NIK ujawnia słabe punkty cyberbezpieczeństwa w samorządach

Kategoria: Komunikacja i Transport
Opublikowano: czwartek, 17, kwiecień 2025 11:38
Katarzyna Sekuła

Z ustaleń Najwyższej Izby Kontroli wynika, że jednostki samorządu terytorialnego w Polsce nie realizują w sposób prawidłowy i skuteczny zadań związanych z zapewnieniem bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych. Skala nieprawidłowości ujawnionych w wyniku kontroli przeprowadzonej w 24 jednostkach – w tym 17 urzędach gmin i siedmiu starostwach powiatowych – jest niepokojąca. W aż 71 procentach badanych urzędów stwierdzono brak przygotowania do zapewnienia funkcjonowania systemów IT w sytuacjach kryzysowych.

Kontrola obejmowała okres od stycznia 2023 roku do września 2024 roku. Jej celem było sprawdzenie, czy samorządy rzetelnie zarządzają bezpieczeństwem informacji, identyfikują i chronią dane, oraz czy posiadają procedury umożliwiające kontynuowanie pracy urzędu w razie awarii, ataku hakerskiego czy katastrofy naturalnej. Wnioski z raportu NIK wskazują na liczne niedopatrzenia zarówno organizacyjne, jak i techniczne.

W większości skontrolowanych urzędów nie zidentyfikowano w sposób pełny zbiorów danych wymagających ochrony, co oznacza, że niektóre informacje – w tym dane niebędące danymi osobowymi, ale istotne dla funkcjonowania instytucji – nie były objęte właściwymi zabezpieczeniami. Tylko nieliczne jednostki posiadały wdrożony i aktualizowany System Zarządzania Bezpieczeństwem Informacji, a wiele nie posiadało dokumentów kluczowych dla przygotowania do sytuacji awaryjnych, takich jak polityki ciągłości działania, plany odtworzeniowe czy scenariusze awaryjne.

W ocenie NIK urzędy nie testowały skuteczności istniejących procedur. Często również nie zapewniano odpowiedniego zabezpieczenia serwerowni przed zagrożeniami zewnętrznymi ani nie prowadzono okresowych analiz ryzyka. Brakowało także szkoleń dla pracowników zajmujących się przetwarzaniem informacji, co dodatkowo zwiększało ryzyko błędów i naruszeń. W części przypadków umowy zawierane z dostawcami usług IT, sprzętu czy oprogramowania nie zawierały zapisów dotyczących obowiązku zachowania poufności przetwarzanych danych.

Urzędy nie były również przygotowane do reagowania w razie utraty danych lub ataku na infrastrukturę cyfrową. Wiele z nich nie tworzyło kopii zapasowych w sposób regularny, nie testowało ich przywracania i nie przechowywało ich poza lokalizacją, w której zostały wytworzone. Nie weryfikowano także uprawnień użytkowników systemów informatycznych – w tym przypadków, gdy pracownik kończył pracę, a jego dostęp do systemów nadal pozostawał aktywny.

Pomimo ujawnienia 222 nieprawidłowości, aż 51 z nich udało się wyeliminować już w trakcie trwania kontroli. Najwyższa Izba Kontroli podkreśla jednak, że wiele urzędów nadal nie podejmuje działań systemowych, które mogłyby realnie zwiększyć bezpieczeństwo i odporność informatyczną administracji publicznej.

W związku z wynikami kontroli, NIK rekomenduje Ministerstwu Cyfryzacji podjęcie stałego wsparcia jednostek samorządu terytorialnego w zakresie wdrażania rozwiązań organizacyjnych i technicznych związanych z bezpieczeństwem informacji i zapewnieniem ciągłości działania urzędów. Z kolei do starostów, prezydentów miast, burmistrzów i wójtów skierowano apel o niezwłoczne wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji, jego bieżącą aktualizację, opracowanie planów ciągłości działania i ich testowanie, organizację cyklicznych szkoleń oraz zapewnienie odpowiedniej ochrony infrastruktury informatycznej.

NIK przypomina także, że skuteczna ochrona danych oraz sprawne działanie urzędu w sytuacji

kryzysowej jest dziś nie tylko obowiązkiem prawnym, ale elementem podstawowej odporności administracji publicznej – zwłaszcza w kontekście rosnących zagrożeń cybernetycznych i hybrydowych.

Pełen raport dostępny w załączniku.

Źródło: NIK