Mimo realizacji projektu „Cyberbezpieczny Samorząd” poziom odporności urzędów gmin na cyberataki wciąż nieznany

21.7.2026 - | Najwyższa Izba Kontroli

Projekt „Cyberbezpieczny Samorząd”, którego celem jest poprawa odporności gmin na zagrożenia teleinformatyczne, był realizowany zgodnie z obowiązującymi procedurami, jednak kontrola NIK wykazała, że zabrakło systemowego podejścia do wzmacniania cyberbezpieczeństwa w gminach oraz oceny rzeczywistych efektów programu. W konsekwencji nie można stwierdzić, w jakim stopniu dofinansowane urzędy faktycznie zwiększyły swoją odporność na cyberataki. Nadzorujące projekt Centrum Projektów Polska Cyfrowa nie wymagało od samorządów przeprowadzenia audytów bezpieczeństwa ani przed przyznaniem dofinansowania, ani po zakończeniu prac. W praktyce oznaczało to akceptację wszystkich wydatków na sprzęt i oprogramowanie bez weryfikacji ich rzeczywistej przydatności.

Rosnąca popularność usług cyfrowych i rozwój nowych technologii to przyczyny zwiększonego zagrożenia cyberprzestępczością. Dodatkowo sytuacja związana z wojną na Ukrainie oraz wojną hybrydową sprawia, że systematycznie rośnie liczba ataków hakerskich na instytucje publiczne. W odpowiedzi na te zagrożenia uruchomiono projekt „Cyberbezpieczny Samorząd”, którego celem jest zwiększenie odporności jednostek samorządu terytorialnego na zagrożenia teleinformatyczne oraz poprawa ich zdolności do zapobiegania, wykrywania i reagowania na incydenty bezpieczeństwa.

Projekt skierowano do wszystkich jednostek samorządu terytorialnego w Polsce – łącznie 2807 gmin, powiatów i województw. Mogły one uzyskać dofinansowanie w formie grantów finansowanych ze środków europejskich. Z budżetu wynoszącego około 1,5 mld zł większość środków (80%) przeznaczono na zakup sprzętu, oprogramowania i usług wdrożeniowych, a pozostałą część na opracowanie procedur, audyty oraz szkolenia. Realizacja grantów trwała do 24 miesięcy, nie dłużej niż do 30 czerwca 2026 r.

Projekt jest realizowany w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), którego celem jest wspieranie cyfrowej transformacji kraju poprzez poszerzenie dostępu do ultraszybkiego internetu szerokopasmowego, podniesienie kompetencji cyfrowych pracowników instytucji sektora publicznego, zwiększenie dostępu do nowoczesnych e-usług i poprawę cyberbezpieczeństwa.

Kontrolą objęto 19 jednostek: 12 urzędów miast i gmin, 5 starostw powiatowych oraz Centrum Projektów Polska Cyfrowa (CPPC) i NASK.

Najważniejsze ustalenia kontroli

W ramach konkursu grantowego w 2023 r. jednostki samorządu terytorialnego (jst) złożyły 2614 wniosków o dofinansowanie na łączną kwotę 1,538 mld zł. Oceniono 2515 wniosków o wartości 1,486 mld zł, a w 2024 r. podpisano 2497 umów grantowych na kwotę 1,475 mld zł. Na koniec sierpnia 2025 r. realizowano 2490 projektów o łącznej wartości 1,471 mld zł.

Do tego czasu grantobiorcy (jst) złożyli jedynie 26 wniosków o płatność w celu rozliczenia grantów na kwotę 16 mln zł, z czego do dnia zakończenia kontroli (5 września 2025 r.) rozliczono zaledwie

17 wniosków o wartości 10,7 mln zł. Łączna kwota wykorzystanych środków na dzień 31 sierpnia 2025 r. wyniosła 1,122 mld zł, co stanowiło 62,4% całkowitego budżetu projektu.

„Cyberbezpieczny Samorząd" w liczbach na dzień 31 sierpnia 2025 r.

Realizacja projektu „Cyberbezpieczny Samorząd" przebiegała zgodnie z jego założeniami i przyjętymi procedurami, jednak nie wiadomo w jakim stopniu przyczynił się on do zwiększenia bezpieczeństwa informacji w jednostkach samorządu terytorialnego.

Najwyższa Izba Kontroli krytycznie oceniła same założenia i konstrukcję konkursu grantowego przygotowaną przez CPPC. Urzędnicy popełnili błędy metodologiczne na dwóch etapach. Przy składaniu wniosków CPPC nie wymagało od jednostek samorządu terytorialnego przeprowadzenia audytu ani przedstawienia jakiejkolwiek obiektywnej oceny ich aktualnego poziomu cyberbezpieczeństwa. Przyznawano granty wyłącznie w oparciu o samoocenę (niejednokrotnie błędną, jak zidentyfikowała NIK) – dokonaną przez jednostki samorządu terytorialnego – jakich konkretnie zabezpieczeń danemu urzędowi brakuje.

Z kolei przy rozliczeniu projektu nie wprowadzono mechanizmu, który uzależniałby uznanie wydatków za kwalifikowalne (prawidłowo wydane) od tego, czy samorząd realnie podniósł swój poziom odporności na cyfrowe zagrożenia.

Głównym celem „Cyberbezpiecznego Samorządu" miało być realne wzmocnienie odporności urzędów na incydenty w systemach informacyjnych i ataki hakerskie. Tymczasem przez brak procedur badających stan „przed" i „po", CPPC straciło możliwość zweryfikowania, czy i w jakim stopniu publiczne pieniądze przyniosły zamierzony skutek. NIK ocenia takie podejście jako nierzetelne i stwarzające ryzyko nieefektywnego, bezcelowego wydawania funduszy.

NIK zauważa, że celem grantu jest zwiększenie poziomu bezpieczeństwa, zatem serwer powinien być wykorzystywany do uruchamiania systemów bezpieczeństwa wdrożonych w ramach projektu grantowego, a wszelkie inne aplikacje powinny działać na odrębnej infrastrukturze. Tymczasem w trakcie realizacji projektów grantowych w ramach „Cyberbezpiecznego Samorządu" dopuszczono do sytuacji, w której na nowo zakupionych serwerach samorządów instalowano i uruchamiano jednocześnie dwa rodzaje oprogramowania: systemy dziedzinowe (codzienne programy urzędowe, np. systemy podatkowe, programy do obsługi petentów, bazy danych mieszkańców) oraz systemy bezpieczeństwa (oprogramowanie ochronne wdrożone w ramach unijnego grantu). NIK jednoznacznie wskazuje, że taka praktyka jest nielegalna i bezpośrednio łamie rozporządzenie w sprawie Krajowych Ram Interoperacyjności (KRI). Oprócz aspektu prawnego, niesie to ze sobą także ryzyko techniczne, gdyż prowadzi to do potencjalnego konfliktu o zasoby serwera, co może obniżyć stabilność i niezawodność systemów bezpieczeństwa.

W wyniku badania 30 umów zawartych przez CPPC z grantobiorcami ustalono, że okres liczony od dnia zakończenia oceny ich wniosków o przyznanie grantu do dnia podpisania umowy wynosił od 3 do 8 miesięcy, czyli średnio około pół roku. Nawet w sytuacji, gdy gmina lub powiat dostarczyły do CPPC kompletny i w pełni poprawny zestaw dokumentów niezbędnych do podpisu, na sam podpis urzędników z Warszawy czekało się od 14 do nawet 182 dni (średnio 3 miesiące).

Kontrola wykazała, że CPPC nie jest w stanie osiągnąć dwóch kluczowych wskaźników realizacji projektu „Cyberbezpieczny Samorząd": jednego wskaźnika produktu (*Liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji)* oraz jednego wskaźnika rezultatu (*Liczba jednostek samorządu terytorialnego wspartych w zakresie cyberbezpieczeństwa).*

Wystąpiły zaniedbania w bieżącym raportowaniu postępów prac. Instytucje nadzorujące realizację projektu nie miały aktualnych danych o tym, jak realnie idą prace w samorządach, ponieważ CPPC aż do 1 lipca 2025 r. nie wpisywało na bieżąco wartości wskaźników do wniosków o płatność.

Obszarem, w którym kontrola NIK nie wykazała systemowych zaniedbań po stronie CPPC, był bieżący nadzór nad Instytutem Badawczym NASK, który pełnił rolę oficjalnego Partnera projektu.

NASK prawidłowo wywiązał się z obowiązku organizacji naboru wniosków w ramach konkursu „Cyberbezpieczny Samorząd". Stworzono dedykowane narzędzie informatyczne (system LSI), przez które urzędy składały dokumenty. NASK zapewnił także samorządom pomoc techniczną i merytoryczną w trakcie naboru, a wsparcie to jest kontynuowane również w fazie wdrażania projektów.

Od początku projektu do 31 lipca 2025 r. NASK zaangażował do pracy duży zespół: 121 pracowników oraz 21 ekspertów oceniających wnioski. NIK potwierdziła, że osoby na kluczowych stanowiskach (Kierownik Projektu, Kierownik Biznesowy, Lider Merytoryczny) oraz 25 pracowników odpowiedzialnych za merytoryczną ocenę wniosków posiadały odpowiednie wykształcenie i doświadczenie zawodowe w dziedzinie cyberbezpieczeństwa. Stwierdzono jednak, że Kierownik Projektu – kluczowy manager – pracował bez oficjalnego powołania przez ponad 18 miesięcy.

Kontrola NIK przeprowadzona na losowej próbie 15 grantów wykazała, że proces oceny wniosków o przyznanie grantów działał bez zarzutu. Wnioski przesyłane przez gminy i powiaty spełniały kryteria formalne i merytoryczne zawarte w regulaminie. Eksperci NASK sprawnie weryfikowali dokumenty, a następnie pracownicy NASK kompletowali pełną dokumentację i przekazywali gotowe umowy o przyznaniu grantu do podpisania do CPPC.

Stwierdzono natomiast brak staranności przy rozliczaniu grantów. Kontrolerzy NIK zbadali próbę 15 wniosków o rozliczenie grantu przesłanych przez samorządy. Aż 13 z 15 tych wniosków zostało przez NASK oficjalnie zatwierdzonych, mimo że zawierały poważne błędy, były sporządzone wadliwie lub brakowało w nich wymaganych, kluczowych załączników. Świadczy to o braku należytej kontroli nad tym, jak samorządy wydatkowały i dokumentowały przyznane im publiczne pieniądze.

Kolejny problem dotyczy obowiązkowych audytów bezpieczeństwa informacji, które samorządy musiały przeprowadzić na koniec realizacji grantu. CPPC, które odpowiadało za przygotowanie dokumentacji konkursowej, w żaden sposób nie ustandaryzowało tych audytów. Każdy samorząd mógł je przeprowadzić według własnego uznania. Wyniki audytu bezpieczeństwa informacji w urzędzie na zakończenie grantu nie miały znaczenia dla rozliczenia grantu.

Badaniem objęto prawidłowość wykorzystania przez jednostki samorządu terytorialnego 17 najwyższych wartościowo grantów w ramach projektu „Cyberbezpieczny Samorząd" finansowanego z Programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027, wybranych spośród tych urzędów jednostek samorządu terytorialnego, które najwcześniej otrzymały wszystkie transze grantu. Łączna wartość grantów przyznanych kontrolowanym urzędom wyniosła 13 mln zł. Na dzień zakończenia poszczególnych kontroli w badanych urzędach, wartość wydatkowanych przez jst środków wyniosła 7,7 mln zł (z uwzględnieniem wkładu własnego w łącznej kwocie 932 tys. zł), co stanowiło 59% środków przyznanych na realizację projektów grantowych. Ponadto, zaangażowanie w umowach jst z wykonawcami w ramach badanych umów grantowych wynosiło 1,5 mln zł, co stanowiło 11,8% łącznej kwoty środków przeznaczonych na realizację projektów grantowych w kontrolowanych jst.

W dokumentach strategicznych większości kontrolowanych urzędów (16 z 17) nie uwzględniono

zagadnień dotyczących zwiększenia poziomu cyberbezpieczeństwa. Tłumaczono to najczęściej małą istotnością tego zagadnienia w momencie opracowywania tych strategii, tj. w latach 2014–2020, a także brakiem prowadzenia analiz w tym zakresie i brakiem wymogów prawnych.

Nieprawidłowości w realizacji grantów stwierdzono w sześciu z siedemnastu kontrolowanych urzędów (36%). Nie miały one jednak zasadniczego wpływu na prawidłowość wykorzystania grantu, z wyjątkiem Urzędu Gminy Świerklany. Dotyczyły one m.in.:

- braku zabezpieczenia interesów zamawiającego, co było działaniem nierzetelnym (Urząd Miasta i Gminy w Górze, Urząd Gminy Kłodzko);
- zakupu komponentów serwera w postaci 14 pamięci RAM o wartości 23 800 zł, co nie mieściło się bezpośrednio w katalogu działań (usług) na jakie można przeznaczyć środki projektu. Ponadto zakup ten nie był ujęty we wniosku o przyznanie grantu (Urząd Miasta i Gminy w Górze);

• wskazania we wniosku o dofinansowanie projektu *Poprawa cyberbezpieczeństwa* informacji niezgodnej ze stanem faktycznym, że starostwo posiada wdrożony i audytowany System Zarządzania Bezpieczeństwem Informacji (SZBI), co było działaniem nierzetelnym (Starostwo Powiatowe w Białobrzegach).

W przypadku Urzędu Gminy Świerklany NIK negatywnie oceniła działalność Urzędu w zakresie realizacji projektu grantowego. Stwierdzono m.in. nieprawidłowości dotyczące: nieuzasadnionego opóźnienia odbioru I etapu przedmiotu umowy na wykonanie usługi doradczej w ramach grantu; udzielenia zamówienia publicznego na dostawę urządzeń i oprogramowania bez zastosowania przepisów ustawy Prawo zamówień publicznych oraz nierzetelnej realizacji przedmiotu tego zamówienia przez wykonawcę; wdrożenia Polityki Bezpieczeństwa Teleinformatycznego, która zawierała nierzetelne zapisy i postanowienia niezgodne z przepisami rozporządzenia KRI, a także nieprzeprowadzenia w 2024 r. okresowego audytu w zakresie bezpieczeństwa informacji.

Kontrola NIK wykazała, że zdefiniowane przez CPPC wskaźniki realizacji projektów grantowych, tak produktu, jak i rezultatu, nie były w żaden sposób powiązane z faktycznym wzrostem poziomu cyberbezpieczeństwa u grantobiorców (jst), a jedynie z liczbą dokonanych zakupów i przeszkolonych osób. W pięciu objętych kontrolą urzędach (29%) na etapie zawierania umowy o powierzenie grantu nie wskazano wskaźników produktu i rezultatu lub nie podano ich wartości.

Zakupione w ramach kontrolowanych projektów grantowych urządzenia i oprogramowanie zostały zainstalowane i były użytkowane lub były na etapie wdrożenia, z wyjątkiem Urzędu Gminy Świerklany. Szkolenia zostały przeprowadzone lub były zaplanowane do realizacji. Zamówione w ramach grantu audyty bezpieczeństwa informacji zostały wykonane. Sformułowane w nich wnioski/rekomendacje zostały w części wdrożone, a pozostałe przyjęto do realizacji.

W większości skontrolowanych urzędów stwierdzono nieprawidłowości w zakresie zapewnienia bezpieczeństwa informacji. Pomimo przystąpienia do projektu „Cyberbezpieczny Samorząd”, w ponad połowie kontrolowanych urzędów nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), który jest kluczowym elementem zapewnienia cyberbezpieczeństwa. Spośród dziewięciu urzędów, w których przed przystąpieniem do projektu grantowego brak było SZBI wymaganego rozporządzeniem KRI, w siedmiu z nich (77%) przewidziano opracowanie SZBI w ramach grantu w zakresie obszaru organizacyjnego, natomiast w dwóch urzędach (23%) działania takie nie były planowane.

W ośmiu urzędach (47%) w 2023 r. lub 2024 r. nie przeprowadzono obowiązkowego audytu

z zakresu bezpieczeństwa informacji, co było niezgodne z rozporządzeniem KRI, lub audyt przeprowadzono nierzetelnie, bądź z naruszeniem zasady niezależności i obiektywizmu audytu. Powyższe nieprawidłowości tłumaczono m.in. brakiem pracowników posiadających niezbędną wiedzę i doświadczenie dla przeprowadzenia takiego audytu.

Inne nieprawidłowości w zakresie zapewnienia bezpieczeństwa informacji dotyczyły m.in. niewłaściwego zabezpieczenia serwerowni urzędów, nieodbierania uprawnień do systemów urzędu byłym pracownikom, niewłaściwego sporządzania kopii zapasowych.

Wnioski

Do Ministra Cyfryzacji we współpracy z Ministrem Funduszy i Polityki Regionalnej oraz Dyrektorem CPPC o:

Zapewnienie powiązania kwalifikowalności wydatków z osiągnięciem zakładanego wzrostu poziomu cyberbezpieczeństwa w przypadku realizowania kolejnych projektów w tym obszarze, w szczególności poprzez:

- uwzględnienie w przyszłych projektach wymogu przeprowadzenia ustandaryzowanego audytu bezpieczeństwa informacji zarówno przed przystąpieniem do projektu, jak i po jego zakończeniu;
- określenie wskaźników realizacji projektów grantowych, tak produktu, jak i rezultatu, pozwalających na zmierzenie wpływu działań zrealizowanych w ramach uczestnictwa w projekcie na poziom cyberbezpieczeństwa.

https://www.nik.gov.pl/aktualnosci/mimo-realizacji-projektu-cyberbezpieczny-samorzad-poziom-odpornosci-urzedow-gmin-na-cyberataki-wciaz-nieznany.html