

Cyberbezpieczny Samorząd w Powiecie Sierpeckim

The infographic is set against a dark red background. At the top left is a white logo consisting of a hexagon with a stylized '@' inside. To its right, the title 'Cyberbezpieczny Samorząd' is written in large, bold, white sans-serif font. Below the title, on the left, is a small white padlock icon next to the heading 'O projekcie Cyberbezpieczny Samorząd'. The text below it explains that the project provides direct financial support to territorial units to raise cyber security levels. On the right side, there are three sections. The first mentions the project is implemented by CPPC in partnership with NASK - Państwowy Instytut Badawczy, with logos for the Ministry of Digital Affairs and NASK. The second section, 'Kto może aplikować o grant?', shows an icon of three people and states that 2807 territorial units can apply. The third section, 'Jaka jest wysokość grantu?', shows an icon of coins and states the grant amount ranges from 200 to 850 thousand PLN, depending on the number of residents. At the bottom, there are logos for 'Fundusze Europejskie na Rozwój Cyfrowy', 'Dofinansowane przez Unię Europejską' with the EU flag, and 'CENTRUM PROJEKTÓW POLSKA CYFROWA'.

Cyberbezpieczny Samorząd

Projekt Cyberbezpieczny Samorząd realizowany jest przez CPPC w partnerstwie z NASK – Państwowym Instytutem Badawczym

Ministerstwo Cyfryzacji **NASK**

O projekcie Cyberbezpieczny Samorząd
„Cyberbezpieczny Samorząd” to bezpośrednie wsparcie finansowe jednostek samorządu terytorialnego na podniesienie poziomu cyberbezpieczeństwa w podmiocie.

Kto może aplikować o grant?
2807 jednostek samorządu terytorialnego

Jaka jest wysokość grantu?
Kwota grantu od **200 tys. zł** do **850 tys. zł** (w zależności od liczby mieszkańców)

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

Starostwo Powiatowe w Sierpcu w projekcie “ Cyberbezpieczny Samorząd w Powiecie Sierpeckim” stawia na Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia zgodnie z Programem Operacyjnym Polska Cyfrowa, Fundusze Europejskie na Rozwój Cyfrowy (FERC).

W ramach projektu Starostwo planuje podniesienie cyberbezpieczeństwa poprzez zakup następujących urządzeń podnoszących bezpieczeństwo teleinformatyczne: serwerów, macierzy dyskowej, urządzenia bezpieczeństwa klasy UTM, generatora prądu, urządzenie do składowania danych i kopii zapasowych wraz oprogramowaniem do wykonywania kopii, urządzenia zasilania awaryjnego (UPS), oprogramowanie EDR, dostęp do platformy szkoleniowej dodatkowo planuje się zakup systemu antywirusowego zabezpieczającego stacje robocze w urzędzie.

W ramach projektu planuje się również aktualizację dokumentacji cyberbezpieczeństwa, przeprowadzenie niezbędnych audytów (SZBI, KRI) oraz szkolenie dla pracowników oraz kadry zarządzającej i pracowników IT, podnoszące ich kompetencje w zakresie cyberbezpieczeństwa.

Uzasadnienie zakresu wydatków i inwestycji do wymagań „Wykaz wymagań bezpieczeństwa dla podmiotów publicznych”:

W chwili obecnej Starostwo Powiatowe w Sierpcu posiada serwery starszej generacji o małej wydajności co wiąże się z niebezpieczeństwem utraty danych. Zakupiony nowy sprzęt zakłada, iż serwery będą wysokiej wydajności i dostępności oraz będą spełniać wymogi nowoczesnych rozwiązań, tym samym podniesie to poziom bezpieczeństwa i pracy całego urzędu. Nowa macierz umożliwi również zabezpieczenie danych zgodnie z polityką cyberbezpieczeństwa; Eksploatowane obecnie przez Starostwo urządzenie klasy UTM jest niewielkiej przepustowości o ograniczonych możliwościach. W ramach projektu Starostwo zostanie

wyposażone w urządzenie bezpieczeństwa klasy UTM. Urządzenie to jest wielofunkcyjną zaporą sieciową, zapewniającą ochronę na wielu poziomach i przed zagrożeniami. Urządzenie odpowiedniej klasy UTM zostanie postawione na styku sieci wewnętrznej z Internetem zabezpieczając dane oraz umożliwiając bezpieczne połączenie pracy zdalnej.

Na styku tego połączenia planowane jest wydzielenie odrębnych podsieci tzw. VLANów, z podziałem na poszczególne grupy użytkowników. Zapewni to dodatkowe zabezpieczenie w przypadku cyber ataków na urząd, gdyż grupy użytkowników będą odseparowane od siebie.

Generator prądu jest rezerwowym źródłem energii elektrycznej w przypadkach awarii sieci energetycznej.

Zakup tego urządzenia pozwoli Starostwu na prace w przypadku braku zasilania lub spadków napięć.

Aktualnie Starostwo posiada niewielkie urządzenie do backupu tylko podstawowych danych z ograniczoną ilością miejsca na nie. Zakup nowego tego typu urządzenia pozwoli na tworzenie kopii zapasowych, które będą deduplikowane. Urządzenie posiada wiele funkcji zabezpieczenia danych pozwala również zaoszczędzić przestrzeń dyskową.

Starostwo Powiatowe w Sierpcu dzięki projektowi zostanie wyposażone w urządzenia zasilania awaryjnego (UPS-y). Zadaniem tych urządzeń będzie podtrzymanie zasilania awaryjnego w przypadku nieprawidłowości lub zaniku zasilania sieciowego. Zasilacze tego typu nie tylko służą do awaryjnego zasilania prądem, ale również chronią przed nagłymi skokami napięcia co pozwoli lepiej chronić zarówno zgromadzone dane jak i urządzenia do niego podłączone.

Oprogramowanie EDR to narzędzie służące wykrywaniu i reagowaniu na podejrzane aktywności na urządzeniach końcowych. Rozwiązania klasy EDR to dodatkowa warstwa bezpieczeństwa, która wraz z tradycyjnymi rozwiązaniami chroni środowisko IT przed szerokim spektrum zagrożeń. EDR nie tylko analizuje i eliminuje zagrożenia, ale pomaga również uzupełnić luki w strategii ochronnej. Zakupione zostaną również licencje na oprogramowanie antywirusowe.

Zakup oprogramowania do wykonywania kopii zapasowych pozwoli starostwu na regularne wykonywanie kopii zapasowych plików systemowych, aby w przypadku awarii, uszkodzenia lub cyber ataku można było je przywrócić lub odzyskać. Zakup oprogramowania pozwoli ponadto na przechowywanie danych w bezpiecznym miejscu, z dala od potencjalnych zagrożeń.

Zaplanowane zostało również przeprowadzenie uaktualnienia dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w ramach którego dokumentacja ta zostanie opracowana według aktualnych wytycznych łącznie ze strategiami i regulaminami niezbędnymi w dokumentacji SZBI.

Audyt KRI pozwoli na sprawdzenie aktualności oprogramowania i sprzętu, które wykorzystywane są do przetwarzania informacji. Audyt koncentruje się także na przeprowadzeniu analizy ryzyka utraty integralności, dostępności czy poufności informacji oraz ma za zadanie wskazać działania, które

zminimalizują to ryzyko.

W ramach projektu Starostwo planuje przeprowadzenie audytu przedwdrożeniowego w celu wykrycia potencjalnych luk w posiadanych systemach i oprogramowaniu.

Planowane są również przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa i bezpieczeństwa informacji. Projekt umożliwi nam na zakup profesjonalnych szkoleń z zakresu cyberbezpieczeństwa dla pracowników oraz kadry zarządzającej i pracowników IT podnoszące ich kompetencje w tym zakresie.

Platforma szkoleniowa zakupiona w ramach projektu to narzędzie dzięki któremu pracownicy będą mogli podnieść świadomość na temat zagrożeń występujących w cyberprzestrzeni. Nabyta podczas szkoleń wiedza przełoży się bezpośrednio na mniejszą podatność na różnego rodzaju ataki hackerskie oraz zmniejszy ryzyko wystąpienia incydentu.

Cyberbezpieczeństwo jest niezwykle istotne z punktu widzenia każdej organizacji. Urzędy operują dziś na niezliczonej ilości danych. Niemal niemożliwe jest funkcjonowanie bez procedur związanych z cyberbezpieczeństwem. Odpowiednio wdrożone procedury i zabezpieczenia danych, systemów i aplikacji to przede wszystkim:

ochrona przed utratą wrażliwych danych (np. w wyniku ataku typu ransomware), zapobieganie stratom finansowym, które często są wynikiem zarówno cyberataków, jak i awarii powodujących przestoje w funkcjonowaniu urzędu, zapobieganie utracie reputacji, która zwykle jest skutkiem nieodpowiedniego dbania o zabezpieczenie danych (utrata reputacji może skutkować poważnymi stratami).

Realizacja projektu pozwoli nam na zabezpieczenie punktów wrażliwych naszej sieci oraz pozwoli nam skutecznie wzmocnić cyfrową odporność na zagrożenia.

Link do projektu: [Cyberbezpieczny Samorząd](#)