Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022 – znaczenie i najbliższe działania

Departament Cyberbezpieczeństwa

Ministerstwo
Cyfryzacji

AGENDA

1. **Cele Krajowych Ram Cyberbezpieczeństwa RP na lata 2017-2022 (KRPC)**
2. **Plan działań na rzecz wdrożenia KRPC**
3. **Główne zadania Planu działań**

Krajowe Ramy Cyberbezpieczeństwa RP na lata 2017-2022

Uchwała nr 52/2017
Rady Ministrów
z dnia 27 kwietnia 2017 r.
w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022

Cele KRPC

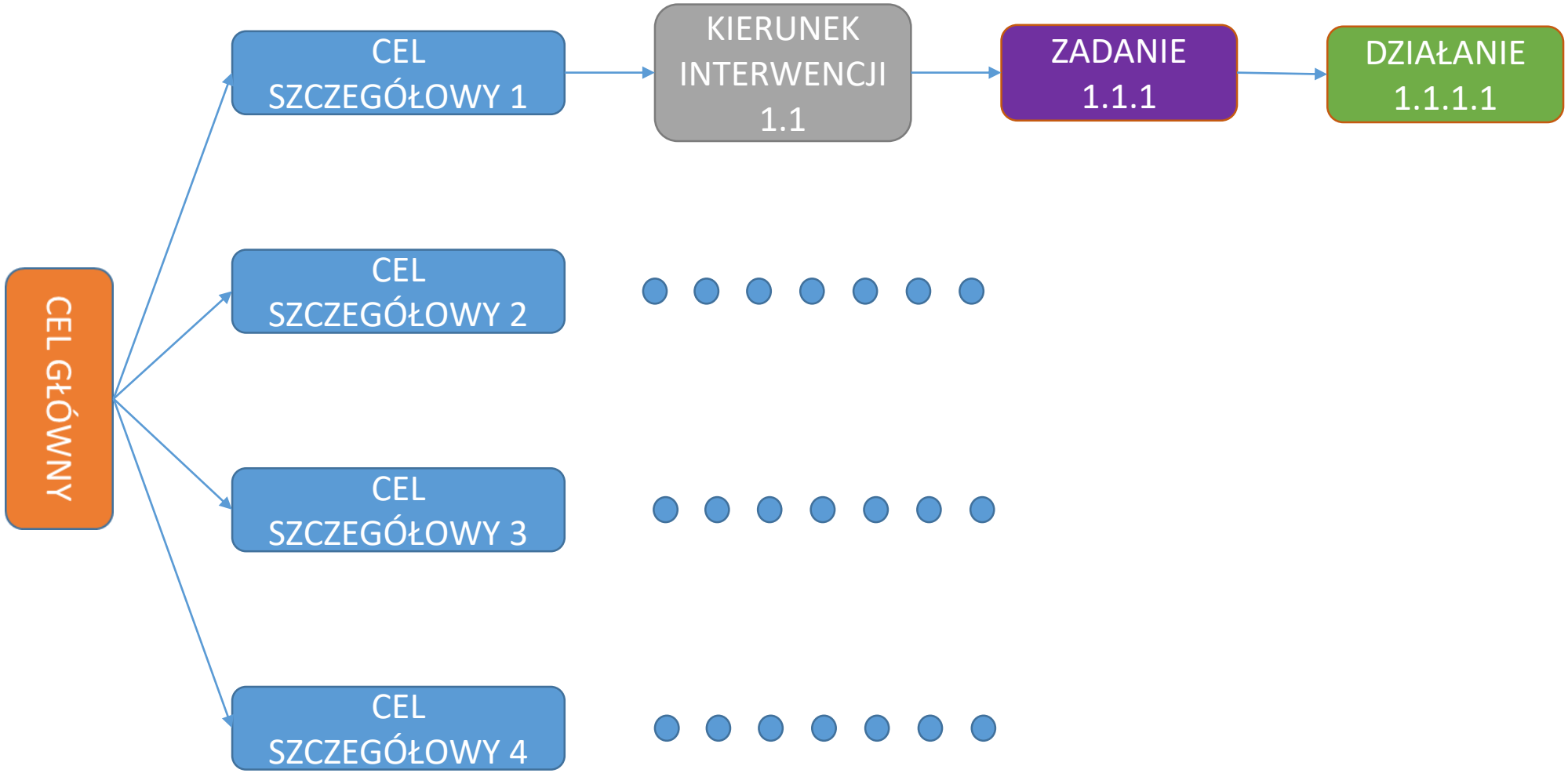

Cel szczegółowy 1.
Osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów . . .
Cel szczegółowy 2.
Wzmocnienie zdolności do przeciwdziałania cyberzagrożeniom
CEL GŁÓWNY
Cel szczegółowy 3.
Zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni
Cel szczegółowy 4.
Zbudowanie silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa.

Plan działań na rzecz wdrożenia KRPC

Plan działań KRPC **będąc <u>dokumentem planistycznym</u> (narzędzie wdrażania KRPC)** przedstawia:

- ramowe obszary interwencji organów administracji rządowej do 2022 roku;
- wykaz zadań służących osiągnięciu celów KRPC;
- wykaz działań w odniesieniu do zidentyfikowanych zadań;
- zagadnienia monitorowania i sprawozdawczości;

Struktura Planu działań na rzecz wdrożenia KRPC



Katalog zadań
Planu działań na rzecz wdrożenia Krajowych Ram Polityki Cyberbezpieczeństwa

Przykład

Kierunek interwencji 1.3. Zwiększenie efektywności współdziałania podmiotów zapewniających bezpieczeństwo cyberprzestrzeni RP	**zadanie 1.3.1** Budowa zintegrowanego systemu wymiany informacji	P
	zadanie 1.3.2 Przygotowanie programu ćwiczeń i treningów w skali kraju i w skali poszczególnych sektorów	P
	zadanie 1.3.3 Aktywny udział w ćwiczeniach prowadzonych zarówno przez organizacje krajowe, podmioty UE i NATO oraz inne podmioty międzynarodowe.	C
	zadanie 1.3.4 Przystąpienie do zaufanych międzynarodowych forów wymiany informacji o zagrożeniach w cyberprzestrzeni.	P

Wykaz działań na rzecz wdrażania Krajowych Ram Polityki Cyberbezpieczeństwa o charakterze projektowym

Przykład

Kierunek interwencji 1.3. Zwiększenie efektywności współdziałania podmiotów zapewniających bezpieczeństwo cyberprzestrzeni RP											
Budowa zintegrowanego systemu wymiany informacji	1.3.1.1 Budowa centralnego modułu zintegrowanego systemu wymiany informacji NPC	T	IX 2017	VIII 2020	System wdrożony w NC Cyber w ramach realizacji projektu Narodowej Platformy Cyberbezpieczeństwa	NASK	MC, IŁ, PW, NCBJ	W ramach projektu NPC (Narodowa Platforma Cyberbezpieczeństwa) powstanie zintegrowany system wymiany informacji o zagrożeniach, incydentach i ryzykach w odniesieniu do cyberprzestrzeni RP	6 000 000 budżet państwa (NCBiR)	16 956 000 (sumaryczna wart. projektu z pkt. 1.3.1, 1.4.2, 1.6.1) budżet państwa (NCBiR)	R
	1.3.1.2 Zaprojektowane wydzielonej sieci NPCnet na potrzeby zintegrowanego systemu wymiany informacji	T	X 2017		Sporządzenie niezbędnej dokumentacji sieci NPCnet	NASK		1. Koncepcja sieci szkieletowej Narodowej Platformy Cyberbezpieczeństwa zawierająca analizę możliwych rozwiązań. 2. Projekt wykonawczy sieci szkieletowej Narodowej Platformy Cyberbezpieczeństwa, szczegółowo opisujący opracowaną koncepcję realizacji sieci szkieletowej. 3. Szczegółowy projekt wykonawczy realizacji podłączeń dla 3 podmiotów 4. Założenia i wytyczne projektowe przyłączeń do sieci szkieletowej Narodowej Platformy Cyberbezpieczeństwa dla pozostałych, podmiotów.	243 485 budżet państwa		P

Wybrane działania Planu KRPC

Ustawa o krajowym systemie cyberbezpieczeństwa

Celem działania jest opracowanie uregulowań prawnych umożliwiających implementacje dyrektywy NIS oraz utworzenie efektywnego systemu bezpieczeństwa teleinformatycznego funkcjonowania państwa

Wybrane działania Planu KRPC

Zbudowanie systemu bieżącego zarządzania bezpieczeństwem cyberprzestrzeni

Celem działania jest objęcie monitorowaniem i korelacją zdarzeń kluczowych usług informatycznych zapewniających bezpieczeństwo funkcjonowania państwa, obywateli i podmiotów gospodarczych, w tym dostarczenie rozwiązań, które umożliwią dostęp do bieżącej informacji o stanie bezpieczeństwa teleinformatycznego niezbędnego do oceny sytuacji i stanu bezpieczeństwa w cyberprzestrzeni w Polsce oraz koordynacji reagowania na incydenty komputerowe na poziomie krajowym

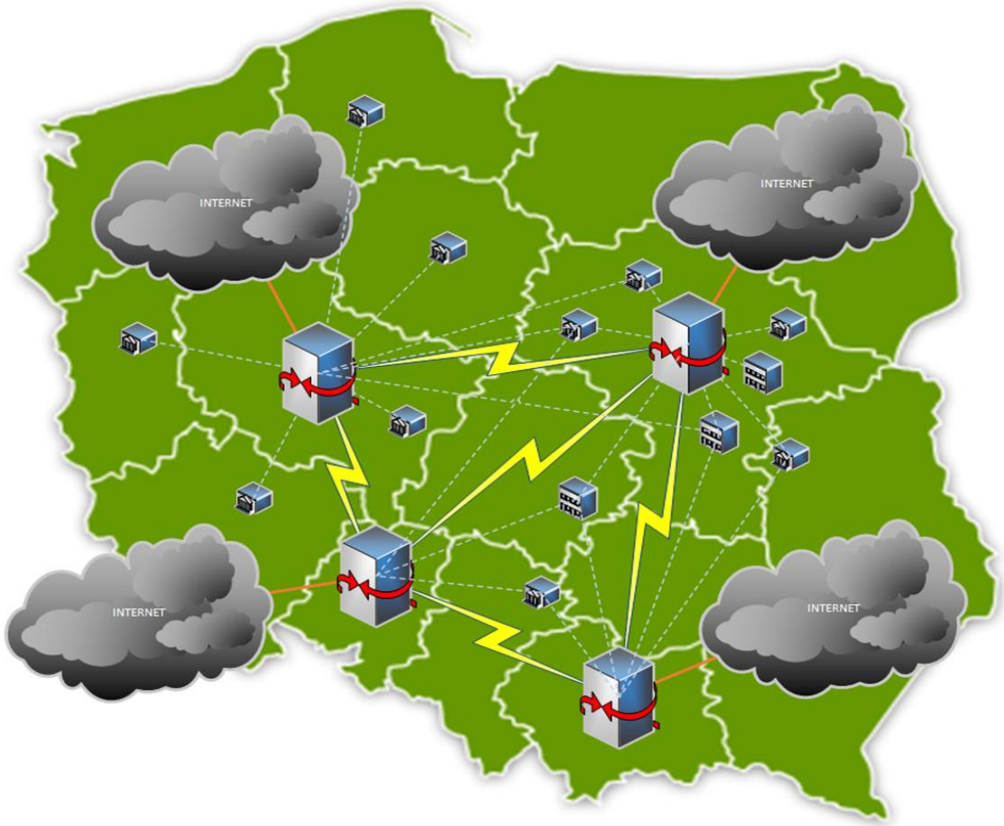
Wybrane działania Planu KRPC

Rządowy Klaster Bezpieczeństwa

Celem działania jest zbudowanie bezpiecznej infrastruktury dla systemów teleinformatycznych państwa składającej się z CPD i rozległej sieci komputerowej umożliwiającej bezpieczne łączenie się podmiotów rządowych pomiędzy sobą, z siecią Internet oraz świadczenie eUsług dla obywateli i przedsiębiorców

Wybrane działania Planu KRPC

Idea rozwiązania



Wybrane działania Planu KRPC

Zbudowanie krajowego systemu oceny i certyfikacji wyrobów sektora IT i uzyskanie pełnego członkostwa w SOGIS MRA

Celem działania jest uzyskanie zdolności do certyfikacji wyrobów sektora TIK według normy PN ISO/IEC 15408 oraz osiągnięcie statusu Polski w porozumieniu SOGIS MRA jako członka wydającego certyfikaty zgodne z Common Criteria, uznawane globalnie

Dziękuję za uwagę

Krzysztof Politowski

Krzysztof.Politowski@mc.gov.pl