NAJWYŻSZA IZBA KONTROLI

DELEGATURA WE WROCŁAWIU

LWR.410.13.4.2024

Pan
Rafael Rokaszewicz
Prezydent Miasta Głogowa
Urząd Miejski w Głogowie
Rynek 10
67-200 Głogów

WYSTĄPIENIE POKONTROLNE

P/24/004 - „Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego”

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miejski w Głogowie, Rynek 10, 67-200 Głogów[1].
Kierownik jednostki kontrolowanej	Rafael Rokaszewicz, Prezydent Miasta Głogowa[2], od 8 grudnia 2014 r.
Zakres przedmiotowy kontroli	Rozwiązania organizacyjne i techniczne w zakresie zapewnienia bezpieczeństwa przetwarzania informacji oraz zapewnienia ciągłości działania w urzędzie i ich stosowanie.
Okres objęty kontrolą	Od 1 stycznia 2023 r. do dnia zakończenia kontroli w 2024 r.[3], (także okresy wcześniejsze w zakresie uczestnictwa w programie Cyfrowa Gmina/Cyfrowy Powiat).
Podstawa prawna podjęcia kontroli	Artykuł 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[4].
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura we Wrocławiu
Kontroler	Cezary Mazik, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LWR/87/2024 z dnia 3 czerwca 2024 r.

(akta kontroli: str. 1, 4)

[1] Dalej: Urząd.
[2] Dalej: Prezydent.
[3] Czynności kontrolne zakończono w dniu 27 sierpnia 2024 r.
[4] Dz. U. z 2022 r. poz. 623; dalej: ustawa o NIK.

II. Ocena ogólna[5] kontrolowanej działalności

OCENA OGÓLNA

Najwyższa Izba Kontroli ocenia pozytywnie działalność kontrolowanej jednostki w zbadanym zakresie.

Uzasadnienie oceny ogólnej

Podstawą pozytywnej oceny ogólnej były oceny cząstkowe, dotyczące trzech obszarów, które zostały poddane kontroli. W szczególności w badanym okresie stosowano dokumentację składającą się na System Zarządzania Bezpieczeństwem Informacji[6] i Politykę Ochrony Danych Osobowych, uwzględniającą wymogi odpowiednio rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[7] oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[8]. Przeprowadzono także przegląd SZBI oraz okresowy audyt wewnętrzny z zakresu bezpieczeństwa informacji.

Ponadto w Urzędzie prawidłowo zidentyfikowano zbiory danych podlegających zabezpieczeniu oraz kluczowe elementy infrastruktury i usług IT. Prowadzono także niezbędne analizy ryzyka oraz sporządzono odpowiednią dokumentację w celu m.in. zapewnienia ciągłości działania, określenia bezpiecznych zasad pracy zdalnej, określenia zasad tworzenia i przechowywania kopii zapasowych, nadawania i odbierania pracownikom uprawnień do pracy w systemach informatycznych oraz postępowania w sytuacjach wystąpienia lub podejrzenia wystąpienia incydentu w zakresie bezpieczeństwa informacji.

Prawidłowo określono i zapewniono także niezbędne zasoby osobowe i techniczne w celu zapewnienia bezpieczeństwa informacji oraz przeprowadzano szkolenia pracowników odpowiedzialnych za przetwarzanie informacji. Wdrożono również właściwie rozwiązania organizacyjne i techniczne zapobiegające możliwości instalowania nieautoryzowanego oprogramowania, zabezpieczono pomieszczenie serwerowni, a także regularnie tworzono i testowano kopie zapasowe danych.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[9] kontrolowanej działalności

OBSZAR

1. Organizacja bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych

Opis stanu faktycznego

1.1. Identyfikacja zbiorów danych wymagających ochrony w Urzędzie dokonywana była corocznie jako element zarządzania ryzykiem w bezpieczeństwie informacji. Oceny wagi tych zbiorów oraz systemów teleinformatycznych, w których były one przetwarzane, dokonywano pod kątem wpływu braku funkcjonowania lub nieprawidłowego ich funkcjonowania na: bezpieczeństwo ludzi oraz zasobów informacyjnych; ciągłości działania oraz realizowania funkcji i zadań Urzędu, które byłyby niemożliwe do realizacji bez systemu teleinformatycznego; możliwości

[5] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[6] Dalej: SZBI.
[7] Dz. U. poz. 773, dalej: rozporządzenie KRI.
[8] Dz. Urz. UE L 119/1 z 4 maja 2016 r., str. 1, ze zm.; dalej: RODO.
[9] Oceny cząstkowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena cząstkowa może być sformułowana jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej.

realizowania konstytucyjnych praw i obowiązków obywatela oraz zaufania obywateli do władzy publicznej.

Według stanu na 11 czerwca 2024 r., w wyniku przeprowadzonej w wyżej opisany sposób inwentaryzacji, zidentyfikowano 55 zbiorów danych i systemów informatycznych o kategorii krytycznej wymagających ochrony.

Dodatkowo w ramach Rejestru Czynności Przetwarzania Danych Osobowych zidentyfikowano 283 czynności, w których przetwarzano dane osobowe. Dla każdej czynności wskazano m.in.: cel przetwarzania, podstawę prawną przetwarzania, właściciela procesu, kategorie osób, danych i odbiorców, sposób przetwarzania i pozyskiwania danych, okres ich przechowywania, ogólny opis środków bezpieczeństwa danych oraz informacje na temat ewentualnego transferu danych do krajów trzecich.

(akta kontroli: str. 40-44 plik 1, 3-5, 9)

1.2. W Urzędzie opracowano i wdrożono SZBI, o którym mowa w § 19 ust. 1 w zw. z ust. 3 rozporządzenia KRI.

Podstawowy elementem SZBI była Polityka Bezpieczeństwa Informacji[10], przyjęta Zarządzeniem nr 21/2021 Prezydenta Miasta Głogowa z dnia 6 sierpnia 2021 r. w sprawie: wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Głogowie[11]. Została ona właściwie przedstawiona i zakomunikowana pracownikom, a jej postanowienia były przedmiotem prowadzonych szkoleń wewnętrznych, zakończonych testami.

Zgodnie z postanowieniami PBI, odpowiadającym za jej opracowanie, nadzór nad realizacją, przegląd i modyfikację był Inspektor Ochrony Danych[12], a osobami odpowiadającymi za jej wdrożenie byli naczelnicy wydziałów i kierownicy komórek organizacyjnych. Natomiast nadzór nad realizacją tych zadań został powierzony Sekretarzowi Gminy Miejskiej[13].

Częścią składową PBI, zatwierdzoną i zakomunikowaną pracownikom urzędu odpowiedzialnym za realizację określonych zadań, były następujące procedury:

- zarządzania infrastrukturą techniczną;
- klasyfikacji informacji;
- kontroli dostępu do informacji;
- bezpieczeństwa środowiskowego i fizycznego;
- bezpieczeństwa zasobów ludzkich;
- profilaktyki antywirusowej;
- stosowania urządzeń mobilnych i pracy na odległość;
- stosowania technik kryptograficznych;
- zarządzania ryzykiem w bezpieczeństwie informatycznym;
- współpracy z osobami trzecimi;
- postępowania z incydentami;
- wykonania kopii awaryjnej;
- przeglądu praw dostępu.

(akta kontroli: str. 40-44 plik 3-4)

[10] Dalej: PBI.
[11] Zmieniona Zarządzeniem nr 24/2022 Prezydenta Miasta Głogowa z dnia 14 lipca 2022 r. w sprawie zmian do Zarządzenia Prezydenta Miasta Głogowa Nr 21/2022 z dnia 6 sierpnia 2021 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Głogowie.
[12] Dalej: IOD.
[13] Dalej: Sekretarz.

1.3. Dokumentacja związana z ochroną danych osobowych uwzględniająca wymogi RODO została wprowadzona Zarządzeniem Nr 22/2021 Prezydenta Miasta Głogowa z dnia 6 sierpnia 2021 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych[14]. Została ona właściwie przedstawiona i zakomunikowana pracownikom, a jej postanowienia były przedmiotem prowadzonych szkoleń wewnętrznych, zakończonych testami.

Według PODO system ochrony danych osobowych w Urzędzie opierał się na inwentaryzacji danych, prowadzeniu rejestru czynności przetwarzania danych, zarządzaniu ryzykiem, zarządzaniu incydentami, zarządzaniu prywatnością przy uruchomieniu nowych projektów i inwestycji, zarządzaniu eksportem danych oraz zarządzaniu obsługą praw jednostki.

(akta kontroli: str. 40-44 plik 5)

1.4. W okresie objętym kontrolą w Urzędzie prowadzone były coroczne analizy ryzyka w związku z potrzebą zachowania ciągłości działania systemów informatycznych. Analizy te wykonywane były w ramach analiz ryzyka utraty integralności, dostępności lub poufności informacji, a jej wyniki w zakresie zapewnienia ciągłości działania wykorzystano przy tworzeniu i aktualizacji planu ciągłości działania. Prowadzona analiza poprzedzona była inwentaryzacją krytycznych zasobów informatycznych, a następnie określono dla nich listę obejmującą 51 zagrożeń/ryzyk z podziałem na zewnętrzne i wewnętrzne. Dla tak zdefiniowanych ryzyk określano prawdopodobieństwo ich wystąpienia oraz skutek ich zmaterializowania oraz proponowano sposób postępowania w celu ich zmniejszenia lub ograniczenia. Dokument taki był przekazywany Sekretarzowi i podlegał akceptacji przez Prezydenta.

(akta kontroli: str. 40-44 plik 9)

1.5. W Urzędzie nie opracowano osobnej polityki ciągłości działania, ale jej elementy były częścią obowiązującej PBI, której jednym ze zdefiniowanych zadań było „*zapewnienie ciągłości działania*". Dodatkowo założenia, zakres oraz podstawowe zasady zarządzania ciągłością działania zostały określone w Polityce zarządzania infrastrukturą techniczną, będącej załącznikiem do PBI. Według tego dokumentu zarządzanie ciągłością działania opierało się na analizie zagrożeń i podatności, a w konsekwencji ocenie ryzyk z nimi związanych. Analiza miała określać najważniejsze zagrożenia dla ciągłości procesów Urzędu, kluczowe zasoby oraz zabezpieczenia. Polityka ta wskazywała także na potrzebę opracowania zasad tworzenia, testowania i wykonywania planów awaryjnych, które powinny określać warunki uruchomienia (początkowe) oraz osoby odpowiedzialne za opracowanie i aktualność tych planów. Dokumenty te zostały, podobnie jak cała PBI wraz z załącznikami, właściwie zatwierdzone i przedstawione pracownikom.

(akta kontroli: str. 40-44 plik 3-4, 6-9)

1.6. Działania zapewniające przywrócenie zdolności realizacji działań Urzędu w przypadku awarii systemu informatycznego zostały określone w Planie ciągłości działania, wprowadzonym Zarządzeniem Prezydenta Miasta Głogowa z 16 listopada 2021 r.[15]. W tym dokumencie dla każdego z 23 zidentyfikowanych krytycznych zasobów (serwerów lub systemów) określono: osoby odpowiedzialne za przywrócenie zasobu, czas przewidziany na przywrócenie zasobu (24 godziny dla wszystkich zasobów), system operacyjny serwera lub uruchomione usługi dla

[14] Dalej: PODO.

[15] W sprawie wprowadzenia do stosowania planów ciągłości działania. Zmieniony Zarządzeniem Nr 25/2022 Prezydenta Miasta Głogowa z dnia 14 lipca 2022 r. w sprawie zmian do Zarządzenia Prezydenta Miasta Głogowa nr 32/2022 z dnia 16 grudnia 2021 r. w sprawie wprowadzenia do stosowania planu ciągłości działania. Dalej: Plan ciągłości działania.

systemów, sprzęt zastępczy, narzędzia wymagane do wykonania procedury, lokalizację podstawową oraz lokalizację awaryjną, miejsce przechowywania narzędzi, listę serwerów wirtualnych obsługiwanych przez serwer, dane konfiguracyjne zasobu oraz czynności do wykonania. Plan ten zawierał także zestawienie niezbędnych narzędzi do przywracania zasobów, a także zobowiązywał do jego przeglądu co najmniej raz na 24 miesiące i w razie potrzeby aktualizowania.

(akta kontroli: str. 40-44 plik 6-7)

1.7. Obowiązujący w Urzędzie Plan ciągłości działania nakładał obowiązek przeprowadzania jego testowania przynajmniej raz na 24 miesiące, mający na celu sprawdzenie jego aktualności. Z czynności takiej należało złożyć raport Sekretarzowi. W okresie objętym kontrolą, w dniach od 2 do 24 października 2023 r., przeprowadzono i udokumentowano testy planu ciągłości działania oraz sprawdzenie jego aktualności, a raport z tych działań przedłożono Sekretarzowi.

(akta kontroli: str. 40-44 plik 6-7, 67)

1.8. Zgodnie z § 19 ust. 2 pkt 1 rozporządzenia KRI, w Urzędzie dokonywano przeglądu i aktualizacji dokumentacji składającej się na SZBI.

Przeglądy takie realizowano w ramach oceny skuteczności stosowanych środków ochrony danych, które przeprowadzał IOD wraz z pracownikami Działu Informatyki Urzędu. Ostatni taki przegląd udokumentowano 23 października 2023 r., nie wykazał on potrzeby zmiany uregulowań wewnętrznych, a sporządzona ocena została przekazana Sekretarzowi oraz zaakceptowana przez Prezydenta.

(akta kontroli: str. 40-44 plik 4, 8)

1.9. Osobą odpowiedzialną za bezpieczeństwo informacji oraz zapewnienie ciągłości działania był IOD. Zadania te zostały mu przypisane w zakresie czynności, a do jego obowiązków należało m.in.: podejmowanie przedsięwzięć zmierzających do podniesienia poziomu bezpieczeństwa informacji; sprawowanie nadzoru i kontroli nad zabezpieczeniami fizycznymi we wszystkich lokalizacjach; nadzór nad przeprowadzaniem analizy ryzyka systemów obejmującej: identyfikację istniejących zagrożeń, kwalifikację tych zagrożeń oraz skutków dla ciągłości działania i prawdopodobieństwa ich urzeczywistnienia; określenie odpowiednich działań mających na celu zmniejszenie zidentyfikowanego ryzyka do akceptowalnego poziomu; wdrożenie działań mających na celu zmniejszenie zagrożeń; dokonywanie zmian w postępowaniu z ryzykiem w świetle wydarzeń i zmian w otoczeniu zgodnie z rozporządzeniem KRI; sprawdzanie zgodności systemów z PBI; wykonywanie zadań wymienionych w PBI; sprawowanie nadzoru nad wykorzystywanym w Urzędzie oprogramowaniem pod kątem jego legalności; kontrola nad ciągłością działania systemów informatycznych; nadzór nad konfiguracją infrastruktury sieciowej; nadzór nad nadawaniem, zmianą lub odbieraniem uprawnień m.in. do kont użytkowników sieciowych, dostępu do poczty elektronicznej, zasobów sieciowych oraz lokalnego systemu operacyjnego a także do BIP oraz prowadzenie rejestru osób posiadających w/w konta; nadzór nad stosowaniem zabezpieczeń kryptograficznych adekwatnie do wyników analizy ryzyka; bieżący monitoring incydentów bezpieczeństwa poprzez przeglądanie rejestru zdarzeń systemowych oraz sporządzanie raportów incydentów bezpieczeństwa i przekazywanie Sekretarzowi; nadzór nad aktualizowaniem oprogramowania antywirusowego oraz systemów operacyjnych; nadzór nad wykonywaniem kopii zapasowych ich przechowywanie oraz okresowe sprawdzenie pod kątem ich dalszej przydatności; nadzór nad prowadzeniem inwentaryzacji sprzętu komputerowego i oprogramowania używanego w Urzędzie; nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych zawierających dane osobowe; przeprowadzanie szkoleń z bezpieczeństwa informacji i ochrony danych osobowych;

utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz zgłaszanie incydentów w ciągu 24 godzin od momentu wykrycia incydentu do CSIRT NASK[16].

Pracownik pełniący obowiązki IOD posiadał odpowiednie kompetencje w zakresie powierzonych obowiązków, potwierdzone posiadanym wykształceniem, doświadczeniem oraz przebytymi szkoleniami.

(akta kontroli: str. 26, 40-44 plik 2-3, 6)

1.10. Zgodnie z art. 37 ust. 1 i 5 RODO oraz art. 8 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[17], Prezydent wyznaczył jedną osobę, będącą pracownikiem Urzędu, do pełnienia funkcji IOD. Osoba ta posiadała odpowiednie kwalifikacje do pełnienia tej funkcji, potwierdzone świadectwem ukończenia studiów podyplomowych w zakresie „Inspektor ochrony danych osobowych", doświadczeniem oraz przebytymi szkoleniami. Zakres obowiązków IOD, oprócz wymienionych w pkt 1.9 wystąpienia pokontrolnego, obejmował także zadania związane z ochroną i zabezpieczeniem danych osobowych, w tym m.in. zapewnianie przestrzegania przepisów o ochronie danych osobowych, wykonywanie zadań wymienionych w art. 39 RODO, prowadzenie rejestru czynności przetwarzania danych osobowych zgodnie z art. 30 RODO, informowanie Prezydenta o przypadkach naruszenia przepisów o ochronie danych osobowych oraz wykonywanie zadań wymienionych w PODO.

(akta kontroli: str. 26, 40-44 plik 2, 5)

1.11. IOD ze względu na zakres swoich obowiązków powiązanych także z bezpieczeństwem informacji i zapewnieniem ciągłości działania podlegał Sekretarzowi z zastrzeżeniem, że nadzór merytoryczny nad realizacją zadań z zakresu ochrony danych osobowych sprawuje Prezydent. Spełniało to wymogi art. 38 ust. 3 RODO[18].

Realizacja przez osobę będącą IOD innych zadań, związanych z bezpieczeństwem informacji oraz zapewnieniem ciągłości działania, ze względu na brak kompetencji w zakresie decydowania o sposobach i celach przetwarzania danych osobowych w organizacji, nie powodowała także konfliktu interesów, o którym mowa w art. 38 ust. 6 RODO.

(akta kontroli: str. 40-44 plik 2)

1.12. Zgodnie z art. 21 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[19], 21 kwietnia 2020 r. wyznaczono IOD jako osobę odpowiedzialną za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Dane ww. osoby zostały przekazane do CSIRT-NASK 21 kwietnia 2020 r., tj. w terminie zgodnym z art. 22 ust. 1 pkt 5 ustawy o ksc[20].

Nie skorzystano natomiast z uprawnienia określonego w art. 21 ust. 2 i 3 ustawy o ksc, tj. nie wyznaczono jednej osoby odpowiedzialnej za utrzymywanie ww. kontaktów w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jednostki organizacyjne Urzędu oraz jednostki podległe i nadzorowane przez Prezydenta. Wynikało to z dużej ilości tych jednostek, które te zadania realizowały we

[16] Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy z siedzibą w Warszawie.
[17] Dz. U. z 2019 r. poz. 1781.
[18] Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.
[19] Dz. U. z 2024 r. poz. 1077, ze zm., dalej: ustawa o ksc.
[20] Tj. w terminie 14 dni od dnia wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.

własnym zakresie, a wyznaczenie dodatkowej osoby do tych celów nie przyniosłoby znaczących korzyści w kontekście istniejących rozwiązań.

(akta kontroli: str. 34, 40-44 plik 2, 11)

1.13. Wszystkie regulacje wewnętrzne stanowiące szczegółowe dokumenty wykonawcze wymagane przez PBI zostały sporządzone, zatwierdzone i opublikowane wraz z tym dokumentem, były to procedury wymienione w punkcie 1.2. niniejszego wystąpienia pokontrolnego.

(akta kontroli: str. 40-44 plik 3-4)

1.14. Urząd posiadał informacje o zasobach informatycznych obejmującą ich rodzaj i konfigurację, co spełniało wymogi wynikające z § 19 ust. 2 pkt 2 rozporządzenia KRI.

Do utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmujących ich rodzaj i konfigurację wykorzystywano arkusze MS Excel obejmujące ewidencję komputerów, serwerów i urządzeń peryferyjnych (skanerów, drukarek i monitorów). Ewidencja ta była prowadzona ręcznie i wymagała aktualizacji w momencie dokonania jakichkolwiek zmian. Obejmowała wszystkie użytkowane 257 komputerów, 216 urządzeń peryferyjnych (monitory, drukarki i skanery) oraz 11 serwerów fizycznych i 27 wirtualnych.

W przypadku komputerów ewidencja obejmowała nazwę i rodzaj komputera, jego użytkownika, numer inwentarzowy, podstawowe parametry, sieć, w której działa, wybrane zainstalowane oprogramowanie, szyfrowanie oraz datę dokonania aktualizacji ewidencji. W przypadku ewidencji urządzeń peryferyjnych, oprócz ich nazwy dostępny był ich numer inwentarzowy oraz użytkownik. Natomiast w przypadku serwerów, ewidencjonowano jego nazwę, rodzaj i opis oraz adres IP[21]. Ponadto do inwentaryzacji sporadycznie, tylko w celu weryfikacji i sprawdzenia zasobu, bez utrzymywania aktualnych danych, wykorzystywano oprogramowanie Open Source GLPI i modułu OCS Inventory.

(akta kontroli: str. 24, 29, 31-32)

1.15. W okresie objętym kontrolą Urząd przystąpił do rządowego programu „Cyberbezpieczny Samorząd", realizując projekt „Rozwój cyberbezpieczeństwa w Gminie Miejskiej Głogów". Umowa o wartości 799 994,96 zł[22] na realizację grantu została zawarta 9 lipca 2024 r., a czas jej realizacji został określony do 30 czerwca 2026 r.

Celem i efektami tego projektu mają być wsparcie transformacji cyfrowej oraz zwiększenie poziomu bezpieczeństwa informacji w Gminie Miejskiej Głogów[23], poprzez:

- wdrożenie w Gminie środków zarządzania ryzykiem w cyberbezpieczeństwie oraz mechanizmów i środków zwiększających odporność na ataki z cyberprzestrzeni (zwiększenie poziomu bezpieczeństwa informacji) poprzez wdrożenie serwera poczty z modułem antywirusowym i antyspamowym oraz mechanizmu uwierzytelniania wielopoziomowego (na potrzeby Urzędu);
- przeprowadzenia audytu SZBI dla 30 jednostek potwierdzającego uzyskanie wyższego poziomu odporności na cyberzagrożenia, wykonanego przez wykwalifikowanych audytorów oraz wypełnienie ankiety dojrzałości cyberbezpieczeństwa;
- rozwinięcie cyfryzacji poprzez zakup i wdrożenie odpowiednich narzędzi, tj. agregatu prądotwórczego (minimum 300kW) dla Urzędu, urządzeń

[21] Adres IP (Internet Protocol Address), to unikalny numer przypisany każdemu urządzeniu, które jest podłączone do sieci komputerowej, wykorzystującej protokół komunikacyjny Internet Protocol.
[22] W tym 711 995,63 zł dofinansowanie w ramach grantu oraz 87 999,33 zł wkład własny Gminy Miejskiej Głogów.
[23] Dalej Gmina.

wielofunkcyjnych UTM[24], macierzy dyskowych oraz dysków USB o dużej pojemności do kopii zapasowych (dla Urzędu i wybranych jednostek Gminy);
- zwiększenie kompetencji pracowników 30 jednostek Gminy poprzez szkolenia z zakresu cyberbezpieczeństwa dla informatyków oraz pracowników tych jednostek przetwarzających informacje.

W ramach oceny realizacji tego projektu przewidziano ewaluację według kryteriów „Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego".

(akta kontroli: str. 40-44 plik 12-13, 53-66)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

OCENA CZĄSTKOWA

NIK pozytywnie ocenia kontrolowaną działalność Urzędu w zakresie organizacji bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych.

2. Wdrożone i wykorzystywane rozwiązania organizacyjne i techniczne zapewniające bezpieczeństwo informacji oraz ciągłość działania

Opis stanu faktycznego

2.1. Przyjęte w Urzędzie rozwiązanie, polegające na nieprzyznawaniu użytkownikom uprawnień administracyjnych do systemu operacyjnego, zapobiegało możliwości instalowania nieautoryzowanego oprogramowania przez pracowników Urzędu na komputerach służbowych. Próba dokonania zainstalowania nieautoryzowanego oprogramowania[25] przeprowadzona na dziesięciu komputerach (sześciu stacjonarnych oraz czterech laptopach[26]) Urzędu nie powiodła się, co było zgodne z wymaganiami wynikającymi z § 19 ust. 2 pkt 4 rozporządzenia KRI.

Według wyjaśnień Prezydenta zabraniano kopiowania i przechowywania danych stanowiących własność Urzędu na służbowych smartfonach i tabletach.

(akta kontroli: str. 32, 45)

2.2. Obowiązek dotyczący podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w sposób adekwatny do wykonywanych przez nie zadań, był realizowany prawidłowo.

Nadanie uprawnień do dostępu do systemów IT oraz ich zmiana/odebranie w Urzędzie następowało na podstawie sformalizowanego wniosku o nadanie/cofnięcie/zmianę uprawnień, wynikającego z obowiązującej procedury kontroli dostępu do informacji (załącznik do PBI). Wniosek ten był sporządzany przez właściwego kierownika i był procedowany elektronicznie w systemie IntraDok w momencie rozpoczęcia pracy lub jej zakończenia przez pracownika oraz podlegał zatwierdzeniu przez Prezydenta. Wniosek ten zawierał wykaz systemów, do których pracownik na jego podstawie uzyskiwał/tracił dostęp wraz ze wskazaniem przypisanej mu roli. Przedmiotowe wnioski przechowywane były w systemie IntraDok, a dostęp do nich mieli administratorzy systemów.

W wyniku przeprowadzonego badania adekwatności uprawnień w systemach informatycznych 15 pracowników Urzędu[27], nie stwierdzono by posiadane przez nich

[24] UTM – wielofunkcyjne zapory sieciowe zintegrowane w postaci jednego urządzenia.
[25] W dniu 4 lipca 2024 r.
[26] Według oświadczenia Kierownika Działu Informatyki Urzędu sprawdzeniu podlegały wszystkie pracujące w momencie prowadzenia oględzin laptopy.
[27] Według stanu na 20 czerwca 2024 r. próba ta stanowiła 7,5 % wszystkich osób zatrudnionych w Urzędzie i użytkujących systemy IT.

uprawnienia wykraczały poza zakres ich obowiązków wynikający z zakresów czynności, co było zgodne z § 19 ust. 2 pkt 4 rozporządzenia KRI.

(akta kontroli: str. 15-23, 40-44 plik 3-4)

2.3. Badanie przeprowadzone na próbie 15 pracowników, którzy zakończyli zatrudnienie po 1 stycznia 2023 r.[28], wykazało, że nie posiadali oni kont użytkowników lub ich konta były zablokowane/nieaktywne, a stosowne wnioski zostały sporządzone niezwłocznie po ustaniu zatrudnienia, co było zgodne z § 19 ust. 2 pkt 5 rozporządzenia KRI.

(akta kontroli: str. 15-23, 40-44 plik 3-4)

2.4. Obowiązujące w Urzędzie zasady nadawania haseł, zawarte w Procedurze kontroli dostępu do informacji (załącznik do PBI), wprowadzały dla nich wymagania określające minimalną liczbę znaków oraz ich złożoność.

Oględziny trzech systemów informatycznych zarządzanych przez Urząd wykazały, że systemy te wymuszały stosowanie haseł zgodnych z cytowaną wyżej procedurą, co było zgodne z § 19 ust. 2 pkt 7 lit. c rozporządzenia KRI.

Stosowane w badanych systemach loginy nie były uniwersalne[29] i nie wskazywały na wykorzystanie ich przez kilku użytkowników.

(akta kontroli: str. 24-25, 40-44 plik 3-4)

2.5. Sprawdzenie usytuowania monitorów ośmiu stanowisk przeprowadzone w salach obsługi klientów w Biurze Obsługi Mieszkańca[30] oraz Dziale Ewidencji Ludności i Dowodów Osobistych[31], wykazało, że we wszystkich przypadkach usytuowanie monitorów uniemożliwiało wgląd do danych przez osoby nieupoważnione. Stan ten był zgodny z wymaganiami wynikającymi z § 19 ust. 2 pkt 7 rozporządzenia KRI.

(akta kontroli: str. 45)

2.6. W Urzędzie opracowano zasady korzystania ze służbowych komputerów przenośnych poza miejscem pracy, które stanowiły załącznik do PBI, co było zgodne z § 19 ust. 2 pkt 8 rozporządzenia KRI.

Korzystanie ze służbowych komputerów przenośnych poza miejscem pracy wymagało uzyskania zgody Prezydenta oraz podpisania umowy, w której pracownik zobowiązywał się do przestrzegania zaleceń związanych z ochroną urządzenia. Zdalny dostęp do systemów informatycznych realizowany był przez sieć VPN tylko i wyłącznie po poprawnej identyfikacji oraz uwierzytelnieniu zdalnego użytkownika. Dostęp do sieci VPN ograniczony został tylko do tych pracowników, którym dostęp ten jest niezbędny do realizacji powierzonych zadań.

(akta kontroli: str. 40-44 plik 3-4)

2.7. Komputery przenośne były zabezpieczone przed dostępem osób nieuprawnionych poprzez oprogramowanie szyfrujące dyski twarde oraz indywidualny login i hasło przypisane do użytkownika, czego wymagała Procedura kontroli dostępu do informacji. Spełniało to wymogi § 19 ust. 2 pkt 9 i 11 rozporządzenia KRI.

(akta kontroli: str. 34, 40-44 plik 3-4)

2.8. Zabezpieczenia fizyczne zastosowane w serwerowni w celu zabezpieczenia informacji uniemożliwiały nieuprawnione jej ujawnienie, modyfikacje lub usunięcie, co było zgodne z § 19 ust. 2 pkt 9 rozporządzenia KRI.

---

[28] Według stanu na 20 czerwca 2024 r. próba ta stanowiła 78,9% wszystkich osób kończących zatrudnienie.
[29] Konstrukcja loginów pozwalała na prostą identyfikację użytkowników.
[30] Cztery stanowiska z oprogramowaniem własnym Urzędu przeznaczonym do obsługi mieszkańców.
[31] Cztery stanowiska z zainstalowaną aplikacją Źródło.

Serwerownia Urzędu była bowiem zlokalizowana w odrębnym, nieoznaczonym, klimatyzowanym pomieszczeniu, do którego dostęp mieli informatycy. Posiadała ona dedykowaną instalację elektryczną oraz systemy zabezpieczeń dostępu. Ponadto w czasie przeprowadzania oględzin była zamknięta i nie przechowywano w niej materiałów zagrażających infrastrukturze IT.

(akta kontroli: str. 9-10)

2.9. W okresie objętym kontrolą obowiązywały 23 umowy zawarte przez Urząd na zakup lub serwis sprzętu informatycznego, oprogramowania i świadczenia usług IT. Szczegółowe badanie czterech z nich wykazało, że we wszystkich przypadkach zawarto zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji, co było zgodne z § 19 ust. 2 pkt 10 rozporządzenia KRI.

(akta kontroli: str. 7, 40-44 plik 22-28)

2.10. W Urzędzie opracowano i wdrożono Procedurę zarządzania infrastrukturą informatyczną oraz Procedurę współpracy z osobami trzecimi[32], według których urządzenia lub elektroniczne nośniki informacji, przeznaczone do napraw w firmach zewnętrznych lub zbycia, pozbawia się w trwały sposób, przed ich naprawą i zbyciem, informacji na nich zawartych albo naprawia się je pod nadzorem pracownika Urzędu.

(akta kontroli: str. 40-44 plik 3-4)

2.11. Zasady stanowiące politykę kopii zapasowych zostały opisane w Procedurze wykonania kopii zapasowej (załącznik do PBI). Określały one sposób archiwizacji danych (tworzenia kopii zapasowych), miejsce i okres ich przechowywania oraz osoby mające do nich dostęp. Ponadto określono sposób postępowania z nośnikami wyłączonymi z użytkowania i zasady testowania kopii bezpieczeństwa.

(akta kontroli: str. 40-44 plik 3-4)

2.12. W toku oględzin[33] ustalono, że kopie zapasowe danych tworzone były zgodnie z zasadami, określonymi w Procedurze wykonania kopii zapasowych, tj. codziennie w sposób automatyczny, na serwery archiwizacyjne (zasoby dyskowe), z czego jeden znajdował się w pomieszczeniu głównej serwerowni Urzędu, a drugi w serwerowni poza głównym budynkiem Urzędu. W procesie tworzenia kopii zapasowych (jako zabezpieczenie przed atakiem na urządzenia sieciowe) wykorzystywane były także dyski zewnętrzne USB. Kopie zapasowe na nich tworzono codziennie, a obrazy serwerów nie rzadziej niż raz na dwa miesiące.

Proces tworzenia kopii zapasowych był nadzorowany przez IOD, który na bieżąco monitorował fakt wykonania kopii zapasowej i ilość wymaganych kopii dla każdego serwera. Dodatkowo zgodnie z procedurą wynikającą z PBI, IOD raz na pół roku sprawdzał kopie zapasowe i określał ich przydatność do wykorzystania w wypadku awarii systemów, dokonując odtworzenia kopii. Z czynności tych sporządzał notatkę przedkładaną Sekretarzowi, w okresie objętym kontrola sprawdzenia te miały miejsce w czerwcu i grudniu 2023 r.

Przeprowadzony w trakcie oględzin test na odzyskiwanie danych z wybranej kopii zapasowej[34] zakończył się poprawnym przywróceniem danych.

Zabezpieczenie serwerów archiwizacyjnych i dysków zewnętrznych USB spełniało wymogi wynikające z § 19 ust. 2 pkt 7 oraz § 19 ust. 2 pkt 12 lit. b i e rozporządzenia KRI.

(akta kontroli: str. 13-14, 40-44 plik 3-4, 14, 68-71)

[32] Obie procedury stanowią załącznik do PBI.
[33] Z 19 czerwca 2024 r.
[34] Baza danych systemu z 6 kwietnia 2024 r.

2.13. W Urzędzie nie przyjęto formalnej procedury monitorowania pojemności nośników pamięci masowych, wykorzystywanych w serwerach. Monitoring taki był prowadzony ręcznie przez informatyków. Przeprowadzony w trakcie oględzin[35] test zajętości dysków twardych na trzech serwerach wykazał, że ich zajętość wynosiła odpowiednio 74%, 93% i 32%.

NIK wskazuje, że zajętość przestrzeni dyskowej powinna być stale monitorowana w celu dostosowywania wykorzystania zasobów oraz przewidywania wymaganej pojemności w przyszłości oraz nie powinna przekraczać 80% dla zapewnienia właściwej wydajności systemu i aplikacji.

(akta kontroli: str. 25)

2.14. W ramach zapewnienia ciągłości działania Urzędu zidentyfikowano kluczowe elementy infrastruktury IT oraz kluczowe usługi IT, wykorzystywane w jednostce. Informacje te zostały wykorzystane do testowania od 2 do 24 października 2023 r. planu ciągłości działania oraz sprawdzenia jego aktualności. Czas przywrócenia poszczególnych systemów oraz procesów do działania wyznaczono do 24 godzin.

(akta kontroli: str. 40-44 plik 6-9, 67)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

OCENA CZĄSTKOWA

NIK pozytywnie ocenia kontrolowaną działalność Urzędu w zakresie wdrożonych i wykorzystywanych rozwiązań organizacyjnych i technicznych, zapewniających bezpieczeństwo informacji oraz ciągłość działania.

OBSZAR

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

3.1. Zgodnie z przyjętą Procedurą zarządzania ryzykiem w bezpieczeństwie informacji, w 2023 r. przeprowadzono w Urzędzie coroczną analizę ryzyka utraty integralności, poufności lub dostępności informacji, zatwierdzoną przez Prezydenta 25 października 2023 r. Na ww. analizę składały się: [1] inwentaryzacja zasobów informatycznych [2] właściwa analiza ryzyka, w której wskazano: krytyczne zasoby informatyczne, zidentyfikowane ryzyka z nimi związane, ocenę prawdopodobieństwa i skutku danego ryzyka oraz skalę tego ryzyka, ewaluację ryzyka oraz plan postępowania z danym ryzykiem.

W jej wyniku stwierdzono, że wszystkie zagrożenia jakie występowały były na poziomie akceptowalnym. Zwrócono przy tym uwagę na konieczność przestrzegania sposobu postępowania z ryzykiem, np. aktualizowania oprogramowania systemowego, narzędziowego, wykonywania codziennych kopii awaryjnych, wykonywania zalecanego skanowania antywirusowego oraz wykonywania kontroli przestrzegania PBI, które warunkują pozostawanie zagrożeń na poziomie akceptowalnym.

(akta kontroli: str. 40-44 plik 9)

3.2. Zgodnie z § 19 ust. 2 pkt 13 rozporządzenia KRI, ustalono w Urzędzie sposób bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji, określony w Procedurze postępowania z incydentami (załącznik do PBI). W dokumencie tym wskazano sytuacje stanowiące naruszenie bezpieczeństwa informacji oraz zasady postępowania w przypadku ich stwierdzenia lub podejrzenia ich zaistnienia.

[35] 25 czerwca 2024 r.

W okresie objętym kontrolą w Urzędzie wystąpiło pięć incydentów w zakresie dotyczącym bezpieczeństwa informacji[36], a dwa z tych incydentów zostały zgłoszone do CSIRT NASK[37]. We wszystkich przypadkach podjęto stosowne działania i zrealizowano postępowania naprawcze.

(akta kontroli: str. 40-44 plik 3-4, 32-52)

3.3. W Urzędzie przeprowadzano szkolenia pracowników z zakresu bezpieczeństwa informacji, wynikające § 19 ust. 2 pkt 6 rozporządzenia KRI.

W okresie objętym kontrolą szkolenie przeprowadzono w grudniu 2023 r. za pomocą przygotowanej przez IOD prezentacji video, udostępnionej w sieci wewnętrznej Urzędu, po którym nastąpiło sprawdzenie wiedzy w formie testów. Wypełniony test przekazało 94,5% pracowników Urzędu[38]. Tematyka przedmiotowego szkolenia obejmowała omówienie rodzajów i charakterystyk zagrożeń spotykanych w sieci, omówienie skutków takich ataków na przykładzie podmiotów publicznych oraz sposobów obrony przed prezentowanymi atakami.

(akta kontroli: str. 40-44 plik 15-18, 25-29)

3.4. W okresie od 24 października 2023 r. do 11 grudnia 2023 r. audytorzy wewnętrzni Urzędu przeprowadzili audyt „Funkcjonowanie systemu zarządzania bezpieczeństwem informacji". W jego wyniku wydali ocenę, że proces opracowania i wdrożenia systemu zarządzania bezpieczeństwem informacji w Urzędzie przebiegał prawidłowo, a system kontroli zarządczej w audytowanym obszarze funkcjonował w należytym zakresie. Spełniało to obowiązek wynikający z § 19 ust. 2 pkt 14 rozporządzenia KRI.

(akta kontroli: str. 40-44 plik 21)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

OCENA CZĄSTKOWA

NIK pozytywnie ocenia kontrolowaną działalność Urzędu w zakresie zapobiegania incydentom bezpieczeństwa informacji.

IV. Uwagi i wnioski

W związku z niestwierdzeniem nieprawidłowości, Najwyższa Izba Kontroli nie formułuje uwag ani wniosków.

[36] Jeden w zakresie danych osobowych (uszkodzenie przesyłki pocztowej), a cztery w zakresie bezpieczeństwa informacji (brak wycofania uprawnień dla osób kończących zatrudnienie; fałszywy mail – dwa zgłoszenia; udostępnienie komputera służbowego osobom nieuprawnionym).

[37] Fałszywy mail podszywający się pod MSWiA oraz mail podszywający się pod GUS.

[38] 171 pracowników przekazało test ze 181 ogółem.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Delegatury NIK we Wrocławiu. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Wrocław, 16 września 2024 r.

Najwyższa Izba Kontroli
Delegatura we Wrocławiu
Kontroler
Cezary Mazik
Główny specjalista kontroli państwowej

Dyrektor
z up. p.o. Wicedyrektor
Artur Urban

.....
podpis

.....
podpis