techniki dla postępowania po incydencie – 100%.

Rezultaty realizacji projektu

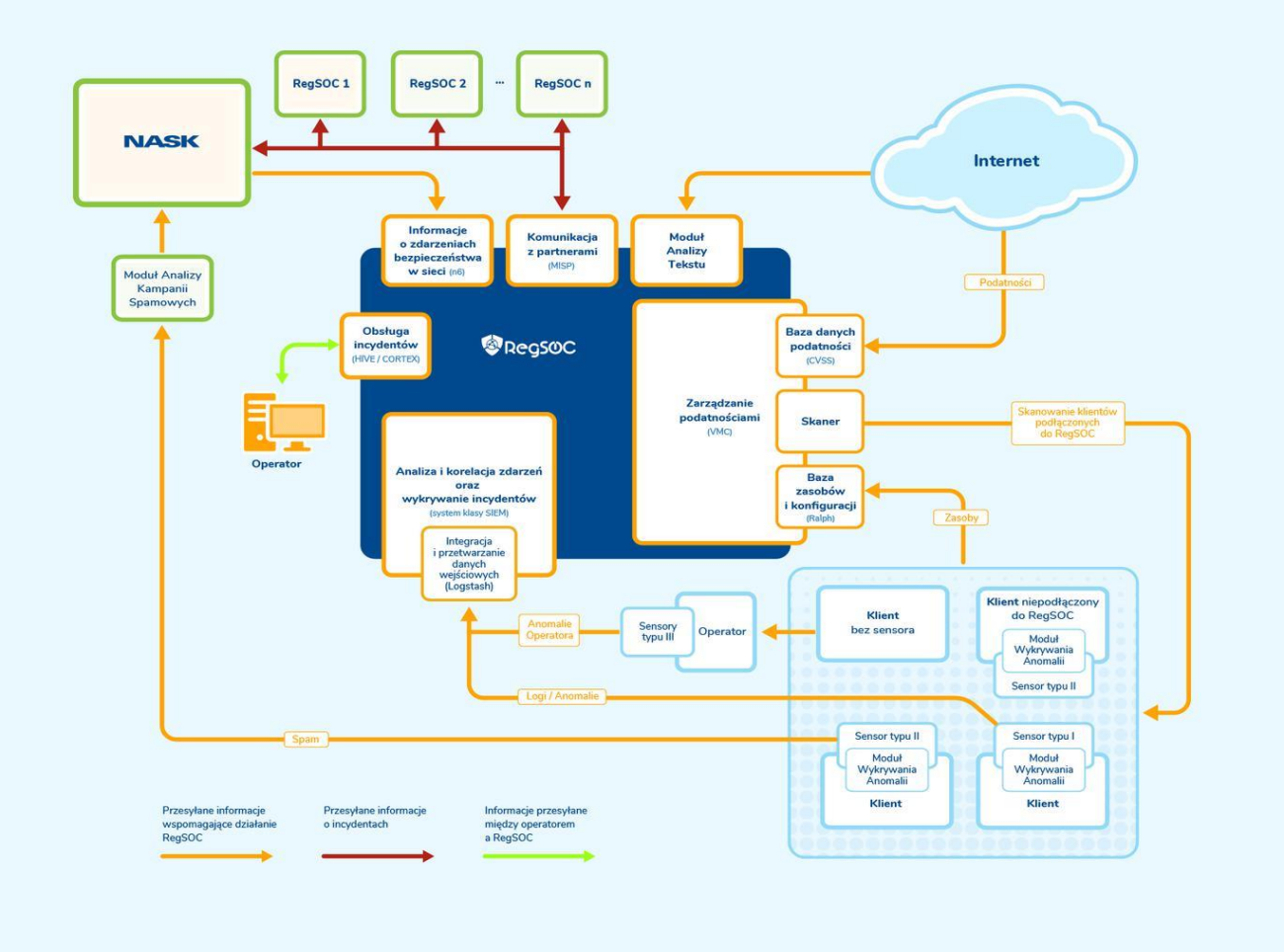
W ramach prowadzonych w projekcie badań przemysłowych, analiz oraz prac rozwojowych opracowano rozwiązanie, w skład którego wchodzą następujące elementy:

- klienckie rozwiązanie sprzętowo-programowe, dedykowane dla instytucji publicznych, funkcjonujące zarówno samodzielnie (autonomicznie), pod lokalnym nadzorem administracyjnym oraz pod nadzorem RegSOC,
- platforma monitorowania bezpieczeństwa cyfrowego na potrzeby RegSOC jako rozwiązanie programowe oraz organizacyjne (model zarządzania i procedury operacyjne), służące także integracji i administracji urządzeń klienckich, z bazą sygnatur i informacji o naruszeniach bezpieczeństwa, udostępnianą w celach zwiększenia potencjału systemów obrony oraz dla umożliwienia dalszego budowania wiedzy przez inne podmioty,
- model integracji centrów regionalnych z NCP, w tym model organizacyjno-proceduralny funkcjonowania regionalnych centrów we współpracy z CSIRT NASK oraz wewnętrzne oprogramowanie integrujące,
- prototypowe RegSOC przy Politechnice Wrocławskiej z komponentami klienckimi wdrożonymi u zainteresowanych podmiotów wspierających projekt,
- raport z realizacji projektu.

Praktyczne wykorzystanie wyników projektu

- Minimalizacji obciążeń masowych sektora publicznego związana z wdrożeniem krajowego systemu bezpieczeństwa informatycznego opartego o rozproszoną infrastrukturę regionalnych centrów cyberbezpieczeństwa.
- Poprawa konkurencyjności polskiej gospodarki, a także jej zrównoważonego rozwoju w aspekcie usług telekomunikacyjych i usług świadczonych drogą elektroniczną, a w szczególności angażujących podmioty publiczne w kontekście prawa publiczno-administracyjnego.
- Poprawa bezpieczeństwa cyfrowego państwa poprzez dostarczenie rozwiązań podnoszących poziom bezpieczeństwa IT w administracji publicznej.
- Zabezpieczenie cyfrowych zasobów i sieci publicznej pozwolające na kontrolowane udostępnianie publicznych zasobów informatycznych w gospodarce.
- Infrastruktura informatyczna oparta o rozwiązanie wypracowane w projekcie funkcjonująca na Politechnice Wrocławskiej.

Komponenty architektury RegSOC i jej integralne otoczenie



Źródło: https://regsoc.pl/offer/8

Korzyści społeczne i gospodarcze wdrożonych wyników projektu

- Korzyści społeczne:
- wdrożenie systemu pozwoli na łatwiejsze, sprawniejsze i niezakłócone korzystanie z szeregu dostępnych cyfrowych usług publicznych osobom fizycznym i firmom,
- korzyści, jakie mogą wynikać dla obywateli i firm w kontaktach z e-administracją (e-usługi publiczne) obejmują: dostępność w jednym miejscu (Internecie), możliwość załatwienia oraz sprawdzenia stanu sprawy w dowolnym miejscu i czasie, umożliwienie osobom z niepełnosprawnościami załatwienia spraw w urzędzie bez potrzeby wychodzenia z domu, nieograniczone godziny urzędowania, korzystanie z jednej bazy dokumentów niezbędnych do korzystania z usług administracji publicznej, ograniczenie konieczności powiadamiania wszystkich urzędów o zmianie danych osobowych, oszczędności materiałowe w firmie,
- do korzyści, jakie ma urząd administracji publicznej można zaliczyć m.in.: usprawnienie i upowszechnienie elektronicznej drogi dostępu do usług administracji publicznej, poprawa wizerunku urzędu, idea „urzędu bardziej przyjaznego obywatelowi", poszerzenie katalogu usług publicznych dostępnych drogą elektroniczną, możliwość korzystania z infrastruktury umożliwiającej wymianę danych pomiędzy urzędami administracji publicznej, standaryzacja wymiany danych, ograniczenie duplikowania czynności, jak również zmniejszenie kosztów funkcjonowania administracji (przesyłanie papierowych dokumentów opatrzonych jak do tej pory tradycyjnymi stemplami i podpisami można zastąpić obiegiem elektronicznym).

Korzyści gospodarcze:

- wymierne oszczędności wynikające z zastąpienia w sektorze publicznym rozwiązań komercyjnych systemem opracowanym w ramach niniejszego projektu,
- grupa oszczędności wynikająca z umożliwienia, dzięki zastosowaniu odpowiednich protokołów bezpieczeństwa, pełniejszego, sprawniejszego i niezakłóconego korzystanie z szeregu cyfrowych usług publicznych,

- oszczędności związane z uniknięciem kar administracyjnych i kosztów odszkodowań wynikających z naruszeń bezpieczeństwa danych.

Produkty, usługi lub procesy będące rezultatem realizacji projektu

Produkty (rozwiązania technologiczne):

1. klienckie rozwiązanie cyfrowo – sprzętowe, dedykowane dla instytucji publicznych, funkcjonujące zarówno samodzielnie (autonomicznie), pod lokalnym nadzorem administracyjnym, oraz pod nadzorem RegSOC,
2. platforma monitorowania bezpieczeństwa cyfrowego na potrzeby RegSOC,- rozwiązanie programowe oraz organizacyjne (model zarządzania oraz procedury operacyjne),
3. model organizacyjno-proceduralny funkcjonowania regionalnych centrów we współpracy z NCCyber oraz wewnętrzne oprogramowanie integrujące RegSOC z Narodową Platformą Cyberbezpieczeństwa (NPC).

Rezultaty wdrożeniowe:

1. modelowe centrum RegSOC przy Politechnice Wrocławskiej z komponentami klienckimi wdrożonymi u zainteresowanych podmiotów,
2. raport z realizacji projektu wskazujący na możliwości techniczne i gospodarcze szerokiego wdrożenia na rynek (w tym międzynarodowy) opracowanego rozwiązania.

Czynniki/uwarunkowania wpływające na przebieg realizacji projektu

- odpowiedni dobór składu konsorcjum - pod kątem zapewniania obszarów kompetencji potrzebnych w projekcie,
- wsparcie projektu na poziomie centralnym w postaci cesji wniosku,
- potencjał badawczy i rozwojowy udostępniony przez Politechnikę Wrocławską połączony z doświadczeniem w badaniach przemysłowych oraz współpracy z biznesem udostępnionymi przez Instytut Technik Innowacyjnych EMAG,
- doświadczenie konsorcjantów jako operatorów telekomunikacyjnych i dostawców usług dla podmiotów publicznych,
- uczestnictwo w projekcie od samego początku jego realizacji jednostek publicznych jako konsultantów,
- zasoby techniczne i infrastruktura informatyczna partnerów udostępniona na potrzeby projektu (m.in. komputery dużej mocy i sieć Politechniki Wrocławskiej).

Mocne i słabe strony projektu

Mocne strony:

- kompetentne, doświadczone w pracy badawczej i operacyjnej z klientami zespoły pracownicze zapewnione przez konsorcjantów,
- stałe monitorowanie przepisów prawa - zgłaszanie swoich rekomendacji do tworzonych przepisów prawa, zgłaszanie luk prawnych, opiniowanie projektów nowelizacji ustaw,
- dobrze ustalone i podzielone pomiędzy konsorcjantami zadania projektowe.

Słabe strony:

- duża rotacja pracowników wśród członków zespołu projektowego – w przypadku ich odejścia, do czasu wdrożenia się nowych osób, powstawała konieczność wydłużania okresu realizacji zadań,
- plan ekonomiczny opłacalności i wdrażania Programu CSI oparty o redukcję kosztów powodował niski wpływ konsorcjantów, pomimo stałej współpracy z Ministerstwem Cyfryzacji, a potem Kancelarią Prezesa Rady Ministrów, na faktyczne wdrażanie rozwiązania projektowego przez krajowe podmioty publiczne i gospodarcze,
- brak wynagrodzenia dla podmiotów testujących rozwiązanie powstające w projekcie.

Opis wpływu na realizację założeń Programu CSI wraz z uwzględnieniem perspektywy długotrwałej

Zadaniem Regionalnego Centrum Cyberbezpieczeństwa jest podniesienie poziomu bezpieczeństwa cyfrowego w sektorze publicznym, głównie w mniejszych, lokalnych urzędach, nie dysponujących odpowiednimi zasobami by chronić się przed atakami hakerów. Rozwiązanie to pozwala uniknąć negatywnych skutków cyberataku (zakłócenia i przestoje

w funkcjonowaniu administracji), pozytywnie wpływa na wizerunek urzędów i minimalizuje ryzyko kar administracyjnych wynikających z naruszenia bezpieczeństwa danych w przypadku ataku. Rezultaty projektu realizują założenia Programu CSI, mając szansę na długoterminowe działanie pod warunkiem wypracowania mechanizmów finansowego wsparcia podmiotów publicznych w ich wdrażaniu.

Źródło: opracowanie własne

Regionalne Centrum Bezpieczeństwa Cybernetycznego (RegSOC)

Cel główny projektu:
podniesienie poziomu bezpieczeństwa cyfrowego w sektorze publicznym poprzez przygotowanie i pilotażowe uruchomienie modelowego Regionalnego Centrum Bezpieczeństwa Cybernetycznego (RegSOC) dedykowanego dla podmioów publicznym z możliwością rozszerzenia na podmioty niepubliczne.

Cel szczegółowy 1:
Opracowanie rozwiązania sprzetowo-programowego stosowanego w punkcie klienckim - miejscu przyłączenia wewnętrznej sieci informatycznej podmiotu do sieci publicznej (część kliencka-lokalna).

Cel szczegółowy 2:
Opracowanie systemu organizacyjnego i oprogramowania dla funkcjonowania regionalnych centrów cyberbezpieczeństwa integrujących urządzenia klienckie z danego obszaru (część regionalna).

Cel szczegółowy 3:
Opracowanie integracji centrów tegionalnych RegSOC z Narodową Platformą Cyberbezpieczeństwa (NPC) (część materialna).

Rezultat 1:
Klienckie rozwiązanie sprzętowo-programowe, dedykowane dla instytucji publicznych, funkcjonujące zarówno samodzielnie (autonomicznie), pod lokalnym nadzorem administracyjnym oraz pod nadzorem RegSOC.

Rezultat 2:
Platforma monitorowania bezpieczeństwa cyfrowego na potrzeby RegSOC jako rozwiązanie programowe oraz organizacyjne (model zarządzania i procedury operacyjne), służące także integracji i administracji urządzeń klienckich, z bazą sygnatur i informacji o naruszeniach bezpieczeństwa, udostępnianą w celach zwiększenia potencjału systemów obrony oraz dla umożliwienia dalszego budowania wiedzy przez inne podmioty.

Rezultat 3:
Model integracji centrów regionalnych z NCP, w tym model organizacyjno-proceduralny funkcjonowania regionalnych centrów we współpracy z CSIRT NASK oraz wewnętrzne oprogramowanie integrujące.

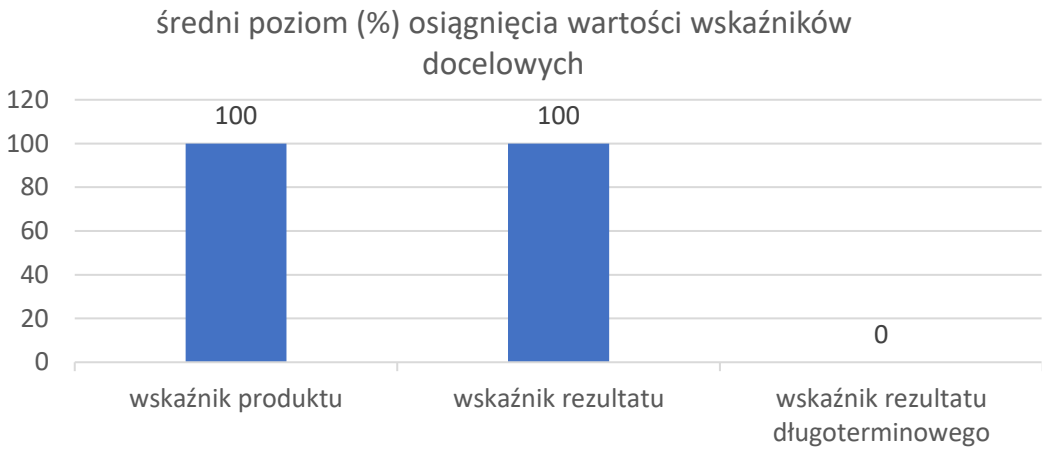
Rezultat 4:
prototypowe RegSOC przy Politechnice Wrocławskiej z komponentami klienckimi wdrożonymi u zainteresowanych podmiotów wspierających projekt.

Rezultat 5:
raport z realizacji projektu.

Wdrażanie efektów w praktyce:

Modelowe centrum RegSOC działające przy Politechnice Wrocławskiej z komponentami klienckimi wdrożonymi u zainteresowanych podmiotów, zainteresowane korzystaniem z rozwiązania powstałego w projekcie jednostki samorządu terytorialnego, szpitale i uczelnie, a także raport z realizacji projektu wskazujący na możliwości techniczne i gospodarcze szerokiego wdrożenia na rynek (w tym międzynarodowy) opracowanego rozwiązania.

Regionalne Centrum Bezpieczeństwa Cybernetycznego (RegSOC)



Dobre praktyki

- konsorcjanci posiadający doświadczenie w obszarach, za których realizację odpowiadają w projekcie,
- praca z klientami – odbiorcami rezultatów projektu w miarę możliwości przez cały okres trwania projektu np. na podstawie listów intencyjnych i podwykonawców wnoszących kolejne jednostki do współpracy.

Najważniejsze czynniki wpływające na realizację

- konsorcjum - pod kątem zapewniania obszarów kompetencji potrzebnych w projekcie,
- wsparcie projektu na poziomie centralnym w postaci cesji wniosku,
- potencjał badawczy i rozwojowy udostępniony przez Politechnikę Wrocławską połączony z doświadczeniem w badaniach przemysłowych oraz współpracy z biznesem udostępnionymi przez Instytut Technik Innowacyjnych EMAG,
- doświadczenie konsorcjantów jako operatorów telekomunikacyjnych i dostawców usług dla podmiotów publicznych,
- uczestnictwo w projekcie od samego początku jego realizacji jednostek publicznych jako konsultantów,
- zasoby techniczne i infrastruktura informatyczna partnerów udostępniona na potrzeby projektu (m.in. komputery dużej mocy i sieć Politechniki Wrocławskiej).