Gmina Zbrosławice

ul. Oświęcimska 2 • 42-674 Zbrosławice

Tel. 32 233 70 12 • fax. 32 233 71 00

www.zbroslawice.pl • email: urzad@zbroslawice.pl

Zbrosławice, 7.5.2025 r.

RG.0003.5.2025

RADA GMINY
Zbrosławice

Szanowny Pan
Andrzej Glomb
Radny Gminy Zbrosławice

W odpowiedzi na Pana Interpelację z dnia 25 kwietnia 2025 r., dotyczącą kontroli w Urzędzie Gminy Zbrosławice, przeprowadzonej w zakresie „Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego" przeprowadzoną przez Najwyższą Izbę Kontroli delegaturę w Katowicach, odpowiadam na zadane pytania:

- Kontrola trwała od 21 czerwca do 4 września 2024 r. i dotyczyła okresu od 1 stycznia 2023 r., aż do dnia zakończenia kontroli.
- Zakres kontroli był obszerny, dotyczył całego spektrum zapewnienia bezpieczeństwa informacji przetwarzanych przez Urząd, oraz ciągłości działania systemów informatycznych, tj. spraw organizacyjnych, kadrowych, zasad przetwarzania danych (zarówno tych w formie papierowej jak i elektronicznej), istniejących procedur, stosowanych praktyk, istniejących protokołów, okresowych przeglądów, przeprowadzonych audytów i szkoleń pracowników, aż do zabezpieczeń technicznych: fizycznych oraz sprzętu i oprogramowania oraz ich konfiguracji. Dokonano także krzyżowej kontroli zgodności poszczególnych dokumentów i procedur oraz praktyk.

W wyniku kontroli stwierdzono nieprawidłowości[1] w dwóch z trzech badanych obszarów.

W obszarze: organizacja bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych

- wykazano brak pełnej identyfikacji usług i technicznych elementów mających wpływ na przerwy w działaniu systemów, niektórych procedur w Polityce Ciągłości Działania, takich jak częstotliwość sporządzania kopii zapasowych oraz czas ich retencji (wspomniane polityki były wprowadzone w systemach informatycznych i były stosowane w praktyce, natomiast nie były opisane „papierowo")
- brak wskazania konkretnych osób odpowiedzialnych za poszczególne czynności w Planie Ciągłości Działania (istniejące zapisy zostały uznane za zbyt ogólne)
- stwierdzono potrzebę szybszego wprowadzenia zmian w dokumentacji Urzędu, po otrzymaniu uwag i zaleceń od Audytora (kilka problemów było wskazanych w przeprowadzonym audycie wewnętrznym, ale istniała zwłoka w realizacji opracowania nowej dokumentacji).

W obszarze: wdrożone i wykorzystywane rozwiązania organizacyjne i techniczne zapewniające bezpieczeństwo informacji oraz ciągłość działania

- w wyrywkowej próbie audytu uprawnień 15 osób (użytkowników) wykazano istniejącą zwłokę w odebraniu uprawnień / resetowaniu haseł, oraz w dwóch przypadkach nadanie uprawnień bez udokumentowania tego odpowiednim wnioskiem. Większość błędów tego typu wynikała z niepoprawnego przepływu informacji między wydziałami Urzędu. Niektóre czynności były

[1] Dokładne i pełne zapisy dotyczące przedmiotowej kontroli są zawarte w dokumencie „Wystąpienie Pokontrolne" nr LKA.410.14.5.2024, opublikowane w serwisie informacyjnym Najwyższej Izby Kontroli https://www.nik.gov.pl/kontrole/wyniki-kontroli-nik/kontrola,25231.html .

Justyna Cieśla
Wydział Organizacyjny Rada Gminy
Główny Specjalista

Urząd Gminy Zbrosławice • ul. Oświęcimska 2
tel. 32 233 75 82
email: rada@zbroslawice.pl

wykonywane na polecenie ustne, nie zawsze terminowo była przekazywana informacja o zakończeniu stosunku pracy itp.

- w dwóch przypadkach, system nie wymuszał okresowej zmiany haseł systemowych, co było zgodne z aktualnymi rekomendacjami CSIRT NASK, lecz niezgodne z zapisami w wewnętrznie przyjętym wcześniej dokumencie „Instrukcja Zarządzania Systemem Informatycznym".
- fakt przechowywania części kopii zapasowych w tym samym pomieszczeniu, co ich miejsce przetwarzania (pomieszczenie powinno być inne, sytuacja była tymczasowa, spowodowana trwającym remontem – urządzenie przeniesiono, aby nie uległo uszkodzeniu z powodu nadmiernego zapylenia).

W obszarze: działania w celu zapobiegania incydentom bezpieczeństwa informacji nie stwierdzono nieprawidłowości.

Na zakończenie kontroli wskazano uwagę, aby bezzwłoczne podejmować działania istotne z punktu widzenia bezpieczeństwa informacji oraz wnioski:

1. Wskazanie w planie ciągłości działania osób odpowiedzialnych za prawidłową i terminową realizację działań w nim przewidzianych.
2. Dokonanie przeglądu nadanych uprawnień pracowników do systemów informatycznych i usunięcie uprawnień niezgodnych z zakresem obowiązków.
3. Zapewnienie bezzwłocznego blokowania dostępu do kont pracownikom, po zakończeniu stosunku pracy.
4. Ustawienie w systemach wymuszenia zmiany hasła nie rzadziej niż co 30 dni, zgodnie z wewnętrznie przyjętymi zasadami. Dokonanie przeglądu Instrukcji zarządzania systemem informatycznym, pod kątem aktualizacji jej zapisów.

Wszystkie uwagi i zastrzeżenia NIK zostały przeanalizowane i niezwłocznie podjęto działania naprawcze. Część z nich wdrożono już w trakcie trwania kontroli. Przede wszystkim, do utworzonego Wydziału Informatyki zatrudniono dodatkową osobę, co organizacyjnie pozwoliło na realizację zastępstw, podział obowiązków i zwiększyło dostępność Administratora Systemów Informatycznych, co w efekcie umożliwia szybsze podejmowanie czynności istotnych z punktu widzenia bezpieczeństwa informacji. W odpowiedzi na wnioski pokontrolne:

1. Dokonano przeglądu Planu Ciągłości Działania. Zaktualizowano i uzupełniono zapisy dotyczące osób odpowiedzialnych za konkretne czynności. Doprecyzowano także sytuacje, w których należy dokonać aktualizacji Planu.
2. Dokonano przeglądu uprawnień pracowników Urzędu do systemów informatycznych. W wyniku dokonanego przeglądu wyłączono jeszcze jedno konto byłego pracownika, które było aktywne.
3. Przyjęto praktykę o przekazywaniu każdorazowo informacji z kadr do ASI, o zakończeniu stosunku pracy, w celu odebrania uprawnień danemu użytkownikowi, nawet w wypadku, niezłożenia wniosku o odebranie uprawnień przez jego bezpośredniego przełożonego.
4. Dokonano przeglądu systemów informatycznych, w przypadkach, które odstępowały od przyjętych zasad, zastosowano systemowe wymuszanie zmiany haseł co 30 dni. Jednocześnie przy następnej zmianie procedur wewnętrznych zaplanowano odstąpienie od tej zasady, zgodnie z aktualnymi rekomendacjami CSIRT-NASK.
5. Zaplanowano dokonanie kompleksowego przeglądu Instrukcji Zarządzania Systemem Informatycznym, w ramach realizowanego przez Urząd projektu „Cyberbezpieczny Samorząd". Stworzenie aktualnej i profesjonalnej dokumentacji w tym zakresie jest jednym z zadań ww. projektu, a uwagi i doświadczenia zdobyte podczas przeprowadzenia kontroli zostaną wykorzystane do poprawy jakości w tworzeniu dokumentacji i procedur.

Z poważaniem

WÓJT

Katarzyna Zyga

Otrzymują:
1. Adresat.
2. Ad acta

Justyna Cieśla
Wydział Organizacyjny Rada Gminy
Główny Specjalista

Urząd Gminy Zbrosławice • ul. Oświęcimska 2
tel. 32 233 75 82
email: rada@zbroslawice.pl