



Projekty CPPC jako narzędzie rozwoju kompetencji cyfrowych i cyberbezpieczeństwa w Polsce



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

Piotr Załęcki

p.o. Dyrektora Biura Projektów Własnych
Centrum Projektów Polska Cyfrowa



zdjęcia: Łukasz Prokop

Historia jest prosta: od ryzyka cyfrowego do odporności państwa



Im więcej usług cyfrowych, tym większe znaczenie odporności instytucji

Administracja publiczna opiera się na systemach cyfrowych, a incydenty mogą dotknąć obywateli bezpośrednio.



Usługi publiczne

wnioski online, e-recepty, deklaracje podatkowe



Dane obywateli

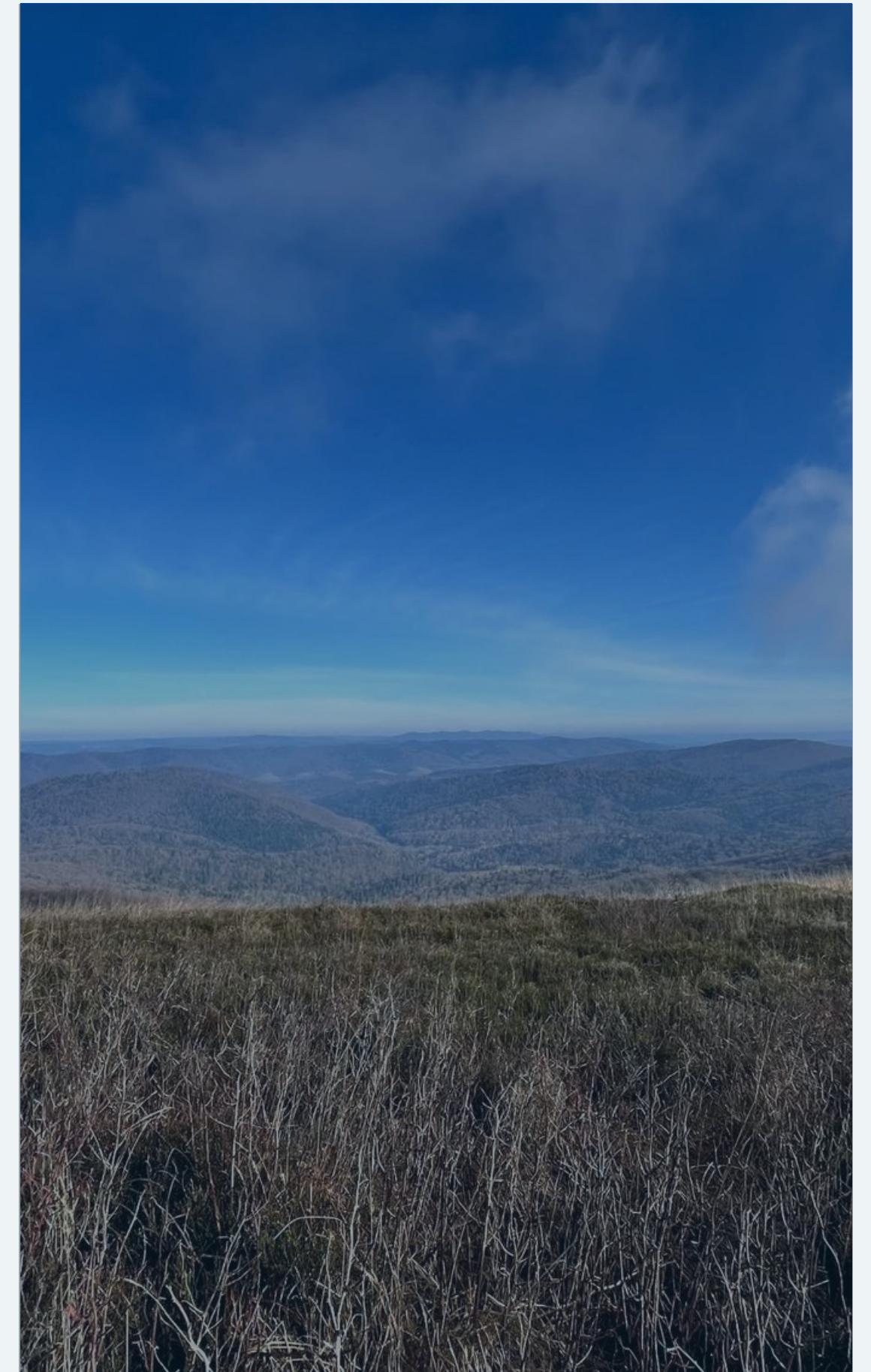
ryzyko wycieku danych i utraty zaufania



Ciągłość działania

awarie i blokady systemów wpływają na obsługę mieszkańców

Cyberbezpieczeństwo nie jest wyłącznie zadaniem technicznym, ale elementem stabilności usług publicznych.



Nasze interwencje pozwalają na kompleksowe podejście

Od lat łączymy poziom centralny i lokalny, a także działamy w obszarach budowy infrastruktury, usług publicznych i edukacji, ponieważ wiemy, że tylko cały komplet i systemowy mechanizm zapewni cyfrowo bezpieczny i nowoczesny kraj.



Cyberbezpieczny Samorząd

granty dla JST
i lokalne procedury
bezpieczeństwa



Cyberbezpieczny Rząd

polityki
bezpieczeństwa,
kompetencje,
infrastruktura IT



Cyberbezpieczne Wodociągi

ochrona
infrastruktury oraz
środowiska IT/OT



Kluby Rozwoju Cyfrowego

świadomość
i bezpieczne nawyki
cyfrowe mieszkańców

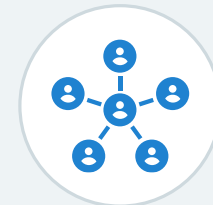
Środki UE to wspólny mianownik tych działań. Wspieramy nie tylko zakup technologii – chcemy tworzyć zamknięty, działający obieg cyfrowej odporności.

Wzmocnienie odporności państwa

Przedsięwzięcie wspiera centralne i naczelne organy administracji rządowej oraz wojewodów.

258,4 mln zł

wartość udzielonego wsparcia w trzech obszarach:



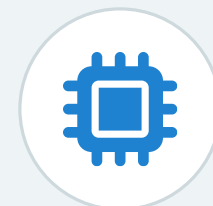
organizacyjny

spójne polityki bezpieczeństwa i procedury



kompetencyjny

większa świadomość i szybsza reakcja



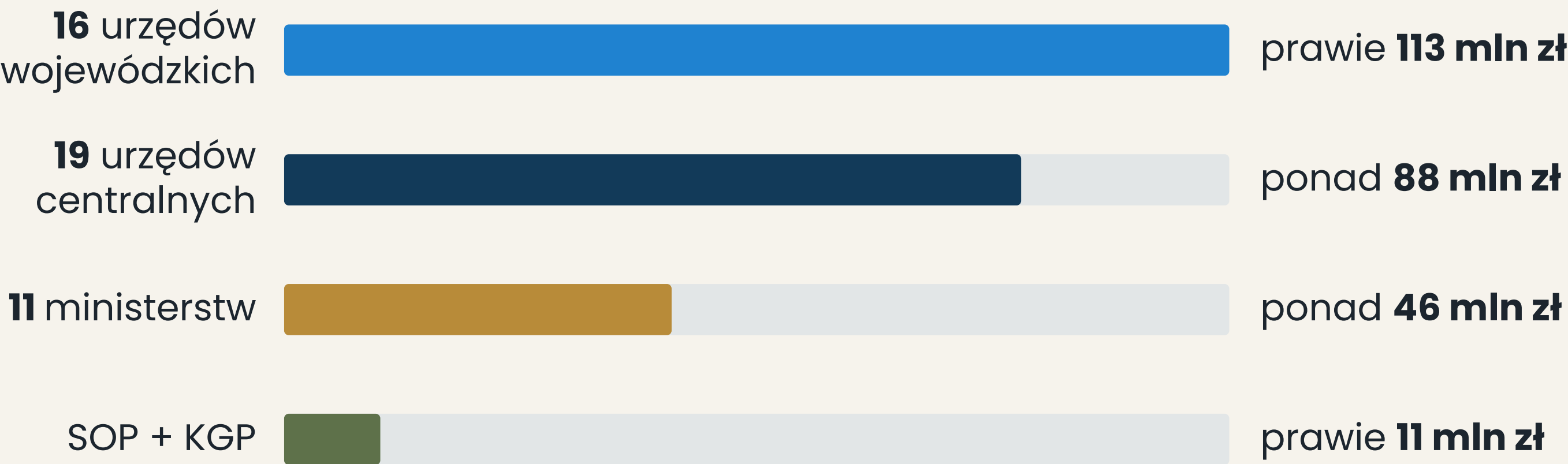
techniczny

nowoczesna i odporna infrastruktura IT

Nasz cel to silne, odporne na zagrożenia cyfrowe państwo.

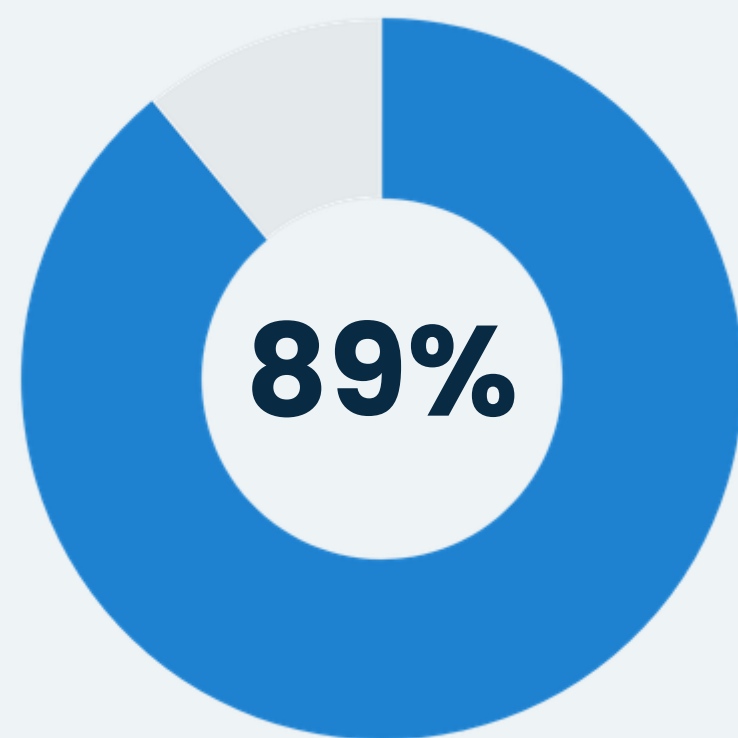
Największe środki trafiły do urzędów wojewódzkich

W podziale instytucjonalnym środki obejmują ministerstwa, urzędy centralne, urzędy wojewódzkie oraz SOP i KGP.



administracja
centralna

Skala programu pokazała realne zapotrzebowanie JST na wsparcie cyberbezpieczeństwa



JST objęte efektem projektu

2 807

podmiotów
uprawnionych
do otrzymania
grantów

2 515

wniosków
w ocenie

2 490

realizowanych umów
z grantobiorcami

Cyberbezpieczeństwo lokalne nie jest dodatkiem do cyfryzacji, to najważniejszy warunek ciągłości usług dla mieszkańców.

Realizowane umowy obejmują wszystkie poziomy samorządu

Wśród 2 490 umów są województwa, powiaty, gminy i miasta na prawach powiatu.

15	województw
298	powiatów
2 177	gmin
64	miasta na prawach powiatu

Struktura gmin



- wiejskie — 1267
- miejsko-wiejskie — 629
- miejskie — 217
- miasta na prawach powiatu — 64

Projekt jest narzędziem systemowym, który objął zarówno duże jednostki, jak i najbliższy obywatelom poziom gminny.

Dane finansowe dla podpisanych umów pokazują dominującą rolę wsparcia publicznego i wkładu UE

1,58 mld zł

wydatki ogółem

1,47 mld zł

dofinansowanie

1,22 mld zł

wkład UE



■ wkład UE · 1 222,8 mln zł ■ wkład BP · 248,4 mln zł ■ wkład własny · 111,7 mln zł

Dofinansowanie
pokrywa

93%

wydatków
ogółem



Samorządy wzmacniają odporność techniczną, organizacyjną i kompetencyjną

Kopie zapasowe

systemy backupu,
magazyny danych,
redundancja

Infrastruktura IT

serwery, wirtualizacja,
sieci, bezpieczne Wi-Fi

Audyty zgodności

Szkolenia z cyberbezpieczeństwa

Monitoring i reakcja

podatności, logi,
korelacja zdarzeń

Ochrona brzegu sieci

firewalle, UTM, ochrona
WWW i poczty

Wdrożenie/aktualizacja SZBI

Fundusze UE wzmacniają odporność tam, gdzie technologia spotyka się z odpowiedzialnością instytucji i użytkowników.

Chronimy infrastrukturę krytyczną

Wsparcie dotyczy zabezpieczenia dostępu do wody, czyli usługi wpływającej bezpośrednio na jakość życia obywateli.



Cyberincydenty mogą przełożyć się na ryzyko przerwy w świadczeniu usługi publicznej.

896

złożonych wniosków

733

podpisane umowy

602,2 mln zł

łączna wartość
realizowanych
projektów

821,6 tys. zł

średnia wartość
grantu/umowy

Działanie usługi zależy od danych, sterowania i ciągłości procesu



IT: kopie zapasowe, kontrola dostępu, monitoring, ochrona sieci i systemów



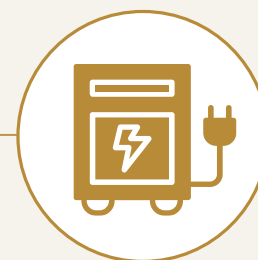
OT: systemy sterowania, SCADA, automatyka, wykrywanie nieprawidłowości



Cyberatak
lub awaria



Zakłócenie
pracy OT i/lub IT



Utrata
monitoringu
lub sterowania



Zakłócenia
uzdatniania lub
pompowania



**Ryzyko
ograniczenia
dostaw wody**

Bezpieczeństwo zaczyna się od edukacji

KRC wzmacniają świadome postawy dorosłych i lokalnych społeczności wobec cyberzagrożeń.



Rozpoznawanie zagrożeń

scamy, phishing, fake newsy



Bezpieczne korzystanie z e-usług

ochrona prywatności, kont i urządzeń



Ochrona danych osobowych

bezpieczne nawyki cyfrowe

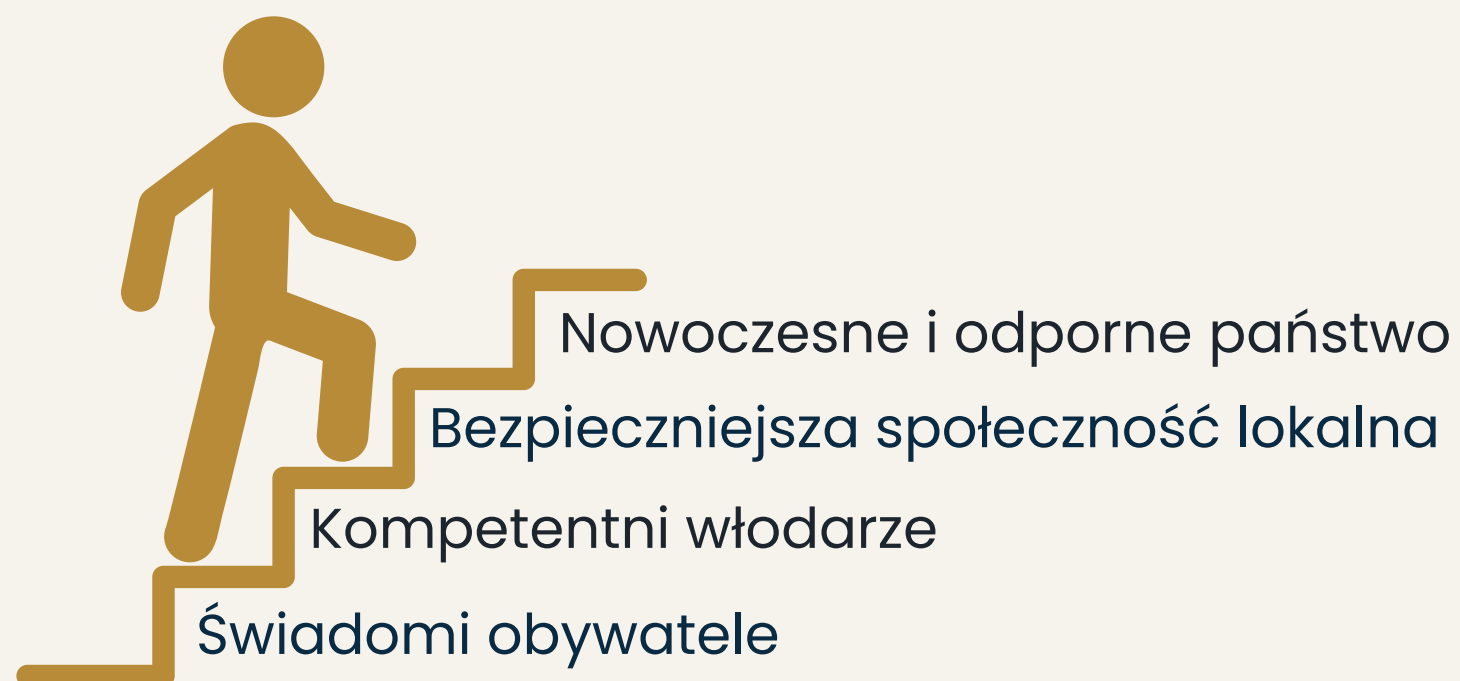


Reakcja na podejrzenie incydentu

właściwe kroki po wykryciu zagrożenia

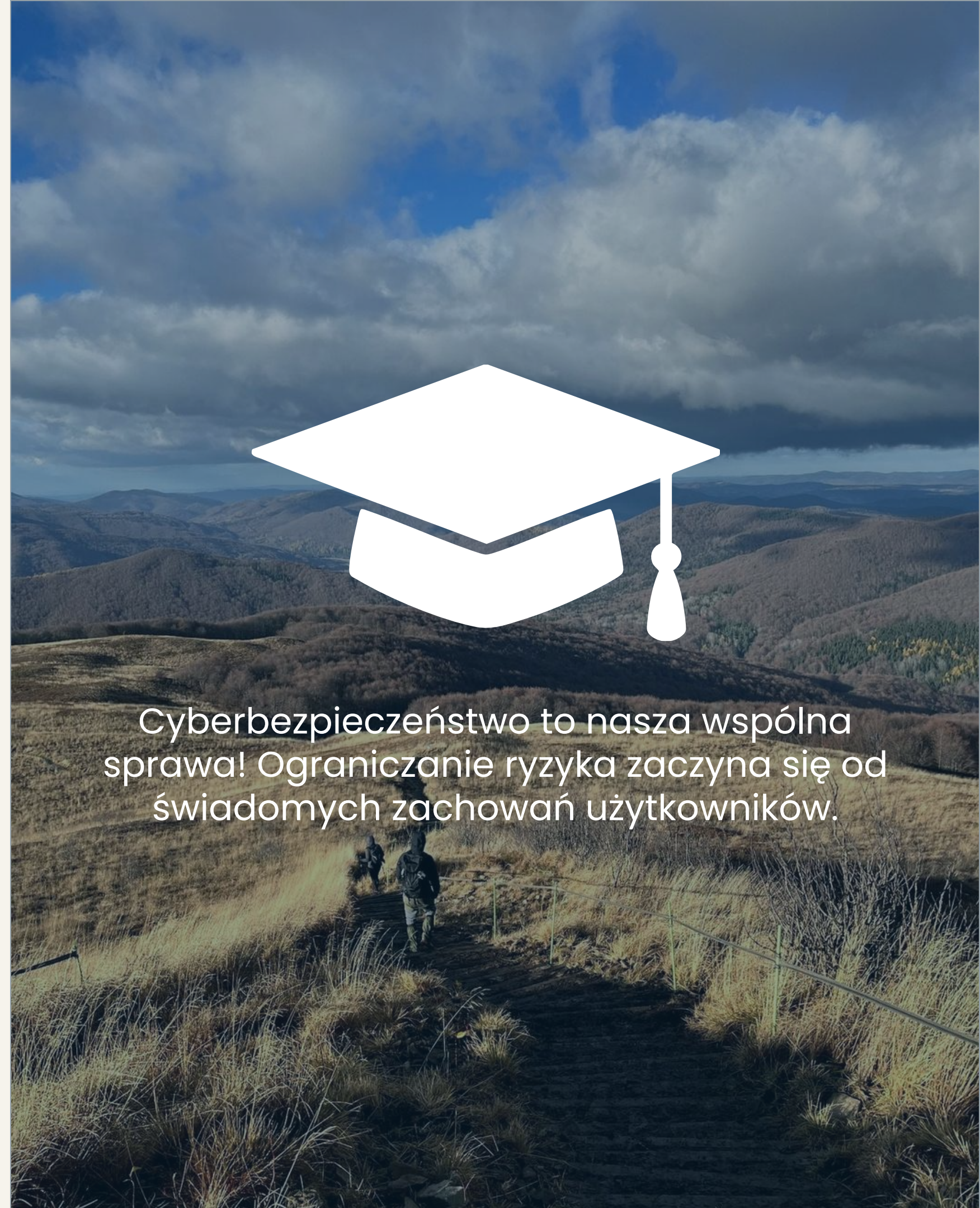
KRC to lokalne centra budowania cyberodporności mieszkańców,
nie tylko miejsca rozwijania kompetencji cyfrowych.

Lokalna edukacja wzmacnia odporność społeczności i państwa



Działania KRC wspierają realizację celów polityki cyberbezpieczeństwa przez:

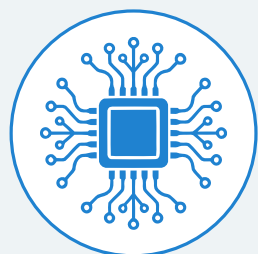
- świadomość cyberzagrożeń
- bezpieczne korzystanie z internetu i e-usług
- kompetencje cyfrowe
- odporność cyfrową społeczności



Cyberbezpieczeństwo to nasza wspólna sprawa! Ograniczanie ryzyka zaczyna się od świadomych zachowań użytkowników.

Najsilniejszy efekt daje połączenie technologii, procedur, kompetencji i współpracy

Tak zaprojektowany model odpowiada zarówno na ryzyko systemowe, jak i na błędy użytkowników.



Technologia

narzędzia ochrony, detekcji i reakcji



Procedury

polityki, SZBI, ciągłość działania



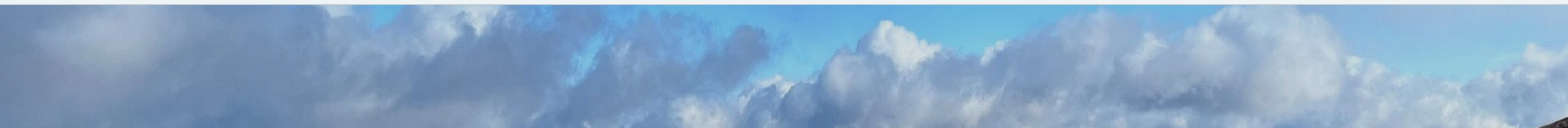
Kompetencje

szkolenia i cyberhigiena



Współpraca

instytucje, JST, społeczności



Podsumowanie

Cyberodporność kraju musimy budować równolegle w instytucjach, usługach i społecznościach

państwo cyfrowe	bezpieczne systemy administracji
lokalny samorząd	procedury, infrastruktura i kompetencje JST
usługi podstawowe	ochrona procesów IT i OT
obywatele	świadomość i bezpieczne nawyki

Fundusze UE są narzędziem wzmacniania odporności. Końcowy efekt zależy od spójnego wdrożenia technologii, procesów i edukacji.



zdjęcia: Łukasz Prokop