NASK | Cyberbezpieczny Samorząd

Cyberbezpieczny Samorząd

Fundusze Europejskie na Rozwój Cyfrowy

Fundusze Europejskie na Rozwój Cyfrowy

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

AGENDA PREZENTACJI

1. Wprowadzenie
    - Wyniki kontroli NIK
    - Diagnoza Cyberbezpieczeństwa
2. Cyberbezpieczny Samorząd - O projekcie
3. Katalog kosztów kwalifikowanych

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

WYNIKI KONTROLI NIK

„Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego”

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

WYNIKI KONTROLI NIK

„Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego”

NASK

Pytanie definiujące cel główny kontroli

Czy przyjęte i wdrożone rozwiązania organizacyjne i techniczne zapewniają bezpieczeństwo przetwarzania informacji w urzędzie?

Jednostki kontrolowane

Kontrolą objęto 23 jednostki: dziewięć starostw powiatowych oraz 14 urzędów miast/miast i gmin/gmin z obszaru pięciu województw.

Okres objęty kontrolą

Od 1 czerwca 2017 r. do dnia zakończenia kontroli w 2018 r.

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

WYNIKI KONTROLI NIK

Ocena ogólna

NIK **negatywnie oceniła wykonywanie przez blisko 70% skontrolowanych urzędów** jednostek samorządu terytorialnego zadań związanych z zapewnieniem bezpieczeństwa przetwarzania informacji w okresie objętym kontrolą.

Brak systemowego podejścia do zapewnienia bezpieczeństwa informacji

- W 61% skontrolowanych urzędów brak było systemowego podejścia do zapewnienia bezpieczeństwa informacji.
- W 74% badanych urzędów brak było pełnej i aktualnej informacji o posiadanych zasobach informatycznych służących do przetwarzania danych.
- W 26% urzędów stwierdzono niedostosowanie uregulowań wewnętrznych w zakresie ochrony danych osobowych do przepisów RODO.

Brak analiz ryzyka i nieprowadzenie audytów bezpieczeństwa informacji

- 48% jednostek nie dokonywano analiz ryzyka,
- a w 70% nie przeprowadzono obowiązkowego corocznego audytu z zakresu bezpieczeństwa informacji.

Nieprzestrzeganie ustanowionych wymogów w zakresie bezpieczeństwa informacji

- W ponad 80% skontrolowanych urzędów wystąpiły nieprawidłowości w zarządzaniu uprawnieniami użytkowników w systemach informatycznych. W zakresie uzyskiwania dostępu do systemów informatycznych,
- w ponad połowie kontrolowanych urzędów (57%) ustanowione zasady nie były przestrzegane.
- W 56% jednostek wykorzystywano komputery z zainstalowanym systemem operacyjnym bez wsparcia producenta,
- a w 48% urzędów stwierdzono nieprawidłowości w zakresie tworzenia, przechowywania oraz weryfikacji kopii zapasowych danych.

Wdrażanie RODO a zapewnienie bezpieczeństwa informacji

Wyniki kontroli NIK wskazują, że o ile w urzędach j.s.t. w większości podjęto działania w celu dostosowania do RODO, to w dalszym ciągu często nie są przestrzegane wymogi dotyczące bezpieczeństwa informacji wynikające z obowiązującego od 2012 r. rozporządzenia KRI. W opinii NIK, nie jest możliwe zapewnienie wysokiego poziomu ochrony danych osobowych bez zachowania właściwego bezpieczeństwa informacji.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

DIAGNOZA CYBERBEZPIECZEŃSTWA W JST

badanie w ramach konkursów Cyfrowa Gmina/Powiat/Województwo

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

DIAGNOZA CYBERBEZPIECZEŃSTWA W JST

Wyniki dla 2285 gmin (wybrane aspekty)

NASK

Opracowanie, ustanowienie i wdrożenie SZBI

- 63% urzędów posiadało wdrożony zarządzeniem SZBI
  - Z czego tylko 40% podmiotów wykonuje jego okresowy przegląd
- 19% urzędów było w trakcie na różnym poziomie zaawansowania
- 18% nie podeszło do opracowania, ustanowienia i wdrożenia SZBI

W większości urzędów funkcjonują polityki w zakresie ochrony danych osobowych z elementami bezpieczeństwa informacji. Nie były one uznane za systemowe podejście do budowania i wdrożenia SZBI.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

DIAGNOZA CYBERBEZPIECZEŃSTWA W JST

Wyniki dla 2285 gmin (wybrane aspekty)

NASK

Przeprowadzanie okresowych analiz ryzyka

- 53% urzędów przeprowadza regularną analizę ryzyka
- 22% urzędów przeprowadza nieregularną lub w ograniczonym zakresie (np. tylko w odniesieniu do danych osobowych) analizę ryzyka
- 25% nie przedstawiło dowodów na przeprowadzenie analizy ryzyka

Ze względu na różnice w ocenie audytorów, wskaźnik 53% jest zawyżony, część audytujących uznawała analizy w zakresie DO za wystarczające. Podobnie zbyt dawne analizy ryzyka były klasyfikowane jako brak zwiększając odsetek czerwony.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

DIAGNOZA CYBERBEZPIECZEŃSTWA W JST

Wyniki dla 2285 gmin (wybrane aspekty)

NASK

Inwentaryzacja sprzętu i oprogramowania

- 63% urzędów przeprowadza regularną inwentaryzację/utrzymuje aktualny spis
- 22% urzędów wykorzystuje spisy środków trwałych i WNP lub przeprowadza inwentaryzację (utrzymanie wykazu) w sposób nieregularny
- 15% nie prowadzi własnych spisów i nie korzysta ze spisów księgowych

Ze względu na różnice w ocenie audytorów, wskaźnik 63% jest zawyżony, część audytujących uznawała spisy księgowe jako spełnienie wymagania. Jedynie 24% podmiotów przeprowadza inwentaryzację automatycznie, za pomocą dedykowanych narzędzi.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

DIAGNOZA CYBERBEZPIECZEŃSTWA W JST

Wyniki dla 2285 gmin (wybrane aspekty)

NASK

Szkolenia i uświadamianie

- **57% urzędów wskazało że szkoli i uświadamia, ale:**
  - Często są to tylko szkolenia w zakresie ochrony danych osobowych.
  - Często są to tylko szkolenia wprowadzające dla nowych pracowników.
  - Wiele urzędów ogranicza się do publikowania informacji w intranecie.

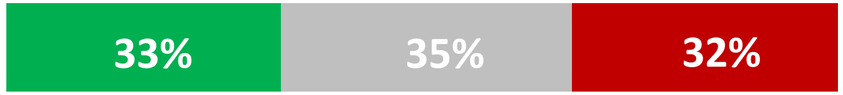
Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

DIAGNOZA CYBERBEZPIECZEŃSTWA W JST

Wyniki dla 2285 gmin (wybrane aspekty)

NASK

Zarządzanie podatnościami systemów



- **33% urzędów prowadzi zarządzanie podatnościami systemów, ale**
  - jedynie 8% podmiotów, stosując albo dedykowany skaner podatności (1% podmiotów) albo rozszerzoną funkcjonalność oprogramowania antywirusowego (7% podmiotów),
  - dbanie o aktualizacje i posiadanie wsparcia producenta nie wyczerpuje zagadnienia.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

DIAGNOZA CYBERBEZPIECZEŃSTWA W JST

Wnioski ogólne

NASK

Diagnoza Cyberbezpieczeństwa przyniosła wiele dobrego

- W wielu przypadkach pokazała problemy (bardziej od strony zgodności z prawem) zapewnienia bezpieczeństwa informacji.
- Otworzyła drzwi gabinetów włodarzy dla specjalistów od IT/Sec, dopuściła ich do planowania budżetów.

Diagnoza Cyberbezpieczeństwa uwidoczniła też poważne problemy

- Zapewnienie odporności na zagrożenia w cyberprzestrzeni jest zadaniem przekraczającym możliwości samodzielnej realizacji przez większość podmiotów JST (gmin).
- Podmioty nie posiadają kompetencji do zarządzania bezpieczeństwem, np. do przeprowadzania analiz ryzyka.
- Systematyczne zarządzanie bezpieczeństwem IT jest kosztowne, szczególnie, że do większości działań JST musi skorzystać z usług zewnętrznych.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

DIAGNOZA CYBERBEZPIECZEŃSTWA W JST

Wnioski ogólne – główne wyzwania

NASK

TECHNICZNE

- identyfikacja co i dlaczego chronimy?
- dobór klas rozwiązań
- zapewnienie ciągłości monitorowania
- utrzymanie zdolności do szybkiej reakcji

ORGANIZACYJNE

- wsparcie kierownictwa
- przygotowanie jednostki
- dyscyplina i higiena
- sprawność operacyjna

KOMPETENCYJNE

- budowanie świadomości
- kompetencje specjalistyczne
- weryfikowanie odporności

Jak zbudować System?

który chroni to co trzeba tak jak trzeba → który jest trwały i nie tylko na papierze → który dba o każde ogniwo

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

CYBERBEZPIECZNY SAMORZĄD

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

CYBERBEZPIECZNY SAMORZĄD

O projekcie

NASK

„Cyberbezpieczny Samorząd” to projekt Ministerstwa Cyfryzacji finansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (w skrócie FERC) w ramach Działania 2.2.

2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa

Interwencja obejmie inwestycje zwiększające poziom bezpieczeństwa informacji poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych państwa oraz podmiotów mających kluczowe znaczenie dla gospodarki.

Celem projektu jest **zwiększenie bezpieczeństwa informacji w administracji samorządowej** poprzez wzmacnianie odporności oraz zdolności do **skutecznego zapobiegania i reagowania na incydenty.**

Sposób realizacji projektu

Projekt realizowany jest poprzez uruchomienie konkursu grantowego adresowanego jednostkom samorządu terytorialnego na poziomie gminy, powiatu, samorządu województwa. W ramach konkursu przyznane są granty na zakup usług i środków technicznych służących zwiększeniu poziomu cyberbezpieczeństwa jednostek samorządowych w obszarach: organizacji, kompetencji i technologii.

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

CYBERBEZPIECZNY SAMORZĄD

O projekcie

NASK

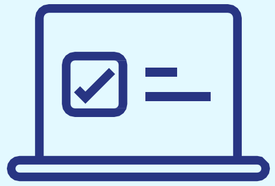
Zakłada się, że realizacja projektu przyczyni się do:

- wdrożenia lub aktualizacji w JST polityk bezpieczeństwa informacji (SZBI)
- wdrożenia w JST środków zarządzania ryzykiem w cyberbezpieczeństwie
- wdrożenia w JST mechanizmów i środków zwiększających odporność na ataki z cyberprzestrzeni
- podniesienia poziomu wiedzy i kompetencji personelu JST kluczowego z punktu widzenia SZBI wdrożonego w urzędzie
- przeprowadzenia w JST audytów SZBI potwierdzających uzyskanie wyższego poziomu odporności na cyberzagrożenia

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

CYBERBEZPIECZNY SAMORZĄD

O projekcie



Organizatorem projektu grantowego jest Centrum Projektów Polska Cyfrowa (CPPC) realizująca projekt w Partnerstwie z Naukową i Akademicką Siecią Komputerową - Państwowym Instytutem Badawczym (NASK-PIB).

Nabór wniosków grantowych realizowany jest w ramach otwartego naboru grantowego na postawie regulaminu dostępnego na stronie: **https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad**

Składanie wniosków grantowych w projekcie „Cyberbezpieczny Samorząd” odbywa się w formie elektronicznej przez **Lokalny System Informatyczny (LSI),** który dostępny jest pod adresem: https://lsi.cppc.gov.pl/beneficjent

Wnioskodawca wypełniać będzie za pośrednictwem LSI:

Dane rejestracyjne (Przekazanie niezbędnych danych kontaktowych).

Formularz aplikacyjny o grant (Opisanie koncepcji realizacji grantu, wskazanie planowanych wydatków w ramach grantu).

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

CYBERBEZPIECZNY SAMORZĄD

O projekcie – harmonogram Konkursu Grantowego

NASK

19.07.2023 r.

Ogłoszenie naboru, uruchomienie LSI i możliwości składania wniosków.

13.10.2023 r.

do godziny 16.00

Zakończenie naboru i składania wniosków.

Okres kwalifikowalności wydatków - od dnia

01.06.2023 r.

i kończy się maksymalnie w ciągu 24 miesięcy od dnia wejścia w życie Umowy o powierzenie grantu (jednak nie później niż w dniu 30.06.2026 r.).

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

CYBERBEZPIECZNY SAMORZĄD

O projekcie – podmioty uprawnione

NASK

Projekt będzie realizowany na terenie całego kraju. Zostaną nim objęte wszystkie jednostki samorządowe tj.

2 477	314	16
GMIN	POWIATÓW	WOJEWÓDZTW

2 807 JST

ŁĄCZNIE

Grupą docelową projektu jest administracja publiczna:

jednostki samorządu terytorialnego (JST) wraz z jednostkami podległymi

(z ograniczeniem do jednostek sektora publicznego, z wyłączeniem placówek ochrony zdrowia).

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

CYBERBEZPIECZNY SAMORZĄD

O projekcie – alokacja

NASK

Alokacja na Granty w konkursie “Cyberbezpieczny Samorząd” wynosi

1 762 235 453,00 PLN

w tym środki unijne w wysokości

1 465 303 702,00 PLN

oraz

środki z budżetu państwa w wysokości

296 931 751,00 PLN

Maksymalna intensywność dofinansowania projektu grantowego może wynosić do

100%

kosztów kwalifikowalnych

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

CYBERBEZPIECZNY SAMORZĄD

O projekcie – poziom dofinansowania

NASK

GMINY

od 200 000 PLN
do 850 000 PLN

Przedział wysokości dofinansowania grantu

POWIATY

do 850 000 PLN

Wysokość dofinansowania grantu

SAMORZĄDY WOJEWÓDZKIE

do 850 000 PLN

Wysokość dofinansowania grantu

Maksymalna kwota dofinansowania dla każdej JST jest wskazana w dokumentacji konkursowej

Załącznik nr 2 – Lista podmiotów uprawnionych do uczestniczenia w naborze

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

KATALOG KOSZTÓW KWALIFIKOWANYCH

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

KATALOG KOSZTÓW KWALIFIKOWANYCH

Główne wyzwania

NASK

TECHNICZNE

- identyfikacja co i dlaczego chronimy?
- dobór klas rozwiązań
- zapewnienie ciągłości monitorowania
- utrzymanie zdolności do szybkiej reakcji

ORGANIZACYJNE

- wsparcie kierownictwa
- przygotowanie jednostki
- dyscyplina i higiena
- sprawność operacyjna

KOMPETENCYJNE

- budowanie świadomości
- kompetencje specjalistyczne
- weryfikowanie odporności

Jak zbudować System?

który chroni to co trzeba tak jak trzeba → który jest trwały i nie tylko na papierze → który dba o każde ogniwo

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

KATALOG KOSZTÓW KWALIFIKOWANYCH

Wydatki w obszarze organizacyjnym

NASK

OBSZAR ORGANIZACYJNY:

Opracowanie, wdrożenie oraz aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

Wprowadzenie lub aktualizacja:

- polityk bezpieczeństwa informacji (PBI),
- analizy ryzyka (w tym opracowanie i wdrożenie metodyk).

Deklaracja stosowania, np.

- procedury eksploatacyjne,
- procedury ciągłości działania biznesowego po katastrofie,
- procedury zasad monitorowania infrastruktury,
- procedury obsługi incydentów.

Audyt Systemu Zarządzania Bezpieczeństwem Informacji

Audyt zgodności z KRI/UoKSC przez wykwalifikowanych audytorów

(Re)certyfikacja SZBI na zgodność z normami 27001, 22301.

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

KATALOG KOSZTÓW KWALIFIKOWANYCH

Wydatki w obszarze kompetencyjnym

NASK

OBSZAR KOMPETENCYJNY:

Podstawowe szkolenia (lub dostęp do platform szkoleniowych) budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników JST.

Szkolenia z zakresu cyberbezpieczeństwa dla pracowników JST, istotnych z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji.

Szkolenia specjalistyczne dla kadry zarządzającej i obsługi informatycznej w zakresie zastosowanych (planowanych do zastosowania) środków bezpieczeństwa w ramach projektu grantowego.

Szkolenia powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcji personelu, w szczególności reagowanie specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

KATALOG KOSZTÓW KWALIFIKOWANYCH

Wydatki w obszarze technicznym

NASK

OBSZAR TECHNICZNY:

Zakup, wdrożenie i utrzymanie systemów teleinformatycznych, w tym urządzeń, oprogramowania i usług zapewniających prewencję, detekcję i reakcję na zagrożenia cyberbezpieczeństwa, z niezbędnym wsparciem producenta.

Zakup, wdrożenie i utrzymanie rozwiązań ciągłego monitorowania bezpieczeństwa, skanery podatności, zarządzanie podatnościami, zarządzanie zasobami IT i aktywami podlegającymi ochronie.

Zakup usług wsparcia realizowanych przez zewnętrznych ekspertów z zakresu cyberbezpieczeństwa.

Zakup, wdrożenie i utrzymanie systemów lub usług na potrzeby centrów cyberbezpieczeństwa (SOC), także jako element Centrum Usług Wspólnych, zakup testów i badań bezpieczeństwa, dostępu do informacji bezpieczeństwa oraz inne usługi integracyjne dotyczące obszaru cyberbezpieczeństwa.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

DZIĘKUJEMY ZA UWAGĘ

Centrum Projektów Polska Cyfrowa ul.
Spokojna 13A
01-044 Warszawa

NASK

Operator NASK - PIB - helpdesk Tel.:
+48 22 182 22 94

Infolinia działa w godzinach 8:00-16:00 od poniedziałku do piątku. e-mail:
cyberbezpiecznysamorzad@cppc.gov.pl

Fundusze Europejskie na Rozwój Cyfrowy

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA