NAJWYŻSZA IZBA KONTROLI

DEPARTAMENT ADMINISTRACJI PUBLICZNEJ

KAP.410.3.3.2024

Pan
Jarosław Tomasz Margielski
Prezydent Miasta Otwocka

Urząd Miasta Otwocka
ul. Armii Krajowej 5
05-400 Otwock

WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
Departament Administracji Publicznej
ul. Filtrowa 57, 02-056 Warszawa
tel. 48224445308, kap@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miasta Otwocka[1], ul. Armii Krajowej 5, 05-400 Otwock.
Kierownik jednostki kontrolowanej	Jarosław Tomasz Margielski, Prezydent Miasta Otwocka, od 17 listopada 2018 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 czynności kontrolnych, tj. do 26 lipca 2024 r. (także okresy wcześniejsze w zakresie uczestnictwa w programie Cyfrowa Gmina).
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[2]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Departament Administracji Publicznej
Kontrolerzy	1. Tomasz Płudowski, główny specjalista kontroli państwowej, upoważnienie do kontroli nr KAP/42/2024 z 21 maja 2024 r. 2. Mariusz Stolarz, doradca techniczny, upoważnienie do kontroli nr KAP/50/2024 z 18 czerwca 2024 r. (akta kontroli str.1-4)

[1] Dalej: Urząd lub Miasto.
[2] Dz. U. z 2022 r. poz. 623, dalej: ustawa o NIK.

II. Ocena ogólna[3] kontrolowanej działalności

OCENA OGÓLNA

W Urzędzie, w okresie objętym kontrolą, nie wprowadzono procedur służących zapewnieniu ciągłości działania systemów informatycznych za wyjątkiem procedury dotyczącej kopii zapasowych[4]. Działania prowadzone w zakresie zapewnienia bezpieczeństwa informacji były ograniczone.

NIK ocenia negatywnie działalność kontrolowanej jednostki w obszarze organizacji bezpieczeństwa informacji oraz zapewnienia ciągłości działania systemów informatycznych, przede wszystkim ze względu na to, że w Urzędzie nie ustanowiono i nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji[5] (w szczególności Polityki Bezpieczeństwa Informacji), co było niezgodne z § 19 ust. 1 w zw. z ust. 3 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[6] (dalej: rozporządzenie KRI). Ponadto nie ustanowiono i nie wdrożono polityk w ramach zapewnienia ciągłości działania systemów informatycznych, co było nierzetelne.

W Urzędzie natomiast prawidłowo realizowano zadania dotyczące opracowania spełniającej wymogi 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[7] (dalej: RODO) dokumentacji z zakresu ochrony danych osobowych oraz gromadzenia aktualnych informacji o zasobach informatycznych obejmujących ich rodzaj i konfigurację.

Ponadto w Urzędzie, w okresie objętym kontrolą, podejmowano działania zapewniające bezpieczeństwo przetwarzania informacji m.in. poprzez prawidłowe przechowywanie i testowanie kopii zapasowych, nadawanie uprawnień pracownikom adekwatnie do realizowanych przez nich zadań oraz stosowanie w umowach serwisowych postanowień gwarantujących odpowiedni poziom bezpieczeństwa informacji. Wprowadzono również procedury dotyczące przekazywania sprzętu komputerowego podmiotom zewnętrznym oraz zasady pracy zdalnej. W toku kontroli stwierdzono jednak nieprawidłowości w zakresie zapewnienia bezpieczeństwa informacji w Urzędzie, które dotyczyły m.in. możliwości instalowania przez pracownika do tego nieuprawnionego nieautoryzowanego oprogramowania, niespełniania przyjętych wymagań dla haseł dostępu oraz braku blokowania kont byłych pracowników w systemach informatycznych wykorzystywanych przez Urząd, co było niezgodne odpowiednio z § 19 ust. 2 pkt 4, 7 i 5 rozporządzenia KRI.

W okresie objętym kontrolą w Urzędzie podjęto działania w celu zapobiegania incydentom bezpieczeństwa informacji, tj. stosownie do § 19 ust. 2 pkt 6 rozporządzenia KRI zorganizowano szkolenia pracowników oraz w myśl § 19 ust. 2 pkt 14 rozporządzenia KRI przeprowadzono audyt z tego zakresu. Nie prowadzono natomiast okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji, o których mowa w § 19 ust. 2 pkt 3 rozporządzenia KRI, a wprowadzona w Urzędzie procedura w zakresie zgłaszania incydentów naruszenia bezpieczeństwa

---

3 Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

4 Wprowadzonej w ramach Instrukcji zarządzania zasobami informatycznymi.

5 Dalej: SZBI.

6 Dz. U. poz. 773. Wcześniej, w okresie objętym kontrolą obowiązywało rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247) – dalej: rozporządzenie KRI z 12 kwietnia 2012 r.

7 Dz. Urz. UE. L 119 z 04.05.2016 r. str. 1, ze zm.

informacji odnosiła się wyłącznie do danych osobowych, co było niezgodne z § 19 ust. 2 pkt 13 rozporządzenia KRI.

NIK zauważa, że w trakcie kontroli część stwierdzonych nieprawidłowości została usunięta w wyniku podjętych w Urzędzie działań.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[8] kontrolowanej działalności

OBSZAR

1. Organizacja bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych

Opis stanu faktycznego

1.1. W Urzędzie poza danymi osobowymi ujętymi w Rejestrze czynności przetwarzania nie zidentyfikowano innych zbiorów danych podlegających zabezpieczeniu (dalszy opis w części *Stwierdzone nieprawidłowości*).

(akta kontroli str. 53-76, 324-331)

1.2. W Urzędzie nie ustanowiono i nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji, o którym mowa w § 19 ust. 1 w zw. z ust. 3 rozporządzenia KRI[9] (dalszy opis w części *Stwierdzone nieprawidłowości*).

(akta kontroli str. 53-76, 503-537)

1.3. W okresie objętym kontrolą w Urzędzie obowiązywały, uwzględniające wymogi RODO, dokumenty dotyczące bezpieczeństwa przetwarzania danych osobowych, które zostały wprowadzone zarządzeniem nr 13/2022 Prezydenta Miasta Otwocka z dnia 19 stycznia 2022 r. w sprawie Polityki Ochrony Danych Osobowych w Urzędzie Miasta Otwocka, tj.:

- Polityka ochrony danych osobowych w Urzędzie Miasta Otwocka,
- Instrukcja zarządzania zasobami informatycznymi.

Prezydent poinformował, że pracownicy Urzędu byli zapoznawani z powyższymi dokumentami w trakcie szkoleń z ochrony danych osobowych i zobowiązywali się do ich stosowania podpisując stosowne oświadczenia.

(akta kontroli str. 192-486, 538-554, 557)

1.4. W Urzędzie nie prowadzono analiz ryzyka w związku z potrzebą zachowania ciągłości działania systemów informatycznych (dalszy opis w części *Stwierdzone nieprawidłowości*).

(akta kontroli str. 53-76, 97-102, 588-602)

1.5. W Urzędzie nie ustanowiono polityk ciągłości działania i nie opracowano planów zapewnienia ciągłości działania oraz planów odtworzeniowych (dalszy opis w części *Stwierdzone nieprawidłowości*)

(akta kontroli str. 53-76, 558-561)

1.6. Osobą odpowiedzialną za zapewnienie ciągłości działania w Urzędzie oraz bezpieczeństwo informacji jest Naczelnik Wydziału Informatyki[10]. Odpowiedzialność ta została określona w zakresie obowiązków pracownika Urzędu, który w okresie objętym kontrolą pełnił obowiązki Naczelnika Wydziału Informatyki. Jak ustalono pracownik ten posiadał odpowiednie kwalifikacje w ww. zakresie.

---

[8] 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.

[9] W trakcie kontroli przedłożono jedynie projekt dokumentacji SZBI.

[10] Wydział Informatyki zgodnie z Regulaminem organizacyjnym Urzędu Miasta Otwocka był bezpośrednio nadzorowany przez Prezydenta.

Jako osobę odpowiedzialną za bezpieczeństwo informacji w Urzędzie Prezydent wskazał również Inspektora Ochrony Danych[11]. Dodatkowo poinformował, że *formalne powołanie pełnomocnika ds. bezpieczeństwa informacji planowane jest przy wdrożeniu SZBI*.

(akta kontroli str. 5-76, 103-112, 588-597)

1.7. W Urzędzie, na podstawie zawartych umów cywilnoprawnych, wyznaczony został Inspektor Ochrony Danych[12]. W umowach tych wśród obowiązków IOD wskazywano m.in. nadzorowanie przestrzegania obowiązków zabezpieczenia danych osobowych, współpracę z organem nadzorczym, prowadzenie szkoleń z zakresu ochrony danych osobowych.

Osoba pełniąca funkcję IOD posiadała niezbędne kwalifikacje zawodowe w tym zakresie (m.in. pełniła wcześniej funkcję Administratora Bezpieczeństwa Informacji).

(akta kontroli str. 53-76, 117-143)

1.8. Zgodnie z Regulaminem organizacyjnym Urzędu Miasta Otwocka[13] IOD podlegał bezpośrednio Prezydentowi, co było zgodne z art. 38 ust. 3 RODO. Prezydent poinformował, że osoba wyznaczona na IOD nie pełni w Urzędzie innych funkcji.

(akta kontroli str. 5-52, 568-604)

1.9. Prezydent Miasta Otwocka 24 marca 2023 r. na podstawie art. 21 ust. 1 i 3 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa[14] (dalej: ustawa o ksc) wyznaczył osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Osobą tą był p.o. Naczelnika Wydziału Informatyki. Zgłoszenie osoby kontaktowej zostało przekazane do CSIRT NASK[15] zgodnie z art. 22 ust. 1 pkt 5 ustawy o ksc.

(akta kontroli str. 113-116)

1.10. W wyniku oględzin oprogramowania[16] wykorzystywanego w Urzędzie do gromadzenia aktualnych informacji w zakresie posiadanego sprzętu informatycznego stwierdzono, że oprogramowanie to umożliwia bieżący monitoring sprzętu IT oraz zawiera informacje o jego konfiguracji. Było to zgodne z § 19 ust. 2 pkt 2 rozporządzenia KRI.

(akta kontroli str. 53-76, 617-625)

1.11. Urząd 14 grudnia 2023 r. złożył wniosek o przystąpienie do programu „Cyberbezpieczny Samorząd". Wartość projektu to 919 677,17 zł (w tym dofinansowanie ze środków Unii Europejskiej: 846 103,03 zł i wkład własny: 73 574,14 zł). Umowa o powierzenie grantu pomiędzy Miastem Otwock a Centrum Projektów Polska Cyfrowa została podpisana 8 lipca 2024 r., a koniec okresu realizacji projektu został wyznaczony na 30 czerwca 2026 r. W ramach projektu planowane jest m.in.: wdrożenie SZBI, szkolenia pracowników z zakresu bezpieczeństwa informacji oraz zakup generatora prądotwórczego.

(akta kontroli str. 53-76, 88-96, 676-705)

---

11 Dalej: IOD.

12 W okresie objętym kontrolą obowiązywały trzy umowy: umowa nr WOR.142.2.2022 z dnia 1 czerwca 2022 r. (aneksowana 2 stycznia 2023 r. oraz 1 lutego 2023 r.), umowa nr WOR.142.2.2023 z 7 marca 2023 r. oraz WOR.142.3.2023 z 29 grudnia 2023 r.

13 Wprowadzonego zarządzeniem nr 1/2020 Prezydenta Miasta Otwocka z dnia 2 stycznia 2020 r. w sprawie nadania regulaminu organizacyjnego Urzędu Miasta Otwocka.

14 Dz. U. z 2024 r. poz. 1077.

15 Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy.

16 Oprogramowanie: Watchguard, UniFi Network oraz Observium.

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1. W Urzędzie nie zidentyfikowano wszystkich posiadanych i przetwarzanych zbiorów danych (innych niż zbiory danych osobowych). Ponadto zidentyfikowanych danych nie sklasyfikowano z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację. Było to niezgodne z pkt A.8.1.1 i A.8.2.1 załącznika A normy PN-EN ISO/IEC 27001:2017, stanowiącymi że należy zidentyfikować informacje, aktywa związane z informacjami i środkami przetwarzania informacji oraz sporządzić i utrzymywać ewidencję tych aktywów; informacje powinny być klasyfikowane z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację.

   Prezydent wyjaśnił, że *klasyfikacja z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości zaplanowana jest przy wdrożeniu SZBI w ramach projektu „Cyberbezpieczny Samorząd"*.

   (akta kontroli str. 53-76, 324-331)

2. W Urzędzie nie ustanowiono i nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji, w szczególności Polityki Bezpieczeństwa Informacji.

   Było to niezgodne z § 19 ust. 1 rozporządzenia KRI, stanowiącym że podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali System Zarządzania Bezpieczeństwem Informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Ponadto § 19 ust. 3 rozporządzenia KRI wskazuje, że wymagania określone w ww. ust. 1 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą[17].

   Prezydent wyjaśnił, że *SZBI zostało ujęte w projekcie „Cyberbezpieczny Samorząd", rozpoczęcie wdrożenia jest zaplanowane na bieżący rok*.

   (akta kontroli str. 53-76, 503-537)

3. W Urzędzie nie prowadzono analiz ryzyka w związku z potrzebą zachowania ciągłości działania systemów informatycznych, co było działaniem nierzetelnym.

   Prezydent wyjaśnił, że *analiza ryzyka w związku z potrzebą zachowania ciągłości działania systemów informatycznych była prowadzona do tej pory w sposób niesformalizowany. Wynikiem prowadzenia tej analizy są elementy wkładu merytorycznego do wniosku w projekcie „Cyberbezpieczny Samorząd". Prowadzenie powyższej analizy ryzyka w sposób sformalizowany jest zaplanowane na wdrożenie SZBI, które będzie miało miejsce w tym roku.*

   Zdaniem NIK prowadzenie usystematyzowanych analiz ryzyka nie jest możliwe w sposób niesformalizowany, gdyż jest to bardzo rozbudowany i złożony proces.

   (akta kontroli str. 53-76, 97-102, 588-602)

[17] W tym: PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem, PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

4. W Urzędzie nie ustanowiono polityk ciągłości działania oraz nie opracowano planów zapewnienia ciągłości działania oraz planów odtworzeniowych, co było nierzetelne.

   Prezydent wyjaśnił, że *projekt procedury zapewnienia ciągłości działania procesów jest zawarty w złożonym projekcie dokumentacji SZBI (…)* oraz, że *plan ciągłości działania oraz plany odtworzeniowe są w trakcie projektowania przed wdrożeniem SZBI*.

   NIK wskazuje, że właściwe zarządzanie ciągłością działania jest kluczowe, gdyż umożliwia ono odtworzenie działalności po katastrofie lub innym incydencie zakłócającym działanie. Służą temu przygotowane polityki ciągłości działania, a działania w nich określone podlegają okresowemu testowaniu.

(akta kontroli str. 53-76, 558-561)

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli ocenia negatywnie działalność kontrolowanej jednostki w zakresie organizacji bezpieczeństwa informacji oraz zapewnienia ciągłości działania systemów informatycznych ze względu na to, że w Urzędzie nie ustanowiono i nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji (w szczególności Polityki Bezpieczeństwa Informacji), nie zidentyfikowano wszystkich zbiorów danych Urzędu podlegających zabezpieczeniu oraz nie ustanowiono i nie wdrożono polityk w ramach zapewnienia ciągłości działania.

W Urzędzie natomiast prawidłowo realizowano zadania dotyczące m.in.: opracowania dokumentacji z zakresu ochrony danych osobowych oraz gromadzenia aktualnych informacji o zasobach informatycznych obejmujących ich rodzaj i konfigurację.

OBSZAR

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

Opis stanu faktycznego

2.1. Kontrola wykazała, że w przypadku jednego z 10 objętych badaniem komputerów służbowych użytkujący go pracownik posiadał uprawnienia administratora umożliwiające zainstalowanie nieautoryzowanego oprogramowania (dalszy opis w części *Stwierdzone nieprawidłowości)*. Użytkownicy pozostałych dziewięciu komputerów nie posiadali tego typu uprawnień.

Odnośnie zabezpieczenia wykorzystywanych w Urzędzie tabletów i smartfonów przed instalacją przez użytkownika dowolnego oprogramowania, Prezydent wyjaśnił, że *w Urzędzie ze względu na brak środków na zakup oprogramowania MDM z wymienioną funkcjonalnością, nie ma możliwości zastosowania tego typu blokad. Z tego względu urządzenia mobilne nie posiadają dostępów do oprogramowania i usług Urzędu i pełnią wprost jedynie funkcję komunikacyjną w postaci rozmów głosowych i/lub dostępu do komercyjnych usług zewnętrznych*.

(akta kontroli str. 588-597, 609-613)

2.2. Analiza uprawnień do systemów informatycznych 15 pracowników Urzędu (w tym sześciu na stanowiskach kierowniczych) wykazała, że uczestniczyli oni w procesie przetwarzania informacji w stopniu adekwatnym do realizowanych przez nich zadań, co było zgodne z § 19 ust. 2 pkt 4 rozporządzenia KRI.

Ponadto ustalono, że nadawanie i odbieranie uprawnień użytkownikom systemów informatycznych Urzędu było dokumentowane w postaci tzw. Arkuszów użytkownika, co było zgodne z przyjętą w tym zakresie w Urzędzie „Procedurą zarządzania uprawnieniami do przetwarzania danych i rejestrowania tych uprawnień”[18].

[18] Stanowiącą część Instrukcji zarządzania zasobami informatycznymi.

(akta kontroli str. 429-435, 558-587, 706)

2.3. W okresie objętym kontrolą zatrudnienie w Urzędzie zakończyło 10 osób. Ustalono, że ich konta w systemach informatycznych Urzędu były nadal aktywne (dalszy opis w części *Stwierdzone nieprawidłowości*).

(akta kontroli str. 656-657)

2.4. W wyniku oględzin trzech systemów informatycznych zarządzanych przez Urząd[19] stwierdzono, że nie zostały spełnione wymagania dla haseł dostępu do tych systemów określone w Polityce Haseł zawartej w procedurze pn. „Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem"[20] (dalszy opis w części *Stwierdzone nieprawidłowości*).

Ponadto w trakcie ww. oględzin systemu informatycznego Groszek (Moduł Auta), zidentyfikowano występowanie w tym systemie loginów użytkowników, których nazwa nie pozwalała na bezpośrednie powiązanie z danym pracownikiem Urzędu (dalszy opis w części *Stwierdzone nieprawidłowości*)

(akta kontroli str. 451-455, 640-651)

2.5. W wyniku oględzin dwóch stanowisk pracy, gdzie obywatele załatwiają sprawy z zakresu wydawania dowodów osobistych, stwierdzono że monitory były nachylone w sposób umożliwiający klientom Urzędu wgląd do treści na nich wyświetlanych (dalszy opis w części *Stwierdzone nieprawidłowości*).

(akta kontroli str. 605-608)

2.6. W Urzędzie zasady wykonywania pracy zdalnej zostały opisane w zawartych w Instrukcji zarządzania zasobami informatycznymi regulacjach pn. „Zasady telepracy", w których określono mechanizmy gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość. Było to zgodne z § 19 ust. 2 pkt 8 rozporządzenia KRI.

Jak poinformował Prezydent, Instrukcja zarządzania zasobami informatycznymi została przedstawiona do zapoznania i stosowania pracownikom Urzędu w trakcie szkoleń z ochrony danych osobowych, na których omawiane są poszczególne dokumenty wewnętrzne polityki.

(akta kontroli str. 475-476, 538-557)

2.7. Jak poinformował Prezydent, w Urzędzie stosuje się specjalne oprogramowanie odpowiedzialne za szyfrowanie danych na dyskach twardych komputerów przenośnych. Było to zgodne z § 19 ust. 2 pkt 9 i 11 rozporządzenia KRI.

(akta kontroli str. 558-561)

2.8. W serwerowni Urzędu zastosowano rozwiązania umożliwiające zabezpieczenie informacji przed nieuprawnionym jej ujawnieniem, modyfikacją, usunięciem lub zniszczeniem. W trakcie oględzin pomieszczenia serwerowni stwierdzono jednak, że znajdowały się w nim materiały łatwopalne (dalszy opis w części *Stwierdzone nieprawidłowości*).

(akta kontroli str. 614-616)

2.9. Analiza czterech umów serwisowych zawartych przez Miasto z podmiotami zewnętrznymi w okresie objętym kontrolą wykazała, że poprzez umieszczenie w nich stosownych postanowień zagwarantowany został odpowiedni poziom bezpieczeństwa informacji. Było to zgodne z w § 19 ust. 2 pkt 10 rozporządzenia KRI.

(akta kontroli str. 658-675)

---

19 Systemy: R2płatnik, Sigid oraz Groszek (Moduł Auta).

20 Stanowiącej część Instrukcji zarządzania zasobami informatycznymi.

2.10. W zakresie wydawania sprzętu komputerowego zewnętrznemu serwisowi lub jego zbycia w Urzędzie w ramach Instrukcji zarządzania zasobami informatycznymi przyjęto „Procedurę wykonywania przeglądów i konserwacji". Ponadto jako dokument wewnętrzny dla pracowników Wydziału Informatyki obowiązywały „Zasady wydawania sprzętu poza Urząd". Zgodnie z ww. zasadami serwisowany lub zbywany sprzęt komputerowy mógł być przekazany do podmiotów zewnętrznych po usunięciu nośników informacji. Powyższe spełniało wymogi określone w § 19 ust. 2 pkt 7 i 9 rozporządzenia KRI.

(akta kontroli str. 425-426, 556)

2.11. W Urzędzie, w ramach Instrukcji zarządzania zasobami informatycznymi przyjęto procedurę pn. „Tworzenie, testowanie i odtwarzanie kopii zapasowych", która określała m.in. zasady przechowywania kopii zapasowych.

W wyniku oględzin sposobu sporządzania kopii zapasowych i ich przechowywania stwierdzono, że w Urzędzie stale prowadzone są działania w zakresie bieżącego sporządzania kopii zapasowych w środowisku wirtualnym oraz jednego serwera fizycznego. Dla każdej kopii zapasowej została przewidziana retencja danych wypełniając wymogi przechowywania kopii zapasowych określone w zakresie zarządzania danymi osobowymi. W zakresie środowiska wirtualnego sporządzane są kopie dzienne, pełne oraz kopia tygodniowa pełna. Serwer fizyczny ma określone sporządzanie kopii w trybie dziennym (kopia różnicowa) oraz tygodniowym (kopia pełna).

Ponadto stwierdzono, że w Urzędzie zastosowano trójstopniowy model przechowywania kopii zapasowych, który wypełnia wymóg, iż kopia zapasowa jest przechowywana poza miejscem wytwarzania danych. Dostęp do sporządzonych kopii zapasowych posiadają pracownicy Wydziału Informatyki.

W wyniku oględzin ustalono również, że prowadzone są okresowe testowe odtworzenia danych.

(akta kontroli str. 412-424, 626-639)

2.12. W Urzędzie nie wprowadzono procedury monitorowania zajętości przestrzeni dyskowej serwerów. P.o. Naczelnika Wydziału informatyki poinformował, że informatycy na bieżąco monitorują zasoby dyskowe wykorzystywanych serwerów.

W wyniku oględzin stopnia zajętości przestrzeni dyskowej w trzech serwerach wykorzystywanych przez Urząd stwierdzono, że przypadku dwóch z nich poziom zajętości wynosił odpowiednio ok. 20% i 25%. W przypadku trzeciego serwera[21] łączny poziom zajętości dysku serwera nie przekraczał 80%, natomiast poziom zajętości jednej z sześciu partycji tego dysku wynosił 99%. Partycja ta, jak poinformował p.o. Naczelnika Wydziału Informatyki służy do zapisywania danych z systemu informatycznego Groszek.

Prezydent wyjaśnił, że *sytuacja z zajętością partycji (…) jest doskonale znana Wydziałowi Informatyki, jest pod kontrolą i jest stale monitorowana. Pozostały 1% oznacza […][22]. Mała ilość miejsca na jednej z partycji nie ma wpływu na wydajność macierzy dyskowej serwera […][23]*.

(akta kontroli str. 598-602, 652-655)

---

[21] O nazwie: […] Wyłączenie jawności informacji na podstawie art. 5 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902).

[22] Wyłączenie jawności informacji na podstawie art. 5 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902).

[23] Wyłączenie jawności informacji na podstawie art. 5 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902).

2.13. W Urzędzie, w ramach zapewnienia ciągłości działania, w sposób udokumentowany, nie zidentyfikowano kluczowych elementów infrastruktury i usług IT oraz ich zabezpieczenia pod kątem wpływu czynników zewnętrznych (dalszy opis w części *Stwierdzone nieprawidłowości)*.

(akta kontroli str. 558-561)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1. Na podstawie oględzin 10 stanowisk komputerowych w Urzędzie ustalono, że jeden z pracowników posiadał uprawnienia do instalowania nieautoryzowanego oprogramowania. Było to niezgodne z wymaganiami określonymi w § 19 ust. 2 pkt 4 rozporządzenia KRI.

   P.o. Naczelnika Wydziału Informatyki wyjaśnił, że wynikało to z przeoczenia. W trakcie kontroli nieprawidłowość została usunięta, w związku z tym NIK nie formułuje wniosku pokontrolnego w tym zakresie.

   (akta kontroli str. 588-597, 609-613)

2. Stwierdzono, że według stanu na dzień 3 lipca 2024 r. wszystkie 10 osób, które w okresie od 1 stycznia 2023 r. do 3 czerwca 2024 r. zakończyły zatrudnienie w Urzędzie, nadal posiadały aktywne konta w systemie informatycznym EZD. Ponadto ustalono, że w przypadku czterech z 10 osób, ich konta w domenie Urzędu były nadal aktywne (nie były zablokowane ani usunięte), oraz że nadal aktywne było konto jednego pracownika wykonującego zadania w systemie Groszek UmowyFV.

   Było to niezgodne z § 19 ust. 2 pkt 5 rozporządzenia KRI, stanowiącym że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji.

   P.o. Naczelnika Wydziału Informatyki, wyjaśnił, że brak usunięcia/zablokowania kont w przypadkach wskazanych wyżej wynika z niedopatrzenia.

   Natomiast Prezydent odnośnie niezablokowanych kont w domenie Urzędu wyjaśnił, że *analiza sytuacji wykazała, że (…) konta zostały odblokowane i zmienione zostały hasła w celu uzyskania dostępu do plików służbowych na potrzebę ich przełożonych. Nie określono terminu ponownej blokady tych kont*. Odnośnie systemu EZD, Prezydent wyjaśnił, że *praktyką przyjętą przez Wydział Informatyki w celu zablokowania dostępu do EZD była zmiana hasła. Wynikło to przyjętych zwyczajów przekazanych przez byłych pracowników Wydziału Informatyki. W wyniku bieżącej kontroli odnaleziono i zastosowano w EZD funkcję blokowania użytkowników.*

   NIK zauważa, że odbieranie uprawnień do systemów informatycznych powinno odbywać się poprzez blokowanie lub usuwanie kont byłych pracowników w tych systemach a nie jedynie poprzez zmianę hasła dostępu. Zmiana hasła i dostęp innego pracownika niż ten do którego należy login uniemożliwia skuteczne rozliczanie z działań prowadzonych w systemie informatycznym.

   Ponadto odnośnie kont w domenie Urzędu, NIK zauważa, że funkcjonalność wykorzystywanego w Urzędzie mechanizmu Microsoft Active Directory pozwala na dostęp do plików służbowych byłych pracowników z poziomu administratora bez konieczności odblokowania kont tych pracowników. W związku z tym konta byłych pracowników powinny być zablokowane.

   (akta kontroli str. 598-602, 656-657)

3. W wyniku oględzin trzech systemów[24] informatycznych zarządzanych przez Urząd stwierdzono, że nie zostały spełnione wymagania dla haseł dostępu użytkowników do tych systemów określone w Polityce Haseł zawartej w procedurze pn. „Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem”[25]. Procedura ta określała wymogi dotyczące złożoności hasła oraz okresów po jakim hasło powinno być zmienione. W przypadku systemu R2płatnik nie określono wymagań odnośnie częstotliwości zmiany hasła. Natomiast w przypadku systemu SIGID wymagania w zakresie złożoności nie były zgodne z Polityką Haseł, a w zakresie częstotliwości zmiany hasła, w przypadku 6 z 11 użytkowników tego systemu, nie ustalono żadnych wymogów. Natomiast w przypadku systemu Groszek (Moduł Auta) nie zostały ustanowione żadne wymagania, co do złożoności i częstotliwości zmiany hasła. Powyższe było również niezgodne z § 19 ust. 2 pkt 7 rozporządzenia KRI.

   P.o. Naczelnika Wydziału Informatyki wyjaśnił, że wymogi dla haseł dostępu do trzech ww. systemów informatycznych zostaną niezwłocznie dostosowane do wymagań wynikających z obowiązującej w Urzędzie Polityki Haseł. O działaniach dostosowawczych w tym zakresie poinformował również Prezydent.

   W trakcie kontroli NIK stwierdzono, że powyższa nieprawidłowość została usunięta w przypadku dwóch ww. systemów[26].

   (akta kontroli str. 451-455, 588-597, 640-651)

4. W wyniku oględzin systemu informatycznego Groszek (Moduł Auta), wśród kont mających status aktywny, zidentyfikowano występowanie w tym systemie sześciu kont (loginów) użytkowników, których nazwa nie pozwala na bezpośrednie ich powiązanie z danym pracownikiem Urzędu.

   Prezydent wyjaśnił, że *według analizy przeprowadzonej przez Wydział Informatyki w trakcie kontroli podane konta nie są używane. Obecny skład Wydziału Informatyki nie zna przeznaczenia i charakteru tych kont, dlatego nie jest w stanie przewidzieć skutków wyłączenia tych kont. Między innymi występowanie takich zaszłości w systemie Groszek jest powodem konieczności standaryzacji i ponownego wdrożenia tego systemu*.

   Funkcjonowanie ww. kont w systemie informatycznym było niezgodne z § 19 ust. 2 pkt 4 i 5 rozporządzenia KRI. NIK zwraca uwagę, że nazwa użytkownika (login) w systemach informatycznych, w przypadku gdy nie są to konta techniczne, powinna pozwalać na identyfikację danego pracownika.

   (akta kontroli str. 598-602, 640-650)

5. W wyniku oględzin dwóch stanowisk pracy, gdzie obywatele załatwiają sprawy z zakresu wydawania dowodów osobistych, stwierdzono że monitory były nachylone w sposób umożliwiający klientom Urzędu wgląd do treści na nich wyświetlanych (m.in. dane osobowe). Było to niezgodne z § 19 ust. 2 pkt 7 rozporządzenia KRI. Sekretarz Miasta Otwocka, pełniąca również funkcję Naczelnika Wydziału Obsługi Mieszkańców i Podmiotów Gospodarczych wyjaśniła, że przez niedopatrzenie Wydziału Informatyki na monitory nie zostały nałożone filtry prywatyzujące.

   W trakcie kontroli NIK nieprawidłowość została usunięta, w związku z tym NIK nie formułuje wniosku pokontrolnego w tym zakresie.

   (akta kontroli str. 588-597, 605-608)

---

[24] Systemy: R2płatnik, Sigid oraz Groszek (Moduł Auta).
[25] Stanowiącej część Instrukcji zarządzania zasobami informatycznymi.
[26] R2płatnik oraz Groszek (Moduł Auta).

6. W trakcie oględzin serwerowni stwierdzono, że znajdują się w niej materiały łatwopalne, tj. kartony. Było to niezgodne z § 19 ust. 2 pkt 9 rozporządzenia KRI.

   W trakcie kontroli kartony zostały usunięte z pomieszczenia serwerowni, w związku z czym NIK nie formułuje wniosku pokontrolnego w tym zakresie.

   (akta kontroli str. 588-597, 614-616)

7. W Urzędzie, w ramach zapewnienia ciągłości działania, w sposób udokumentowany nie zidentyfikowano kluczowych elementów infrastruktury i usług IT oraz ich zabezpieczenia pod kątem wpływu czynników zewnętrznych, co było nierzetelne.

   Prezydent wyjaśnił, że *obszary krytyczne są zidentyfikowane i funkcjonują w świadomości Wydziału Informatyki. Sformalizowanie ww. zaplanowane jest na wdrożenie SZBI.*

   (akta kontroli str. 558-561)

OCENA CZĄSTKOWA

W Urzędzie, w okresie objętym kontrolą, podejmowano działania w zakresie zapewnienia bezpieczeństwa informacji m.in. poprzez prawidłowe przechowywanie i testowanie kopii zapasowych, nadawanie uprawnień pracownikom adekwatnie do realizowanych przez nich zadań oraz stosowanie w umowach serwisowych zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji. Wprowadzono również procedury dotyczące przekazywania sprzętu komputerowego podmiotom zewnętrznym oraz zasady pracy zdalnej.

Stwierdzone w tym obszarze nieprawidłowości dotyczyły m.in. możliwości instalowania przez pracownika do tego nieuprawnionego nieautoryzowanego oprogramowania, niespełniania przyjętych wymagań dla haseł dostępu w trzech systemach informatycznych oraz braku blokowania kont byłych pracowników w systemach informatycznych wykorzystywanych przez Urząd.

OBSZAR

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

3.1. W Urzędzie w okresie objętym kontrolą nie przeprowadzono okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji (dalszy opis w części *Stwierdzone nieprawidłowości*).

(akta kontroli str. 558-561)

3.2. Procedura w zakresie zgłaszania incydentów naruszenia bezpieczeństwa informacji w Urzędzie odnosiła się wyłącznie do danych osobowych (dalszy opis w części *Stwierdzone nieprawidłowości*). Sposób postępowania w przypadku wystąpienia incydentu naruszenia ochrony danych osobowych został opisany w przyjętej w ramach Polityki ochrony danych osobowych procedury pn. „Polityka zarządzania incydentem ochrony danych osobowych". Procedura uwzględniała postanowienia art. 33 i 34 RODO.

Prezydent poinformował, że w okresie objętym kontrolą nie wystąpił żaden incydent z zakresu naruszenia bezpieczeństwa informacji[27]. Jednocześnie wskazał, że *przyjętą w Urzędzie praktyką jest zgłaszanie przez pracowników podejrzeń wystąpienia incydentów do Wydziału Informatyki. Wydział Informatyki po zidentyfikowaniu incydentu niezwłocznie informuje Najwyższe Kierownictwo, które powołuje doraźny zespół do obsługi incydentu. Następnie, nie później niż w 24*

[27] Wg stanu na dzień 24 czerwca 2024 r.

godziny od wystąpienia incydentu informowany jest CSIRT NASK. Zgłoszenie przesyłane jest za pośrednictwem systemu S46 lub telefonicznie.

(akta kontroli str. 223-235, 558-561)

3.3. W okresie objętym kontrolą w Urzędzie przeprowadzono szkolenia pracowników z zakresu bezpieczeństwa informacji, co było zgodne z § 19 ust. 2 pkt 6 rozporządzenia KRI[28]. Zakres tematyczny tych szkoleń obejmował m.in. cyberbezpieczeństwo i ochronę danych osobowych.

(akta kontroli str. 53-76)

3.4. W Urzędzie w październiku 2023 r. przeprowadzono audyt z zakresu bezpieczeństwa informacji, co było zgodne z § 19 ust. 2 pkt 14 rozporządzenia KRI[29]. W jego wyniku sformułowano 18 rekomendacji. Jak poinformował Prezydent dotychczas zrealizowano sześć z nich[30], a pozostałe są planowane do zrealizowania, w szczególności w ramach realizacji projektu „Cyberbezpieczny Samorząd".

(akta kontroli str.144-191, 538-555)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1. W Urzędzie w okresie objętym kontrolą nie przeprowadzono okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji, co było niezgodne z § 19 ust. 2 pkt 3 rozporządzenia KRI[31].

   Prezydent wyjaśnił, że *okresowe analizy ryzyka utraty integralności, poufności lub dostępności informacji z okresu objętego kontrolą zostały wstrzymane i zaplanowane do przeprowadzenia wraz z wdrożeniem SZBI.*

   (akta kontroli str. 558-561)

2. Procedura w zakresie zgłaszania incydentów naruszenia bezpieczeństwa informacji w Urzędzie odnosiła się wyłącznie do danych osobowych. Było to niezgodne § 19 ust. 2 pkt 13 rozporządzenia KRI, który stanowi, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo warunków umożliwiających realizację i egzekwowanie bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

   Prezydent wyjaśnił, że *projekt procedury zgłaszania incydentów jest zawarty w złożonym projekcie dokumentacji SZBI.*

   (akta kontroli str. 223-235, 558-561)

OCENA CZĄSTKOWA

W Urzędzie, w okresie objętym kontrolą, podjęto działania w celu zapobiegania incydentom bezpieczeństwa informacji, tj. zorganizowano szkolenia pracowników oraz przeprowadzono audyt z zakresu bezpieczeństwa informacji.

Nie przeprowadzono natomiast okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji, a wprowadzona w Urzędzie procedura

---

[28] W dniach 7 i 21 sierpnia 2023 r. 150 pracowników wzięło udział w szkoleniu pn. „Szkolenie on-site z zakresu zagrożeń cyberbezpieczeństwa"; w dniach 23-25 sierpnia 5 pracowników Wydziału Informatyki uczestniczyło w szkoleniu pn. „Szkolenie on-site wydziału informatyki z zakresu bezpieczeństwa sieciowego i systemu zarządzania bezpieczeństwem informacji; 28 sierpnia 2023 r. przeprowadzono indywidualne szkolenie on-site dotyczące ochrony informacji dla czterech członków Kierownictwa Urzędu; 20 maja 2024 r. 120 pracowników wzięło udział w szkoleniu pn. „Szkolenie z zakresu ochrony danych osobowych – RODO".

[29] Na dzień przeprowadzenia audytu §20 ust. 2 pkt 14 rozporządzenia KRI z 12 kwietnia 2012 r.

[30] Według stanu na 14 czerwca 2024 r.

[31] Wcześniej, w okresie objętym kontrolą obowiązywał w tym zakresie § 20 ust. 2 pkt 3 rozporządzenia KRI z 12 kwietnia 2012 r.

w zakresie zgłaszania incydentów naruszenia bezpieczeństwa informacji odnosiła się wyłącznie do danych osobowych.

IV. Wnioski

W związku ze stwierdzonymi nieprawidłowościami, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, przedstawia wnioski:

Wnioski

1. Zidentyfikowanie wszystkich posiadanych i przetwarzanych informacji; sklasyfikowanie ich z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację; przypisanie informacjom odpowiedniego poziomu ochrony.
2. Ustanowienie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji, o którym mowa w § 19 ust. 1 rozporządzenia KRI uwzględniającego zalecenia normy PN-ISO/IEC 27001 i norm z nią związanych (PN-ISO/IEC 27002, PN-ISO/IEC 27005, PN-ISO/IEC 24762).
3. Prowadzenie analiz ryzyka w związku z potrzebą zachowania ciągłości działania systemów informatycznych Urzędu.
4. Ustanowienie polityk ciągłości działania oraz opracowanie i wdrożenie planów zapewnienia ciągłości działania i planów odtworzeniowych.
5. Zapewnienie niezwłocznego i trwałego odbierania byłym pracownikom Urzędu uprawnień do systemów informatycznych.
6. Zapewnienie stosowania haseł dostępu do systemów informatycznych zgodnych z wymaganiami wynikającymi z obowiązującej w Urzędzie Polityki Haseł.
7. Określanie nazw użytkowników (loginów) w systemach informatycznych wykorzystywanych przez Urząd w sposób umożliwiający identyfikację do kogo należą.
8. Zidentyfikowanie kluczowych elementów infrastruktury i usług IT oraz ich zabezpieczenia pod kątem wpływu czynników zewnętrznych.
9. Prowadzenie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji i podejmowanie działań minimalizujących stwierdzone ryzyko.
10. Ustanowienie i wdrożenie procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji uwzględniającej ogół zdarzeń zachodzących w Urzędzie (nie tylko z zakresu ochrony danych osobowych).

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 Departamentu Administracji Publicznej. 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.

Obowiązek poinformowania NIK o sposobie wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Warszawa, 2 sierpnia 2024 r.

Najwyższa Izba Kontroli
Departament Administracji Publicznej
w zastępstwie Dyrektora
Agnieszka Klimowicz
p.o. Wicedyrektor

/podpisano elektronicznie/

Kontroler
Tomasz Płudowski
Główny specjalista kontroli państwowej

/podpisano elektronicznie/

Kontroler
Mariusz Stolarz
Doradca techniczny

/podpisano elektronicznie/