RegSOC – Regionalne Centrum Bezpieczeństwa Cybernetycznego

Konferencja Miasta w Internecie

Bartłomiej Balcerek
Wrocławskie Centrum Sieciowo-Superkomputerowe, Politechnika Wrocławska
Gdańsk, 28 czerwca 2018

Agenda

- Statystyki
- Metryka projektu
- Cel projektu
- Uczestnicy projektu i ich role
- Rezultaty projektu
- Aspekty i obszary badawcze
- Fazy i zadania projektu
- Elementy ekonomiczne

Incydenty w podziale na gałęzie gospodarki

	Incidents				Breaches			
	Total	Small	Large	Unk	Total	Small	Large	Unk
Total	42,068	606	22,273	19,189	1,935	433	278	1,224
Accommodation (72)	215	131	17	67	201	128	12	61
Administrative (56)	42	6	5	31	27	3	3	21
Agriculture (11)	11	1	1	9	1	0	1	0
Construction (23)	6	3	1	2	2	1	0	1
Education (61)	455	37	41	377	73	15	15	43
Entertainment (71)	5,534	7	3	5,524	11	5	3	3
Finance (52)	998	58	97	843	471	39	30	402
Healthcare (62)	458	92	108	258	296	57	68	171
Information (51)	717	57	44	616	113	42	21	50
Management (55)	8	2	3	3	3	2	1	0
Manufacturing (31-33)	620	6	24	590	124	3	11	110
Mining (21)	6	1	1	4	3	0	1	2
Other Services (81)	69	22	5	42	50	14	5	31
Professional (54)	3,016	51	21	2,944	109	37	8	64
Public (92)	21,239	46	20,751	442	239	30	59	150
Real Estate (53)	13	2	0	11	11	2	0	9
Retail (44-45)	326	70	36	220	93	46	14	33
Trade (42)	20	4	10	6	10	3	6	1
Transportation (48-49)	63	5	11	47	14	3	4	7
Utilities (22)	32	2	5	25	16	1	1	14
Unknown	8,220	3	1,089	7,128	68	2	15	51
Total	42,068	606	22,273	19,189	1,935	433	278	1,224

Źródło:
2017 Data Breach Investigations Report, Verizon

Metryka projektu

- Regionalne Centrum Bezpieczeństwa Cybernetycznego (RegSOC)

Program:	**CyberSecIdent - Cyberbezpieczeństwo i e-Tożsamość**
Oś:	
Działanie:	
Konkurs:	**II konkurs w ramach programu: CyberSecIdent - Cyberbezpieczeństwo i e-Tożsamość**
Okres realizacji:	**01.03.2018 – 28.02.2021**

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.
- Projekt dostarczy:
  - Rozwiązania komplementarne z usługami Narodowego Centrum Cyberbezpieczeństwa (NCCyber) jako element realizacji kompleksowego i wielopoziomowego systemu bezpieczeństwa cyberprzestrzeni RP.

Cel projektu

- Cele szczegółowe:
  - Opracowanie rozwiązania sprzętowo-programowego stosowanego w punkcie klienckim - miejscu przyłączenia wewnętrznej sieci informatycznej podmiotu do sieci publicznej (część kliencka – lokalna),
  - Opracowanie systemu organizacyjnego i oprogramowania dla funkcjonowania regionalnych centrów cyberbezpieczeństwa integrujących urządzenia klienckie z danego obszaru (część regionalna),
  - Opracowanie integracji centrów regionalnych RegSOC z NCCyber (część centralna).

Cel projektu

- Wpływ rozwiązań opracowanych w projekcie na podniesienie bezpieczeństwa cyberprzestrzeni
  - Rezultaty projektu w znaczący sposób podniosą poziom bezpieczeństwa w cyberprzestrzeni na wielu płaszczyznach poprzez:
    - wykrywanie i przeciwdziałanie zagrożeniom zewnętrznym oraz atakom na podmioty objęte monitoringiem RegSOC,
    - ochronę przed zagrożeniami wewnętrznymi (ataki z wewnątrz, penetracja sieci, budowanie sieci botnet).
  - Projekt ma umożliwić przygotowanie wzorcowego rozwiązania, następnie adaptowanego i rozszerzanego na kolejne regiony Polski
    - skuteczność obrony będzie rosła wraz ze wzrostem liczby sieci objętych ochroną.

Uczestnicy projektu i ich role

- Konsorcjum RegSOC:

Lider: **Politechnika Wrocławska,**
Partner: Naukowa Akademicka Sieć Komputerowa PIB,
Partner: Instytut Technik Innowacyjnych EMAG,

Politechnika Wrocławska

- Odpowiada za opracowanie rozwiązania dla regionu (platformy i procedur organizacyjnych i operacyjnych), metody analizy zagrożeń i prototypowanie,
- Odpowiada za przygotowanie do wdrożenia.

NASK-PIB

- Odpowiada za opracowanie mechanizmów integracji na poziomie centralnym, proceduralnych i technicznych,
- Uczestniczy w opracowaniu rozwiązań regionalnych. Wsparcie w komunikacji i współpracy z NC Cyber, CERT Polska.

ITI EMAG

- Odpowiada za uwzględnienie wymagań podmiotów niepublicznych,
- Uczestniczy w opracowaniu metod analizy zagrożeń.

Uczestnicy projektu i ich role

- Zainteresowanie i wsparcie (Listy wspierające):

Obszar Samorządowy

Gmina Miejska w Złotoryi (Burmistrz)
Urząd Gminy w Złotoryi (Wójt)
Rejonowe Przedsiębiorstwo Komunalne Spółka z o.o. w

Urząd Miasta i Gminy Lądek-Zdrój

Przedsiębiorcy i stowarzyszenia

Stowarzyszenie na rzecz rozwoju Społeczeństwa Informacyjnego "e-Południe" (przedsiębiorcy)

Śląski Klaster ICT (przedsiębiorcy, j. naukowe, IOB)

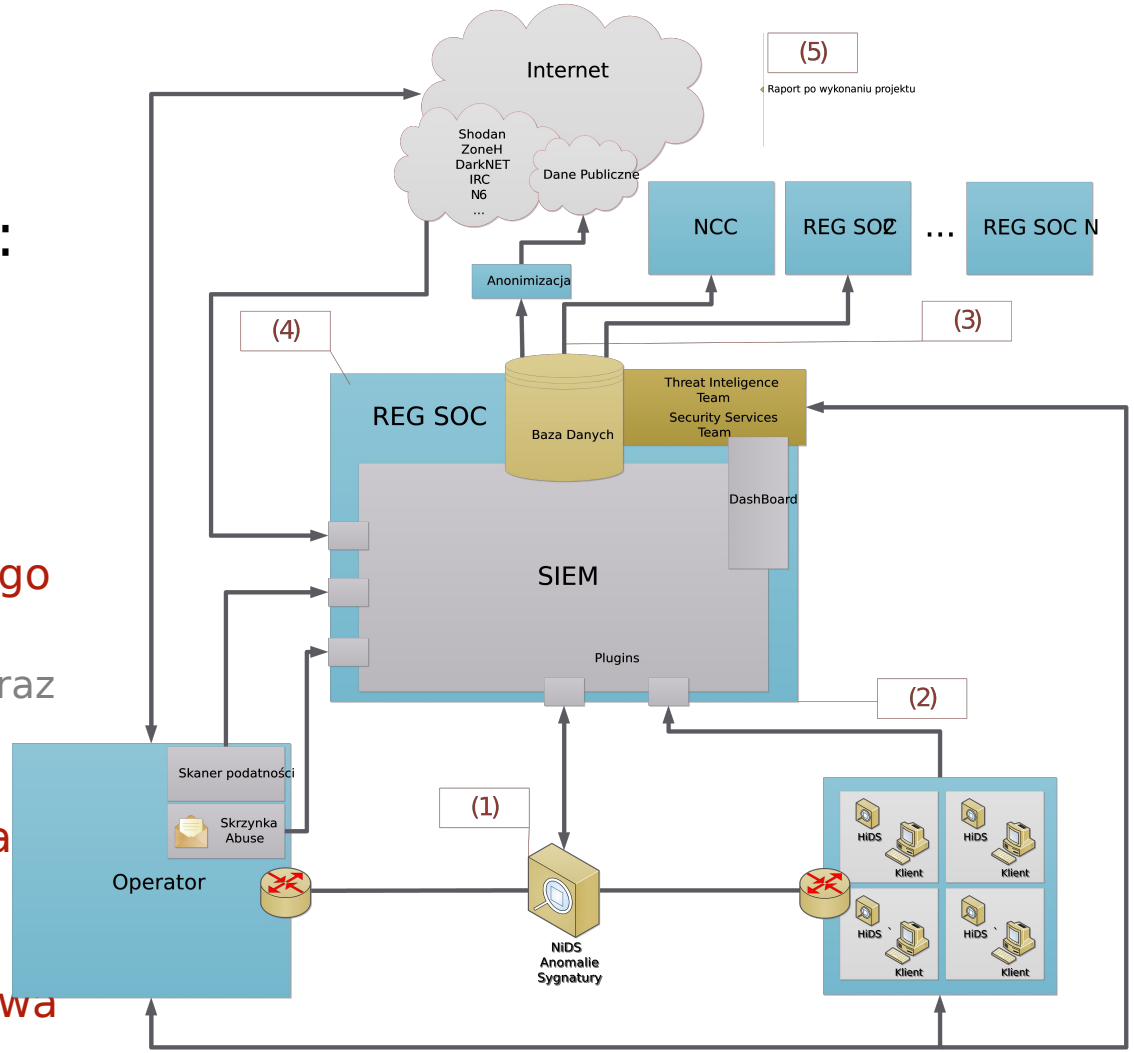
Operatorzy telekomunikacyjni

DSS Operator

Rezultaty projektu

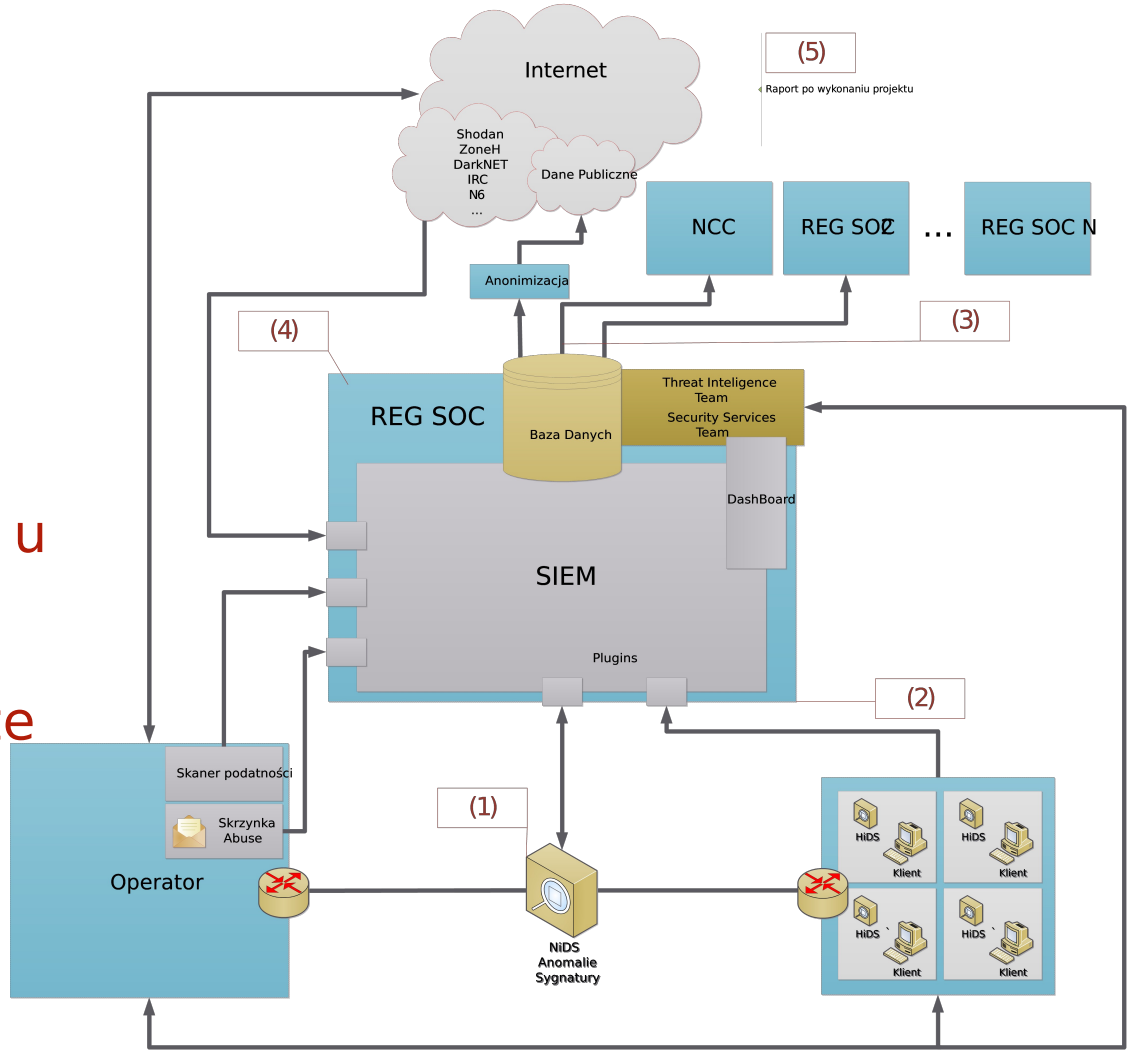
- Produkty (rozwiązania technologiczne):
  - (1) klienckie rozwiązanie cyfrowo – sprzętowe, dedykowane dla instytucji publicznych, funkcjonujące zarówno samodzielnie (autonomicznie), pod lokalnym nadzorem administracyjnym, oraz pod nadzorem RegSOC;
  - (2) platforma monitorowania bezpieczeństwa cyfrowego na potrzeby RegSOC
    - platforma powstanie jako 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 projektu

- Produkty (rozwiązania technologiczne):
  - (4) modelowe centrum RegSOC przy Politechnice Wrocławskiej z komponentami klienckimi wdrożonymi u zainteresowanych podmiotów;
  - (5) raport z realizacji projektu wskazujący na możliwości techniczne i gospodarcze szerokiego wdrożenia na rynek (w tym międzynarodowy) opracowanego rozwiązania.



Aspekty i obszary badawcze

- Obszary badawcze projektu:
  1) Wykrywanie zagrożeń bezpieczeństwa systemów informatycznych z wykorzystaniem metod detekcji anomalii,
  2) Wykrywanie naruszeń bezpieczeństwa na podstawie danych tekstowych,
  3) Śledzenie trwających i identyfikacja nowych kampanii spamowych.

Aspekty i obszary badawcze

1) Wykrywanie zagrożeń bezpieczeństwa systemów informatycznych z wykorzystaniem metod detekcji anomalii

- ✓ planowane w projekcie opracowanie metody wykrywania anomalii na potrzeby diagnozowania poziomu bezpieczeństwa,
- ✓ ma mieć unikalny charakter poprzez uwzględnienie:
  - zmienności monitorowanego środowiska,
  - rzeczywistych, aktualnych danych o naruszeniach bezpieczeństwa,
  - danych o zależnościach pomiędzy podmiotami zarówno na:
    - niskim poziomie charakterystyki systemu (połączenie sieciowe),

    jak i na:
    - poziomie wysokim (powiązania między użytkownikami).

Aspekty i obszary badawcze

2) Wykrywanie naruszeń bezpieczeństwa na podstawie danych tekstowych

- ✓ przeprowadzone zostaną badania i zbudowane zostaną narzędzia do analizy danych tekstowych w celu wykrywania naruszeń zasad bezpieczeństwa oraz procedur ich zastosowania.
  - odtwarzane będą sposoby i ustrukturalizowane procedury przeprowadzonych naruszeń bezpieczeństwa.
  - analiza tekstów języka naturalnego - dla języka angielskiego oraz polskiego.
- ✓ zostaną zaadoptowane aktualnie używane metody:
  - ekstrakcji informacji, tematów, aspektów oraz podstawowych jednostek retorycznych z danych tekstowych,
  - wykrywania nazw własnych,
  - budowania ontologii,
  - reprezentacji tekstów w formie wektorowej,
  - innych technik analizy danych tekstowych oraz sieciowych.
- ✓ wymienione metody zostaną odpowiednio zintegrowane i zmodyfikowane tak, aby uwzględnić:
  - specyfikę źródeł danych (szczególnie Darknet),
  - cel ich pozyskania tj. identyfikację zdarzeń dotyczących bezpieczeństwa.
- ✓ prace dążyć będą do:
  - opracowania nowych metod łączących wiedzę o procedurach naruszeń bezpieczeństwa, systemach IDS (zaawansowane metody przetwarzania języka naturalnego oraz uczenie maszynowe, zwłaszcza nienadzorowane),
  - przeprowadzenia szeregu badań eksperymentalnych na rzeczywistych danych,
  - oszacowania miar jakościowych (zwłaszcza dokładności i kompletności, a także AUC, F-miary) oraz efektywnościowych zaproponowanych metod.

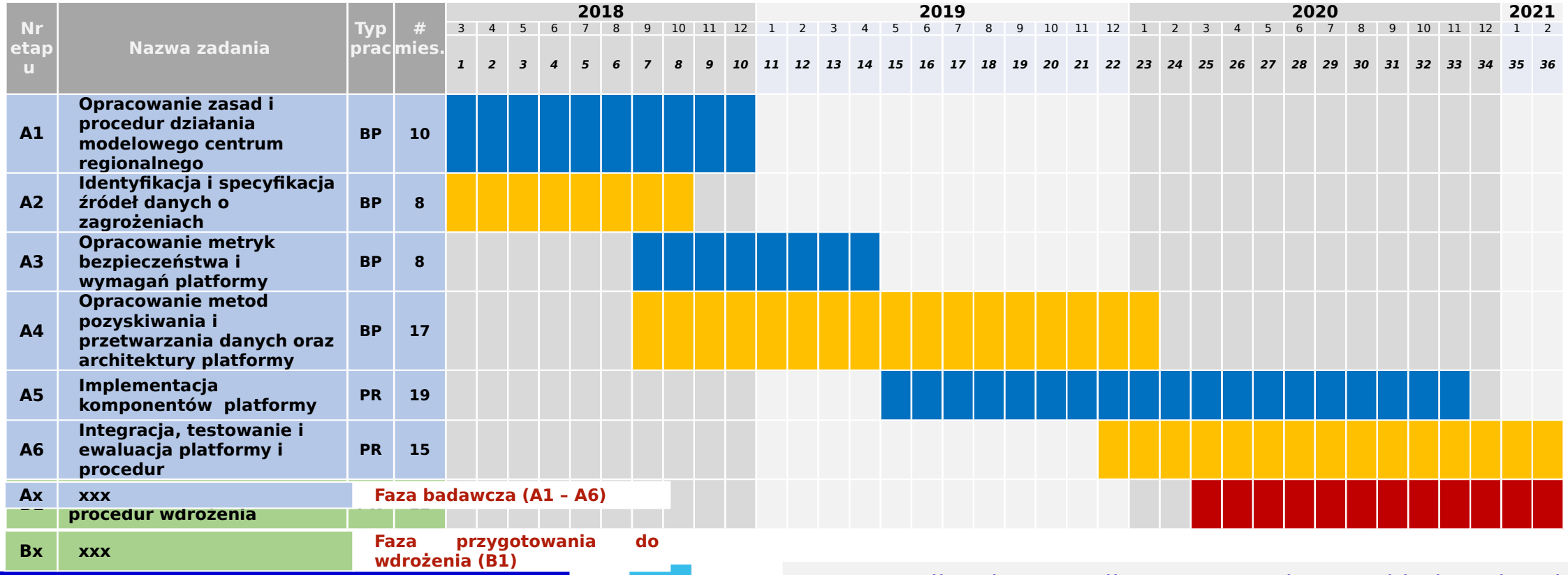
Aspekty i obszary badawcze

3) Śledzenie trwających i identyfikacja nowych kampanii spamowych

- ✓ Opracowane zostaną metody śledzenia trwających i identyfikacji nowych kampanii spamowych (np. phishingowych) dotyczących, lub bezpośrednio celowanych w chronione podmioty, na podstawie korelacji niepożądanych wiadomości
- ✓ W wyniku prac B+R powstanie moduł analizy ww. kampanii spamowych obejmujący:
  - posadowiony w sensorach moduł pobierania danych o kampaniach spamowych,
  - moduł analizy kampanii spamowych na poziomie regionalnym.

Fazy i zadania projektu

- Harmonogram projektu



Fazy i zadania projektu

- Zadania: realizatorzy prac

Faza /Etap		Realizatorzy		
		PWr	NASK-PIB	ITI EMAG
A	Faza badawcza	⊥H	⊥H	⊥H
A 1	Opracowanie zasad i procedur działania modelowego centrum regionalnego	⊟	⊟	⊟
A 2	Identyfikacja i specyfikacja źródeł danych o zagrożeniach	⊟	⊟	⊟
A 3	Opracowanie metryk bezpieczeństwa i wymagań platformy	⊟	⊟	
A 4	Opracowanie metod pozyskiwania i przetwarzania danych oraz architektury platformy	⊟	⊟	⊟
A 5	Implementacja komponentów platformy	⊟	⊟	⊟
A 6	Integracja, testowanie i ewaluacja platformy i procedur	⊟	⊟	⊟
B	Faza przygotowania do wdrożenia	⊥H		

Elementy ekonomiczne

- Model ekonomiczny - oszczędności w trzech zasadniczych grupach:

(1) wynikające z **zastąpienia** w sektorze publicznym rozwiązań komercyjnych systemem opracowanym w ramach niniejszego projektu,

(2) wynikające z **umożliwienia**, dzięki zastosowaniu odpowiednich protokołów bezpieczeństwa,

(3) wynikające z **uniknięcia** kar administracyjnych i kosztów odszkodowań wynikających z naruszeń bezpieczeństwa danych.

Elementy ekonomiczne

- Model ekonomiczny - osiągnięcie oszczędności w trzech zasadniczych grupach:

  (2) wynikające z **umożliwienia**, dzięki zastosowaniu odpowiednich protokołów bezpieczeństwa

  - pełniejsze, sprawniejsze i niezakłócone korzystanie z szeregu cyfrowych usług publicznych.
    - obliczenie korzyści w ramach tej grupy oszczędności jest trudne i opiera się wyłącznie na szacunkach.
    - założony minimalny wskaźnik zwiększenia wykorzystania e-usług publicznych z uwagi na większe bezpieczeństwo na najniższym możliwym poziomie: 1%.
      - ustalany przez poszczególne rządy współczynnik ekonomicznej efektywności publicznych inwestycji ICT, niebiorący pod uwagę korzyści społecznych (Udział całkowitych bezpośrednich korzyści finansowych z tytułu inwestycji w ICT, raportowane przez rządy w 2014), wynosi dla Polski 25-50%

        [*Źródło: OECD, Government at Glance (2015a)*]

Elementy ekonomiczne

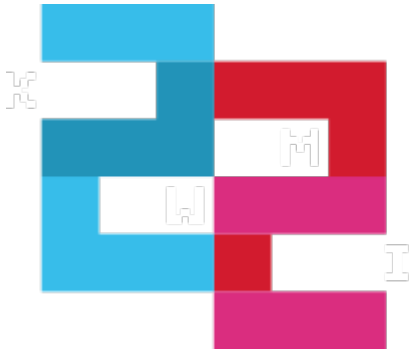
- Model ekonomiczny - osiągnięcie oszczędności w trzech zasadniczych grupach:

(3) wynikające z **<u>uniknięcia</u>** kar administracyjnych i kosztów odszkodowań wynikających z naruszeń bezpieczeństwa danych.

- W zakresie, w jakim nowe przepisy przewidują możliwość nałożenia kary pieniężnej na sektor publiczny, istnieje możliwość nałożenia kary do 100 000 zł za każde naruszenie tajemnicy danych osobowych.
  - Do GIODO wpłynęło 2610 skarg w 2016 r.
  - W porównywalnym roku 2015 wpłynęło ponad 400 skarg na instytucje sektora publicznego.
  - Ryzyko kar jest duże:
    - W toku przeprowadzonych w 2015 r. czynności kontrolnych przez GIODO stwierdzono tylko jeden przypadek stosowania podwyższonego poziomu bezpieczeństwa przetwarzania danych osobowych w publicznych systemach informatycznych !!!
- Redukując zakres potencjalnych oszczędności do naruszeń występujących w sieci teleinformatycznej (15% ogółu), proporcji uznanych skarg (40%) i prawdopodobieństwa wymierzenia kary finansowej (50%) oszczędności netto z tytułu wdrożenia projektu w tym zakresie są szacowane na 1 mln zł rocznie.

[na podstawie: dane statystyczne GIODO (http://www.giodo.gov.pl/pl/1520114/9175) i „Sprawozdanie GIODO 2015”].

Dziękuję za uwagę



22. KONFERENCJA MIASTA W INTERNECIE
27-28 CZERWCA 2018

Konferencja Miasta w Internecie

Bartłomiej Balcerek
Wrocławskie Centrum Sieciowo-Superkomputerowe, Politechnika Wrocławska
Gdańsk, 28 czerwca 2018