Ministerstwo
Cyfryzacji

Podsekretarz Stanu
Rafał Rosiński

DPiS.WWKS.510.1.16.2025
Warszawa, 15 lipca 2025 r.

Pan Andrzej Płonka
Prezes Zarządu
Związku Powiatów Polskich

Dotyczy: Stanowiska XXXII Zgromadzenia Ogólnego Związku Powiatów Polskich w sprawie cyberbezpieczeństwa w samorządach.

Szanowny Panie Prezesie,

bardzo dziękuję za przekazanie do Ministerstwa Cyfryzacji Stanowiska XXXII Zgromadzenia Ogólnego Związku Powiatów Polskich w sprawie cyberbezpieczeństwa w samorządach. Pragnę zapewnić, że Ministerstwo Cyfryzacji konsekwentnie buduje i rozwija krajowy system cyberbezpieczeństwa, aby zapewnić ochronę cyberprzestrzeni RP na właściwym poziomie. Zapewnienie cyberbezpieczeństwa jest jednym z głównych priorytetów ministra cyfryzacji.

Ministerstwo Cyfryzacji wspiera również samorządy w zakresie cyberbezpieczeństwa poprzez następujące działania:

Wsparcie finansowe - konkurs grantowy „Cyberbezpieczny Samorząd"

W 2023 roku uruchomiony został, współfinansowany ze środków UE oraz budżetu państwa w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, projekt grantowy pn. „Cyberbezpieczny Samorząd", przewidujący wsparcie finansowe dla wszystkich jednostek samorządu terytorialnego w kraju. Wysokość grantu wynosiła od 200 tys. zł dla najmniejszych gmin do maksymalnie 850 tys. zł dla największych samorządów. Celem tego projektu jest zwiększenie bezpieczeństwa informacji poprzez wzmacnianie odporności jednostek samorządu terytorialnego oraz ich zdolności do skutecznego zapobiegania incydentom bezpieczeństwa teleinformatycznego, wykrywania ich i reagowania na nie. Wsparcie to obejmuje trzy kluczowe obszary cyberbezpieczeństwa, tj.: obszar organizacji, technologii oraz kompetencji.

Do końca 2024 r. zostały podpisane wszystkie (2 495) umowy z JST, które złożyły wniosek o wsparcie grantowe i sukcesywnie wypłacane są im środki na realizację grantów, których łączna wartość wynosi 1 474 312 573,61 zł. Na dzień 20.06.2025 r. do JST przekazano już ponad 977 mln zł. Projekty grantowe mogą być realizowane do 30 czerwca 2026 r. Dokumentacja naboru oraz dodatkowe materiały informacyjne dot. tego projektu zostały opublikowane pod adresem: https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad.

Łączne nakłady, jakie samorządy zaplanowały do poniesienia na poprawę swojego cyberbezpieczeństwa w okresie 2024-2026, w związku z udziałem w konkursie „Cyberbezpieczny Samorząd" wyniosą 1 585 710 570,92 zł. Na te środki składają się:

- wkład środków UE w wysokości 1 223 637 467,71 zł,
- wkład środków z budżetu państwa w wysokości 249 779 567,18 zł,

telefon: +48 22 245 59 13
adres email: sekretariat.dpis@cyfra.gov.pl
www.gov.pl/cyfryzacja

ul. Królewska 27
00-060 Warszawa

- wkład własny JST w wysokości 111 202 417,56 zł.

Środki, które pozyskały JST, będą wykorzystane także m.in. na zapewnienia ciągłości działania systemów informatycznych (m.in. wykonywanie kopii zapasowych, określenie procedur i zasad działania w obszarze cyberbezpieczeństwa, audyty bezpieczeństwa, szkolenia personelu itp.)

Wsparcie finansowe - konkurs grantowy „Cyberbezpieczne Wodociągi"

W pierwszej połowie sierpnia br. planowane jest ogłoszenie naboru wniosków o granty w ramach współfinansowanego ze środków KPO (inwestycja C3.1.1), konkursu pn. „Cyberbezpieczne wodociągi". Wsparcie to będzie adresowane do podmiotów prowadzących działalność w zakresie zbiorowego zaopatrzenia w wodę, objętych krajowym system cyberbezpieczeństwa, wykorzystujących technologie operacyjne w przemysłowych systemach sterowania, będące:

- przedsiębiorstwem wodociągowo-kanalizacyjnym, które jest operatorem usług kluczowych w rozumieniu art. 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222) lub
- spółką prawa handlowego wykonującą zadania o charakterze użyteczności publicznej w rozumieniu przepisów ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2021 r. poz. 679), lub
- jednostką sektora finansów publicznych w rozumieniu art. 9 pkt 2–4 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2024 r. poz. 1530, 1572, 1717, 1756 i 1907 oraz z 2025 r. poz. 39).

Zakres tego wsparcia będzie obejmował możliwość sfinansowania:

- wdrożenia środków organizacyjnych służących zapewnieniu cyberbezpieczeństwa,
- zakupu lub modernizacji środków technicznych służących zapewnieniu cyberbezpieczeństwa,
- rozwoju kompetencji personelu w zakresie cyberbezpieczeństwa.

Środki alokowane na to przedsięwzięcie wyniosą ok. 300 mln zł (szczegółowa wartość zostanie określona w regulaminie konkursu), a maksymalny limit wydatków w ramach jednego wniosku o przyznanie grantu ograniczony będzie wysokością pomocy de minimis, tj. 300 tys. EUR (otrzymana w ciągu 3 lat). Okres kwalifikowalności wydatków w ramach wsparcia obejmie okres od 1 stycznia 2025 r. do 30 czerwca 2026 r;

W związku z faktem, iż wsparcie realizowane w ramach konkursu „Cyberbezpieczne wodociągi" będzie miało charakter pomocy publicznej, jego zasady reguluje rozporządzenie Ministra Cyfryzacji z dnia 29 maja 2025 r. w sprawie udzielania pomocy de minimis na wsparcie podmiotów prowadzących działalność w zakresie zbiorowego zaopatrzenia w wodę objętych krajowym systemem cyberbezpieczeństwa, w ramach Krajowego Planu Odbudowy i Zwiększania Odporności, które weszło w życie z dniem 4 czerwca 2025 r. Akt ten został opublikowany w Dzienniku Ustaw pod pozycją 729. Link do rozporządzenia: https://dziennikustaw.gov.pl/DU/2025/729.

Projekt utworzenia lub rozwoju „Lokalnych Centrów Cyberbezpieczeństwa"

Pod koniec 2025 r., w ramach współfinansowania ze środków programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, planowane jest uruchomienie nowego projektu wspierającego tworzenie lub rozwój Lokalnych Centrów Cyberbezpieczeństwa (LCC). Centra, które powstaną w jego wyniku, zapewnią kompleksowe i systemowe wsparcie dla samorządów. Zakres ich działania będzie obejmował w szczególności:

- monitorowanie i reagowanie na incydenty (monitorowanie lokalnych sieci i systemów informacyjnych, analizowanie potencjalnych zagrożeń oraz koordynowanie działań w przypadku incydentów cyberbezpieczeństwa);
- wsparcie techniczne (usługi doradcze i techniczne, obejmujące audyty bezpieczeństwa, wdrażanie środków ochrony, zarządzanie ryzykiem oraz tworzenie polityk bezpieczeństwa);
- edukację i szkolenia (szkolenia i warsztaty dla lokalnych pracowników, specjalistów IT i przedstawicieli instytucji publicznych);
- współpracę z inicjatywami krajowymi (z krajowymi instytucjami, takimi jak CERT Polska oraz innymi agencjami zajmującymi się cyberbezpieczeństwem, w celu koordynowania działań na poziomie regionalnym i krajowym).

Przyjmuje się, że środki alokowane na ten projekt wyniosą łącznie ok. 270 mln zł, a okres jego realizacji przypadnie na lata: 2025 – 2029.

Projekt LCC ma być, w szczególności, odpowiedzią na deficyt specjalistów z zakresu cyberbezpieczeństwa w jednostkach samorządu terytorialnego. Istotnym wsparciem dla upowszechnienia ww. podejścia będą także przygotowywane w Ministerstwie Cyfryzacji rozwiązania legislacyjne, które zostaną wprowadzone w ramach nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa.

Działania podnoszące kompetencje z zakresu cyberbezpieczeństwa

Jednym z istotnych elementów wspierających administrację publiczną w budowaniu odporności na cyberzagrożenia są prowadzone przez Ministerstwo Cyfryzacji działania podnoszące kompetencje z zakresu cyberbezpieczeństwa, w tym rozwijany od 2022 roku projekt SecureV.

Początkowo projekt obejmował najważniejszych polityków i parlamentarzystów, jednak ze względu na skalę zagrożeń oraz rosnące zainteresowanie szkoleniami, jego zasięg został rozszerzony na kolejne grupy odbiorców, w tym jednostki samorządu terytorialnego. W 2022 roku zrealizowano pilotaż w woj. podlaskim, obejmując kluczowych przedstawicieli samorządu lokalnego – wójtów, burmistrzów, prezydentów miast, starostów, członków zarządów, skarbników i kierowników USC.

Równolegle zrealizowano także pilotażowy projekt szkoleniowy dla personelu Podstawowej Opieki Zdrowotnej w powiecie pajęczańskim. Od 2023 roku działania edukacyjno-prewencyjne objęły zasięgiem cały kraj. Szkolenia w ramach projektu SecureV są również kontynuowane w 2025 r. a szkoleniami objęci są: przedstawiciele władzy ustawodawczej i wykonawczej, w tym kadra zarządzająca i pracownicy organów administracji rządowej, przedstawiciele jednostek samorządu terytorialnego, pracownicy sądów i prokuratury, przedstawiciele i członkowie Krajowego Biura Wyborczego oraz organów wyborczych.

W ramach obecnej edycji projektu na lata 2025- 2026 zaplanowano przeprowadzenie 8 tys. szkoleń. Szkolenia będą realizowane indywidulanie lub w małych grupach. Ponadto przeprowadzony zostanie pilotaż, którego celem jest zbudowanie kompetencji trenerskich w zakresie cyberbezpieczeństwa w JST. Szkoleniem trenerskim zostanie objętych minimum 2 przedstawicieli JST w każdym województwie. Zadaniem wyszkolonej osoby będzie planowanie działań edukacyjnych, organizacja regularnych szkoleń w jednostce, w tym szkolenia z nowych zagrożeń.

Ważnym filarem są również szkolenia online dla podmiotów krajowego systemu cyberbezpieczeństwa, realizowane we współpracy z ekspertami z NASK-PIB i partnerami

Programu Współpracy w Cyberbezpieczeństwie – PWCyber. Do tej pory w szkoleniach tych wzięło udział ponad 56 tys. osób.

Szkolenia są dostosowane do różnych poziomów zaawansowania i podzielone na trzy główne grupy:

- Szkolenia 100 – z zakresu cyberhigieny, dla szerokiego grona użytkowników,
- Szkolenia 200 – dla kadry zarządzającej i pracowników działów IT,
- Szkolenia 300 – specjalistyczne warsztaty dla administratorów, programistów i osób odpowiedzialnych za zarządzanie cyberbezpieczeństwem.

Planowana jest kolejna edycja szkoleń, która zostanie poszerzona o moduły poświęcone zagadnieniom z obszaru obowiązków wynikających z dyrektywy NIS2 - adresowana jednostkom administracji publicznej, w tym samorządowej.

Jednostki samorządu terytorialnego a krajowy system cyberbezpieczeństwa

Projekt ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw wdraża do porządku krajowego dyrektywę NIS 2, która w znacznym zakresie rozbudowuje obowiązki podmiotów krajowego systemu cyberbezpieczeństwa. Celem jest zapewnienie wysokiego wspólnego poziomu bezpieczeństwa w całej Unii Europejskiej. Kluczową rolę odgrywać będą w systemie podmioty kluczowe i podmioty ważne. Do katalogu tych podmiotów zaliczane będą również podmioty publiczne, w tym jednostki samorządu terytorialnego. Wraz z nowymi obowiązkami pojawią się również nowe środki nadzorcze, które będą stanowiły narzędzia dla organów właściwych do spraw cyberbezpieczeństwa pozwalając na skuteczne egzekwowanie przestrzegania przepisów ustawy przez podmioty kluczowe i ważne.

Projektodawca ma na uwadze, że nowe obowiązki mogą stanowić obciążenie dla podmiotów obecnie tworzących krajowy system cyberbezpieczeństwa, a także dla podmiotów, które do tej pory nie były objęte zakresem ustawy. Stanowić to będzie pewne wyzwanie organizacyjne. Z tego powodu ministerstwo cyfryzacji we współpracy z JST przygotowało przepisy, które znacznie ułatwią realizację ustawowych zadań.

Przepisy te obejmują możliwość zawierania porozumień i wspólnego wykonywania zadań z zakresu cyberbezpieczeństwa. Możliwe będzie wyznaczenie jednostki odpowiedzialnej za realizację ustawowych obowiązków na rzecz pozostałych jednostek samorządu terytorialnego. Może to być jednostka budżetowa, samorządowy zakład budżetowy albo spółka komunalna.

Dopuszczalne będzie także utworzenie wspólnej jednostki dla kilku gmin, kilku powiatów czy nawet samorządów województw (nowe brzmienie Art. 16 d ust. 5-9). Rozwiązanie to, na etapie konsultacji, było postulowane przez stronę samorządową Komisji Wspólnej Rządu i Samorządu Terytorialnego. Jego celem jest efektywne wykorzystanie dostępnych zasobów w samorządach. Taki model współpracy w realizacji zadań samorządowych jest już spotykany w JST. Przykładem są centra usług wspólnych, zajmujące się np. obsługą administracyjną placówek oświatowych. Kierownik jednostki wyznaczonej do realizacji zadań z zakresu cyberbezpieczeństwa będzie odpowiedzialny za realizację obowiązków przez jednostki, które obsługuje, np. w zakresie wdrożenia i utrzymania Systemu Zarządzania Bezpieczeństwem Informacji.

Do wyznaczenia jednostki odpowiedzialnej stosowane będą odpowiednio przepisy art. 74 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym, art. 5 ust. 2-4 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym, art. 8 ustawy z dnia 5 czerwca 1998 r. o

samorządzie województwa. Przepisy ustawy umożliwią także docelowo współpracę w zakresie cyberbezpieczeństwa pomiędzy gminami a powiatami, tak aby zapewnić jeszcze większą skuteczność, prawidłową realizację obowiązków i zmitygować koszty.

Podmioty publiczne, dla których jednostka wyznaczona realizuje obowiązki z zakresu cyberbezpieczeństwa będą musiały współpracować z tą jednostką w zakresie przekazywania informacji o incydentach i wykonywania decyzji kierownika tej jednostki w zakresie systemu zarządzania bezpieczeństwem informacji. Będą obowiązane również publikować na swojej stronie internetowej adres strony internetowej jednostki wyznaczonej zawierające informacje o cyberbezpieczeństwie, a kierownik jednostki będzie obowiązany uczestniczyć w szkoleniach z zakresu cyberbezpieczeństwa, jeżeli prowadzone są przez jednostkę wyznaczoną.

Jednostka wyznaczona zgłaszać będzie w imieniu podmiotu publicznego wczesne ostrzeżenie, zgłoszenie, sprawozdanie okresowe i sprawozdanie końcowe. Będzie wskazywać również osobę kontaktową do podmiotów publicznych, które realizują zadania z zakresu cyberbezpieczeństwa. Zobowiązana będzie korzystać z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 w celu realizacji obowiązków z zakresu cyberbezpieczeństwa (system S46).

Proponowane przepisy w znacznym stopniu ułatwią wdrażanie i realizację obowiązków z zakresu cyberbezpieczeństwa szczególnie w tych jednostkach samorządu terytorialnego, które zmagają się z problemami kadrowymi, czy niewystarczającymi środkami finansowymi.

Z wyrazami szacunku
Rafał Rosiński
Podsekretarz Stanu
/dokument podpisany elektronicznie/

Do wiadomości:

1) Pan Donald Tusk, Prezes Rady Ministrów
2) Pan Jan Maciej Czajkowski, Współprzewodniczący Zespołu ds. Społeczeństwa Informacyjnego KWRiST

telefon: +48 22 245 59 13
adres email: sekretariat.dpis@cyfra.gov.pl
www.gov.pl/cyfryzacja

ul. Królewska 27
00-060 Warszawa