

CYBERBEZPIECZNY SAMORZĄD



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Gmina Kruszwica uzyskała dofinansowanie na realizację projektu pn.

Poprawa cyberbezpieczeństwa Gminy Kruszwica.

Projekt dofinansowany w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd” o numerze FERC.02.02-CS.01-001/23, Umowa o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/2416/ FERC.02.02-CS.01-001/23/2024.

Celem projektu jest wzrost bezpieczeństwa przetwarzanie danych oraz zapewnienie cyberbezpieczeństwa samorządowych systemów informatycznych Gminy Kruszwica.

Projekt przewiduje rozwiązania zwiększające poziom cyberbezpieczeństwa oraz stworzenie silnej i odpornej infrastruktury bezpieczeństwa informacji na poziomie lokalnym. Projekt zakłada, że dzięki wdrożeniu nowoczesnych narzędzi i rozwiązań technologicznych, Gmina Kruszwica będzie w stanie skutecznie odpierać ataki, minimalizować ryzyko incydentów, chronić dane obywateli oraz zapewnić stabilność działania usług publicznych.

Zaplanowane działania:

OBSZAR ORGANIZACYJNY:

1.W01,W02:Usługa przeglądu/audytu oceniająca aktualny stan SZBI, porównanie funkcjonujących procesów i procedur z wymaganiami aktualnych norm oraz wskazania ewentualnych niezgodności i możliwości do wdrożenia działań korygujących w obszarze dokumentacji i technologii. Opracowanie poprawek i dostosowanie do nowych wymagań oraz wdrożenie poprawionej dokumentacji SZBI, w tym m.in. Polityki Bezpieczeństwa Informacji wraz z niezbędnymi procedurami, zarządzanie ryzykiem oraz przeprowadzenie procesu analizy ryzyka.

2.W01:Przeprowadzenie wymaganego w regulamin konkursu grantowego pn. Cyberbezpieczny Samorząd audytu wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z warunkami określonymi w regulaminie.

3.W02:Doradztwo techniczne, przygotowanie postępowania, w tym przygotowanie opisu przedmiotu zamówienia SWZ, przygotowanie dokumentacji postępowania, przygotowanie zapytania ofertowego wraz z załącznikami dla przetargów i zamówień niewymagających PZP. Doradztwo na etapie prowadzenia postępowania o udzielenie zamówienia publicznego, udzielanie odpowiedzi podczas postępowania i przetargów, wsparcie i doradztwo specjalistów przy odbiorze usług i sprzętu itd.

OBSZAR KOMPETENCYJNY

1.W02:Szkolenie stacjonarne z zakresu cyberbezpieczeństwa dla wybranych przedstawicieli kadry JST, istotnych z punktu widzenia polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji:po wdrożeniu poprawionego SZBI.

2.W07:Podstawowe szkolenia (lub dostęp do platform szkoleniowych) budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników JST.

3.W02,W16:Szkolenia specjalistyczne dla informatyka w zakresie zastosowanych w Projekcie (planowanych do zastosowania) środków bezpieczeństwa w ramach zakupionego sprzętu i oprogramowania.

OBSZAR TECHNICZNY

1.W16:Rozbudowa klastra macierzy obiektowej HCP do pełnego limitu pojemności dyskowej tego modelu w celu zagwarantowania odpowiedniej przestrzeni na ważne dane użytkowników wymagające bezpiecznego przechowywania oraz planowanego wdrożenia obiegu dokumentów. Podyktowane jest to również stale rosnącą ilości danych a także wykorzystaniem macierzy obiektowej oraz systemu HCP Anyware jako chmury prywatnej dla jej użytkowników. Efektem rozbudowy będzie wzrost przestrzeni dyskowej o 24TB.

2.W16:Modernizacja infrastruktury sieciowej poprzez wymianę starych przełączników na nowe. Celem jest uniknięcie wystąpienia przestoju w pracy urzędu (odmowa świadczenia usług zarówno dla pracowników urzędu jak i interesantów eUsługi) spowodowanych potencjalnie awariami wyeksploatowanych i w większości posiadających status End Of Life (EOL) przełączników. Wymiana przełączników podniesie bezpieczeństwo infrastruktury, zwiększy przepustowość a także ułatwi jej zarządzanie.

Planowany jest zakup przełączników posiadających możliwość uruchomienia funkcjonalności związanych z tradycyjnymi sieciami LAN jak i sieciami w DC oraz WAN (porty miedziane 1/10G do obsługi LAN i infrastruktury serwerowej DC oraz porty światłowodowe do połączenia 2 serwerowni) a w szczególności:

a)Elastyczna i rozbudowana tablica forwardingu/routingu/MAC. System zapewniający opcje konfigurowalne za pomocą interfejsu CLI, które mogą zoptymalizować różne scenariusze wdrożenia.

b)Automatyzacja: obsługa funkcji automatyzacji sieciowej i operacyjnych funkcji plug-and-play, w tym ZTP i skryptów zdarzeń, automatyczne cofanie zmian (rollback).

c)Zestaw funkcji MPLS, w tym VPN warstwy 3, inżynieria ruchu RSVP i LDP, umożliwiający standaryzowaną segmentację sieci i wirtualizację.

d)Przebieg czynnik zdolny do świadczenia zarówno usług bramy warstwy 2, jak i 3.

3.W16:Zakup i wdrożenie kompletnego serwera do backupu (appliance), który zapewni ochronę, zarządzanie i odzyskiwanie kluczowych danych.

4.W09,W10:Zakup i wdrożenie urządzeń klasy UTM. Migracja starego urządzenia do 2 nowych urządzeń w celu stworzenia grupy HA. Konfiguracja dwóch zapór sieciowych w parze HA zapewni redundancję i pozwoli zapewnić ciągłość działania Internetu co jest kluczowe do bezpiecznego funkcjonowania urzędu oraz świadczenia eUsług.

5.W16:Zakup zasilaczy awaryjnych UPS a)do zasilania szafy dystrybucyjnej w DC:1szt. b)do zasilania PC:minimum 10szt.

6.W09,W10:Zakup i dostawę licencji subskrypcyjnych na system do ochrony stacji roboczych z funkcjonalnością EDR w ramach aktualizacji do wersji COMPLETE posiadanego systemu Symantec Endpoint Security w wersji ENTERPRISE.

7.W10:Zakup i dostawa licencji subskrypcyjnych dla posiadanego urządzenia klasy PAM BeyondTrust Privilege Remote Access w ramach przedłużenia ich na kolejny okres użytkowania i zakupu nowych.

8. W10, W16:Zakup i wdrożenie serwera NAS. Szczegółowe odniesienie do wymagań z Poradnika znajduje się w załączniku do wniosku.

W wyniku realizacji projektu osiągnięte zostaną następujące wskaźniki:

-Liczba pracowników IT podmiotów wykonujących zadania publiczne objętych wsparciem szkoleniowym:1,

-Liczba pracowników podmiotów wykonujących zadania publiczne nie będących pracownikami IT, objętych wsparciem szkoleniowym:57 ,

-Liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji:3szt.,

-Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych: 3000/rok ,

-Liczba JST wspartych w zakresie cyberbezpieczeństwa:1szt

#FunduszeUE #FunduszeEuropejskie

Wartość projektu: 966 360,00 zł

Wydatki kwalifikowalne: 904 254,99 zł

Kwota dofinansowania: 850 000,00 zł, w tym: UE: 705 499,99zł, BP: 144 500,00zł



**Fundusze
Europejskie**

**Dofinansowane przez
Unię Europejską**



Gmina Kruszwica
realizuje projekt pn. Poprawa cyberbezpieczeństwa
Gminy Kruszwica

Dofinansowanie projektu z UE: 705 499,99 PLN

www.mapadotacji.gov.pl