NAJWYŻSZA IZBA KONTROLI

DEPARTAMENT ADMINISTRACJI PUBLICZNEJ

KAP.410.3.6.2024

Pan
Marek Banaszek
Burmistrz Miasta Józefowa

Urząd Miasta Józefowa
ul. Kardynała Wyszyńskiego 1
05-420 Józefów

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 Józefowa[1], ul. Kardynała Wyszyńskiego 1, 05-420 Józefów.
Kierownik jednostki kontrolowanej	Marek Banaszek, Burmistrz Miasta Józefowa, od 6 listopada 2018 r. (dalej: Burmistrz)
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 6 września 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	Tomasz Kwitowski, doradca techniczny, upoważnienie do kontroli nr KAP/49/2024 z 3 czerwca 2024 r.

(akta kontroli str. 1-2)

[1] Dalej: Urząd.
[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, ustanowiono i wdrożono System Zarządzania Bezpieczeństwem Informacji (dalej: SZBI), a w ramach niego Politykę Bezpieczeństwa Informacji (dalej: PBI), jednak stwierdzono nieprawidłowości wpływające na prawidłowe zarządzanie bezpieczeństwem informacji.

Burmistrz Miasta Józefowa, zgodnie z wymogami określonymi w RODO[4], powołał Inspektora Ochrony Danych (dalej: IOD) i umożliwił mu realizację zadań w sposób niezależny. Osoba pełniąca tę funkcję, a także inni pracownicy, którzy byli odpowiedzialni za bezpieczeństwo informacji, posiadali odpowiednie przygotowanie merytoryczne i doświadczenie zawodowe.

Wprowadzono zasady tworzenia haseł dostępu do systemów informatycznych, a zabezpieczenia komputerów pracowników uniemożliwiały zainstalowanie nieautoryzowanego oprogramowania. Zapoznano pracowników z ustanowionymi w Urzędzie zasadami pracy zdalnej. Prowadzono także elektroniczny rejestr zasobów teleinformatycznych, który umożliwiał weryfikację sprzętu oraz jego konfiguracji.

W Urzędzie zorganizowano szkolenia pracowników oraz przeprowadzono audyt z zakresu bezpieczeństwa informacji. Wprowadzono procedurę dotyczącą zarządzania incydentami naruszenia bezpieczeństwa informacji. W przypadku stwierdzenia incydentów podejmowano właściwe działania wyjaśniające i naprawcze.

Ponadto, w Urzędzie zabezpieczono serwerownię Urzędu przed nieuprawnionym dostępem. Uprawnienia nadawano pracownikom adekwatnie do realizowanych przez nich zadań. Pojemnością wykorzystywanej przestrzeni dyskowej zarządzano w sposób zapewniający właściwą wydajność systemów.

Należy zauważyć, że w Urzędzie wdrożono klaster serwerów w celu zapewnienia ciągłości działania środowiska serwerowego Urzędu, jak i zaplanowano zakup wydajniejszego serwera repliki, który umożliwi szybsze odtworzenie wirtualnych serwerów w przypadku awarii oraz zakup dwóch macierzy dyskowych przeznaczonych do wykonywania backupu klastra serwerów oraz do przechowywania repliki backupu poza serwerownią Urzędu.

Stwierdzone w trakcie kontroli nieprawidłowości polegały m.in. na:

- niezapewnieniu przechowywania kopii zapasowych danych z badanych systemów informatycznych poza miejscem wytwarzania danych, co stanowiło naruszenie §19 ust. 2 pkt 12 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[5] (dalej: rozporządzenie KRI),
- nieustanowieniu polityk ciągłości działania oraz nieopracowaniu planów zapewnienia ciągłości działania oraz planów odtworzeniowych, co było nierzetelne,

---

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

[4] Rozporządzenie 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), Dz. Urz. UE L 119 z 04.05.2016 r., str. 1, ze zm.

[5] Dz. U. poz. 773. Weszło w życie 23 maja 2024 r. Poprzednio 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: stare rozporządzenie KRI.

- niewprowadzeniu do systemu służącego m.in. do inwentaryzacji sprzętu informatycznego oraz monitorowania dostępu do danego urządzenia i systemu informatycznego przez pracowników Urzędu dwóch urządzeń IT, co stanowiło naruszenie § 19 ust. 2 pkt 2 rozporządzenia KRI,
- niedokonaniu pełnej identyfikacji aktywów informacyjnych wymagających ochrony i niespisaniu innych informacji wymagających ochrony, takich jak powierzone przez kontrahentów tajemnice przedsiębiorstwa, zasady bezpieczeństwa fizycznego i informatycznego w jednostce, informacje finansowe z deklaracji podatkowych itp., co było nierzetelne,
- niespełnieniu wymagań dla haseł dostępu użytkowników do dwóch systemów, co było niezgodne z § 19 ust. 2 pkt 7 rozporządzenia KRI, a także z pkt 4 Instrukcji Zarządzania Systemami Informatycznymi (dalej: IZSI) pn. „Stosowane metody i środki uwierzytelniania w systemie oraz procedury związane z ich zarządzaniem i użytkowaniem".

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[6] kontrolowanej działalności

OBSZAR

1. Organizacja bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych

Opis stanu faktycznego

1. W Urzędzie poza danymi osobowymi ujętymi w „Rejestrze zbiorów danych osobowych przetwarzanych przez Administratora Danych Osobowych w Urzędzie Miasta Józefowa" i poza bazami danych ujętymi w załączniku nr 6 „Schemat tworzenia kopii zapasowych" do IZSI, nie zidentyfikowano innych zbiorów danych podlegających zabezpieczeniu (dalszy opis w części *Stwierdzone nieprawidłowości*).

(akta kontroli str. 12-13, 566-576)

2. W okresie objętym kontrolą w Urzędzie obowiązywały zarządzenia: Nr 66/2018 Burmistrza Miasta Józefowa z dnia 22 czerwca 2018 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych, Instrukcji Zarządzania Systemami Informatycznymi oraz Procedury zgłaszania i obsługi incydentów naruszeń bezpieczeństwa informacji w Urzędzie Miasta Józefowa (dalej: Polityka Bezpieczeństwa Informacji i Ochrony Danych Osobowych) i Nr 67/2018 Burmistrza Miasta Józefowa z dnia 22 czerwca 2018 r. w sprawie wprowadzenia Regulaminu określającego zasady i procedury korzystania z zasobów informatycznych w Urzędzie Miasta Józefowa, a od 11 czerwca 2024 r. zarządzenie Nr 99/2024 Burmistrza Miasta Józefowa w sprawie wprowadzenia „Polityki Ochrony Danych Osobowych w Urzędzie Miasta Józefowa" (dalej: Polityka Ochrony Danych Osobowych), której elementami są m.in. Regulamin określający zasady i procedury korzystania z zasobów informatycznych w Urzędzie Miasta Józefowa (dalej: Regulamin), IZSI oraz PBI. Powyższe regulacje w Urzędzie składały się na SZBI, o którym mowa w § 19 ust. 1 w zw. z ust. 3 rozporządzenia KRI. O wprowadzeniu *Polityki Ochrony Danych Osobowych* w Urzędzie powiadomiono kadrę kierowniczą mailem wysłanym 18 czerwca 2024 r., a także opublikowano ten dokument na wewnętrznym portalu ABC_Urzędnika.

(akta kontroli str. 27-222, 481-554, 610-611)

[6] 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.

3. W okresie objętym kontrolą obowiązywały *Polityka bezpieczeństwa Informacji i Ochrony Danych Osobowych* oraz *Polityka Ochrony Danych Osobowych*, uwzględniające wymogi RODO. Ww. dokumenty zostały zakomunikowane mailowo wszystkim pracownikom Urzędu z obowiązkiem stosowania, jak również opublikowane na wewnętrznym portalu ABC-Urzędnika. W ww. dokumentach określono m.in. obowiązki administratora danych osobowych oraz osób zaangażowanych w przetwarzanie danych osobowych.

(akta kontroli str. 481-554, 610-611)

4. W związku z potrzebą zapewnienia ciągłości działania systemów informatycznych w Urzędzie w dniu 10 stycznia 2024 r. Referat Informatyki opracował *Rejestr ryzyk*, w którym wskazano m.in. zidentyfikowane ryzyka, czynniki ryzyka, zastosowane środki kontroli ryzyka, prawdopodobieństwa wystąpienia ryzyka oraz ich skutki, a także prawdopodobieństwo ich wystąpienia i określono reakcje na ryzyko. W dniu 4 stycznia 2024 r. Zastępca Burmistrza wraz z Inspektor Ochrony Danych Osobowych w Urzędzie (dalej: IOD) opracowali *Analizę zagrożeń i ryzyka przy przetwarzaniu danych osobowych*, w której zawarto m.in. prawdopodobieństwo wystąpienia zagrożenia, przykładowe zagrożenia, skutki naruszenia, sposoby postępowania z ryzykiem, jak również zalecenia dotyczące zminimalizowania ryzyka wystąpienia braku ciągłości działania systemów informatycznych w Urzędzie. Burmistrz wyznaczył w Urzędzie osoby odpowiedzialne za wdrożenie zaleceń IOD oraz monitorowanie zagrożeń.

(akta kontroli str. 223-426, 577-580)

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. 555-565, 899-903, 977-982)

6. Zgodnie z § 19 ust. 2 pkt 1 rozporządzenia KRI, w Urzędzie w okresie objętym kontrolą dokonano przeglądu regulacji wewnętrznych stanowiących SZBI, czego efektem było wprowadzenie od 11 czerwca 2024 r. nowej *Polityki Ochrony Danych Osobowych.* W Urzędzie nie wyznaczono formalnie osoby odpowiedzialnej za opracowanie, wdrożenie, ocenę, przegląd i modyfikację PBI oraz osób odpowiedzialnych za zapewnienie ciągłości działania. PBI została opracowana przez Referat Informatyki oraz IOD. Burmistrz poinformował, że *w Urzędzie przyjęto założenie, że osobami kompetentnymi do wykonania SZBI są pracownicy Referatu Informatyki oraz Inspektor Ochrony Danych, ale nie zostali oni formalnie wyznaczeni jako osoby odpowiedzialne za opracowanie, wdrożenie, ocenę, przegląd i modyfikację PBI oraz jako osoby odpowiedzialne za zapewnienie ciągłości działania. Obowiązek zapewnienia ciągłości działania systemu informatycznego wynika z zakresu obowiązków pracowników Referatu Informatyki*.

(akta kontroli str. 27-222, 555-565, 899-903, 977-982)

7. Burmistrz jako Administrator Danych Osobowych (dalej: ADO) oraz jako Kierownik Urzędu Miasta wyznaczył IOD sprawującego nadzór w imieniu Burmistrza nad wdrożonym w Urzędzie systemem zarządzania w celu sprawowania nadzoru nad przestrzeganiem obowiązujących zasad bezpieczeństwa danych, w tym danych osobowych, a także Administratora Systemu Informatycznego (dalej: ASI) dbającego o bezpieczeństwo i utrzymanie ciągłości działania sieci teleinformatycznych oraz systemów i oprogramowania używanego w Urzędzie.

Zadania w zakresie bezpieczeństwa informacji oraz zapewnienia ciągłości działania systemów teleinformatycznych zostały określone w zakresach obowiązków trzech pracowników Referatu Informatyki. Pracownicy ci posiadali wyższe wykształcenie

o profilu informatycznym, a także ukończyli szkolenia związane z bezpieczeństwem systemów teleinformatycznych.

(akta kontroli str. 140-154, 633-645)

8. W Urzędzie, na podstawie zarządzenia Nr 198/2023 Burmistrza Miasta Józefowa z dnia 18 września 2023 r. wyznaczony został Inspektor Ochrony Danych Osobowych. W zawartej umowie cywilnoprawnej[7] wśród obowiązków IOD wskazano m.in. realizowanie polityk administratora w dziedzinie ochrony danych osobowych, monitorowanie przestrzegania RODO oraz innych przepisów Unii i państw członkowskich oraz polityk administratora, szkolenie personelu uczestniczącego w operacjach przetwarzania, przeprowadzanie systematycznych audytów, w szczególności w zakresie zgodności przetwarzania danych.

Osoba pełniąca funkcję IOD posiadała niezbędne kwalifikacje zawodowe w tym zakresie (m.in. posiada certyfikaty Stowarzyszenia Inspektorów Ochrony Danych i TÜV NORD - Audytora Wiodącego Systemu Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO/IEC 27001:2023-08, świadectwa ukończenia studiów podyplomowych w zakresie cyberbezpieczeństwa i informatyki śledczej oraz zarządzania cyberbezpieczeństwem). Powyższe było zgodne z art. 37 ust. 1 i 5 RODO oraz art. 8 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[8].

(akta kontroli str. 646-661)

9. Burmistrz Miasta Józefowa 9 września 2021 r. na podstawie art. 21 ust. 1 w związku z art. 4 pkt 7 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa[9] (dalej: ustawa o ksc) wyznaczył osoby odpowiedzialne za utrzymywanie kontaktów z podmiotem krajowego systemu cyberbezpieczeństwa. Osobami tymi byli Kierownik Referatu Informatyki i Inspektor w Referacie Informatyki. Zgłoszenie osób kontaktowych zostało przekazane do CSIRT NASK[10] zgodnie z art. 22 ust. 1 pkt 5 ustawy o ksc.

(akta kontroli str. 662-664)

10. W Urzędzie prowadzono elektroniczny rejestr zasobów teleinformatycznych za pomocą systemu GLPI (służącego m.in. do zarządzania zasobami IT, w tym do inwentaryzacji sprzętu informatycznego oraz monitorowania dostępu do danego urządzenia i systemu informatycznego przez pracowników Urzędu). W wyniku przeprowadzonych oględzin sprzętu informatycznego znajdującego się w Urzędzie, tj. próby 10 komputerów stacjonarnych, jednego serwera, dwóch laptopów, jednego routera i jednej drukarki stwierdzono, że dane zawarte w systemie GLPI umożliwiały zweryfikowanie, który pracownik jest użytkownikiem ww. sprzętu informatycznego oraz w jaki sposób sprzęt ten jest skonfigurowany, poza serwerem i routerem, które nie zostały wprowadzone do systemu ewidencji sprzętu i oprogramowania (dalszy opis w części *Stwierdzone nieprawidłowości*).

(akta kontroli str. 7-11, 14-26)

11. Urząd 13 grudnia 2023 r. złożył wniosek o przystąpienie do programu „Cyberbezpieczny Samorząd". Wartość projektu to 988 372,00 zł (w tym dofinansowanie ze środków Unii Europejskiej: 850 000,00 zł i wkład własny: 138 372,00 zł). Umowa o powierzenie grantu pomiędzy Miastem Józefów a Centrum Projektów Polska Cyfrowa została podpisana 12 czerwca 2024 r., a koniec okresu realizacji projektu został wyznaczony na 30 czerwca 2026 r. W ramach projektu

---

7 Umowa na pełnienie funkcji inspektora ochrony danych nr 712/2023 z dnia 28 grudnia 2023 r.

8 Dz. U. z 2019 r. poz. 1781.

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

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

planowane jest m.in.: przeprowadzenie obowiązkowego audytu systemu zarządzania bezpieczeństwem informacji; opracowanie kompleksowej dokumentacji SZBI obejmującej m.in. aktualizację PBI, badanie analizy ryzyka i jej wdrożenie w Urzędzie; zlecenie opracowania kompleksowego programu szkoleniowego oraz zakup platformy szkoleniowej w celu zapewnienia regularnego podnoszenia poziomu świadomości cyberbezpieczeństwa dla pracowników Urzędu oraz dla kadry zarządzającej i służb IT w zakresie planowanych do zastosowania środków bezpieczeństwa w ramach projektu grantowego. Planowany jest również zakup serwera i dwóch macierzy dyskowych przeznaczonych do wykonywania backupu oraz do przechowywania repliki backupu poza serwerownią UM Józefowa.

(akta kontroli str. 427-456, 472-480)

Stwierdzone nieprawidłowości

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

1. W Urzędzie nie dokonano pełnej identyfikacji aktywów informacyjnych wymagających ochrony. Przeprowadzono ją wyłącznie w odniesieniu do danych osobowych. Danym tym nie przypisano odpowiednich wag zgodnych z ich istotnością i nie przypisano odpowiedniego poziomu ochrony. Zidentyfikowanych danych nie sklasyfikowano z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację. Było to nierzetelne. Ponadto, jak wskazano w pkt A.8.1.1 i pkt 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 te powinny być klasyfikowane z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację.

Burmistrz wyjaśnił, że *W Urzędzie Miasta Józefowa zidentyfikowano kluczowe systemy, które podlegają zabezpieczeniom, co zostało opisane w Załączniku nr 6 do IZSI Urzędu Miasta Józefów, a wprowadzonej zarządzeniem nr 99/2024 z dnia 11 czerwca 2024 roku. Z uwagi na to, że system backup'u który wdrożono w Urzędzie Miasta Józefowa wykonuje kopie zabezpieczające całych wirtualnych serwerów uznano, że dane, które znajdują się na tych serwerach mają jednakową wagę, jednakże dodatkowa kopia zabezpieczająca kluczowych baz danych i aplikacji jest wykonywana na zewnętrzne nośniki danych, które przechowywane są w żaroodpornym sejfie. W ramach realizacji projektu grantowego „Cyberbezpieczny Samorząd" planowane jest wykonanie audytu obecnie posiadanej dokumentacji SZBI i aktualizacja jej pod kątem zgodności z obecnie obowiązującymi przepisami prawa i normami.*

Zdaniem NIK, należy zidentyfikować wszystkie zbiory danych wymagające ochrony i przypisać im odpowiednie wagi. Identyfikacją należy objąć m.in.: powierzone przez kontrahentów tajemnice przedsiębiorstwa, zasady bezpieczeństwa fizycznego i informatycznego w jednostce, informacje finansowe z deklaracji podatkowych.

(akta kontroli str. 7-13, 558-576, 899-903, 977-982)

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

Burmistrz wyjaśnił, że *w lipcu 2023 roku w Urzędzie Miasta Józefowa wdrożono klaster Hyper-V Windows Server 2019. Elementem wdrożenia jest dokumentacja podjętych działań, w której jako podstawowy cel wdrożenia klastra Hyper-V wskazano zapewnienie ciągłości działania środowiska serwerowego Urzędu. Z uwagi na zakres informacji zawartych w tej dokumentacji, których ujawnienie może stanowić zagrożenie, dokumentacja ta dostępna jest tylko dla pracowników Referatu*

Informatyki. Pozostałymi dokumentami stanowiącymi elementy polityki ciągłości działania są „Polityka bezpieczeństwa Informacji" „Instrukcja Zarzadzania Systemami Informatycznymi – UM Józefów".

Zdaniem NIK, samo wdrożenie klastra nie gwarantuje w pełni zminimalizowania ryzyka utraty ciągłości działania w przypadku wystąpienia takiego incydentu, jak np. zalanie czy pożar. Istotne jest zatem opracowanie i wdrożenie polityk w odniesieniu do wszystkich stwierdzonych ryzyk.

(akta kontroli str. 558-565, 612- 632, 977-982)

3. Do systemu GLPI, służącego m.in. do inwentaryzacji sprzętu informatycznego oraz monitorowania dostępu do danego urządzenia i systemu informatycznego przez pracowników Urzędu, nie wprowadzono informacji o serwerze oraz routerze, co było niezgodne z § 19 ust. 2 pkt 2 rozporządzenia KRI. Ponadto stwierdzono, że:

- w przypadku komputera znajdującego się w Referacie Windykacji Należności nr inwentaryzacyjny na komputerze był inny, niż w systemie GLPI;
- w przypadku laptopa znajdującego się w Referacie Wymiaru i Kontroli Podatkowej, w systemie miał on status „REZERWA" i powinien znajdować się w Referacie Informatyki, a znajdował się w pokoju pracownika;
- w przypadku laptopa, który znajdował się w Referacie Geodezji i Gospodarki Nieruchomościami, w systemie miał on status „używany", tymczasem laptop ten nie był wykorzystywany.

Kierownik Referatu Informatyki wyjaśnił, że *wprowadzenie serwera (…) oraz routera (…) do systemu ewidencji sprzętu i wyposażenia zostało przeoczone. Numery inwentaryzacyjne dla serwera (…) oraz routera (…) były nadane w systemie ewidencyjnym Środki Trwałe Info System, ale przeoczono ich nakleić. Po ujawnieniu tego faktu podczas kontroli naklejki z numerami inwentaryzacyjnymi zostały wydrukowane i naklejone na serwer (…) i router (…) znajdujące się w serwerowni. Serwer oraz router (…) zostały także wprowadzone do systemu ewidencji sprzętu i oprogramowania GLPI*. Odnośnie komputera wyjaśnił, że błędnie wprowadzono numer inwentaryzacyjny do systemu GLPI, a odnośnie laptopów wyjaśnił, że nie zaktualizowano wpisu w systemie GLPI z powodu wielokrotnego pobierania i zwracania sprzętu przez pracowników.

Zdaniem NIK, dla skutecznego zarządzania infrastrukturą informatyczną niezbędne jest utrzymywanie w Urzędzie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

W trakcie kontroli nieprawidłowości zostały usunięte, w związku z tym NIK nie formułuje wniosku pokontrolnego w tym zakresie.

(akta kontroli str. 865-898)

OCENA CZĄSTKOWA

W Urzędzie prawidłowo realizowano zadania dotyczące ustanowienia SZBI, w tym PBI. Z dokumentami tymi zapoznano pracowników Urzędu. W 2024 r. przeprowadzono również „Analizę zagrożeń i ryzyka przy przetwarzaniu danych osobowych" i opracowano „Rejestr ryzyk", a także dokumentację z zakresu ochrony danych osobowych. Zapewniono odpowiednie zasoby kadrowe dla zachowania bezpieczeństwa informacji.

Stwierdzone nieprawidłowości polegały na niewprowadzeniu do systemu służącego m.in. do inwentaryzacji sprzętu informatycznego dwóch urządzeń IT i nieustanowieniu polityk ciągłości działania, nieopracowaniu planów zapewnienia ciągłości działania oraz planów odtworzeniowych, a także niedokonaniu pełnej identyfikacji aktywów informacyjnych wymagających ochrony.

OBSZAR

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

Opis stanu faktycznego

1. W Urzędzie została zablokowana możliwość instalacji przez użytkowników systemów informatycznych nieautoryzowanego oprogramowania na komputerach służbowych i tabletach. Na służbowych smartfonach nie są przetwarzane dane Urzędu. Na podstawie oględzin przeprowadzonych na próbie 10 komputerów ustalono, że we wszystkich przypadkach użytkownicy nie mieli możliwości zainstalowania nieautoryzowanego oprogramowania, ze względu na brak uprawnień. Było to zgodne z § 19 ust. 2 pkt 4 rozporządzenia KRI.

(akta kontroli str. 826, 1000)

2. Analiza uprawnień do systemów informatycznych 15 pracowników Urzędu (w tym dziewięciu 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 uprawnień użytkownikom systemów informatycznych Urzędu było dokumentowane w postaci wniosku o przyznanie uprawnień w systemach informatycznych Urzędu oraz o wydanie upoważnienia do przetwarzania danych, co było zgodne z przyjętą w tym zakresie w Urzędzie „Procedurą zarządzania uprawnieniami do pracy w systemie informatycznym Urzędu" i „Procedurą monitoringu i kontroli dostępu do zasobów teleinformatycznych, prowadzenia logów systemowych"[11].

(akta kontroli str. 119-120, 126-127, 749-824)

3. W okresie objętym kontrolą zatrudnienie w Urzędzie zakończyło dziewięć osób, z tego trzy osoby przeszły na zasadzie porozumienia do Miejskiego Ośrodka Pomocy Społecznej w Józefowie. Ustalono, że w przypadku jednej osoby konto było nadal aktywne, w przypadku pozostałych ośmiu pracowników konta w systemach informatycznych zostały zablokowane, jednak nie można było stwierdzić, kiedy to nastąpiło i dlaczego dokonywano modyfikacji na tych kontach. Ustalono też, że we wszystkich badanych przypadkach nie zostały sporządzone formalne wnioski o zamknięcie kont/odebranie uprawnień przez przełożonego (dalszy opis w części *Stwierdzone nieprawidłowości*).

(akta kontroli str. 855-864)

4. W wyniku oględzin trzech systemów informatycznych zarządzanych przez Urząd[12] stwierdzono, że nie zostały spełnione wymagania dla haseł dostępu do tych systemów określone w pkt 4 IZSI (dalszy opis w części *Stwierdzone nieprawidłowości*).

(akta kontroli str. 827-835)

5. W wyniku oględzin dwóch stanowisk pracy, gdzie obywatele załatwiają sprawy z zakresu wydawania dowodów osobistych, stwierdzono że w przypadku jednego z tych stanowisk monitor był ustawiony w sposób umożliwiający klientom Urzędu wgląd do treści na nim wyświetlanych (dalszy opis w części *Stwierdzone nieprawidłowości*).

(akta kontroli str. 825)

[11] Stanowiącymi część IZSI.

[12] Systemy: SIDAS EZD, Sygnity oraz Groszek.

6. W Urzędzie zasady wykonywania pracy zdalnej zostały opisane w „Regulaminie pracy zdalnej w Urzędzie Miasta Józefowa" wprowadzonym zarządzeniem Nr 44/2020 Burmistrza Miasta Józefowa z dnia 11 maja 2020 r. w sprawie wprowadzenia Regulaminu pracy zdalnej w Urzędzie Miasta Józefowa. W ww. Regulaminie określono m.in. sposób uzyskiwania dostępu zdalnego do zasobów systemu teleinformatycznego Urzędu dla pracowników Urzędu, a także stosowane zabezpieczenia pracy zdalnej i pracy mobilnej. Było to zgodne z § 19 ust. 2 pkt 8 rozporządzenia KRI.

(akta kontroli str. 457-462)

7. Jak poinformował Burmistrz, 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. 7-11)

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

(akta kontroli str. 11, 836-837)

9. Analiza czterech umów (jednej serwisowej i trzech na dostawę sprzętu i oprogramowania) zawartych przez Miasto z podmiotami zewnętrznymi w okresie objętym kontrolą wykazała, że w dwóch z tych umów[13] nie umieszczono stosownych postanowień gwarantujących odpowiedni poziom bezpieczeństwa informacji (dalszy opis w części *Stwierdzone nieprawidłowości*)

(akta kontroli str. 904-976)

10. Przekazanie sprzętu komputerowego do serwisu oraz utylizacji w Urzędzie regulowała „Procedura wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych"[14] oraz „Procedura bezpiecznej utylizacji sprzętu komputerowego"[15]. Zgodnie z ww. procedurami 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. 128-129)

11. W Urzędzie kopie zapasowe danych są tworzone według zapisów zawartych w „Procedurze tworzenia i testowania kopii zapasowych", stanowiącej pkt 6 IZSI. Kopie zapasowe danych zweryfikowano w zakresie trzech systemów IT zarządzanych przez Urząd – systemu kadrowo-płacowego „Pakiet dla Administracji" – Info-System, EZD-SIDAS Madkom i do obsługi odpadów komunalnych – Gomig – Odpady Arisco. Ustalono, że do tworzenia kopii zapasowych w Urzędzie wykorzystuje się oprogramowanie Veeam Backup & Replication – program do tworzenia kopii zapasowych wirtualnych maszyn.

W badanych trzech systemach IT replika wirtualnych serwerów jest wykonywana co 24 godziny. Miejsca przechowywania danych zostały zabezpieczone w odpowiedni sposób. Ustalono jednak, że kopie zapasowe są przechowywane w miejscu wytwarzania danych, w jednym budynku w siedzibie Urzędu, w tej samej lokalizacji co baza produkcyjna (dalszy opis w części *Stwierdzone nieprawidłowości*).

W celu sprawdzenia poprawności wykonywania kopii zapasowej, dokonano testu odzyskiwania danych z kopii zapasowej wykonanej w dniu 2 i 30 kwietnia 2024 r.

[13] Umowa nr 398/2023 z 1 czerwca 2023 r. i nr 686/2023 z 12 grudnia 2023 r.
[14] Stanowiąca pkt 12 IZSI.
[15] Stanowiąca pkt 13 IZSI.

dotyczącej jednego modułu wybranego systemu. Po wgraniu danych z ww. kopii wyświetliły się prawidłowe dane z ww. modułu do miesiąca kwietnia 2024 r.

Zgodnie z pkt 6 IZSI pkt 4 testowanie kopii zabezpieczającej w Urzędzie wykonywane jest poprzez testowe uruchomienie zreplikowanych wirtualnych serwerów. Testy odtwarzania kluczowych baz danych oraz aplikacji odbywają się przy okazji przenoszenia tych zasobów pomiędzy wirtualnymi serwerami. Według wyjaśnień Kierownika Referatu Informatyki *testowanie kopii zapasowych nie było wykonywane regularnie, gdyż zakładano, że system działa, a w okresie objętym kontrolą zostało przeprowadzone jeden raz, jednak nie ma dokumentacji potwierdzającej dokonanie testu*. Kierownik odnośnie przyczyn braku testowania kopii zapasowych wyjaśnił, że *w celu regularnego testowania odtwarzania systemu z backup'ów istnieje potrzeba utworzenia w Urzędzie środowiska testowego, co przy obecnie posiadanych zasobach sprzętowych jest trudne do zrealizowania*.

(akta kontroli str. 123-124, 838-849)

12. Pracownicy Referatu Informatyki prowadzili na bieżąco monitorowanie zasobów informatycznych, w tym wydajności i pojemności nośników pamięci systemów Urzędu. Podejmowane były działania w zakresie zwiększenia zasobów informatycznych, w szczególności serwerowni w związku z rosnącymi potrzebami. W tym celu dokonywano zakupów sprzętu informatycznego, jak np. serwera, jak również wdrożono klaster Hyper-V. Monitorowanie odbywa się w oparciu o przyjętą w Urzędzie „Procedurę zarządzania pojemnością dysków" (pkt 10 IZSI). Monitorowanie przypisane jest do obowiązków informatyków.

W Urzędzie wykorzystywana jest macierz dyskowa. Macierz zapewnia przestrzeń dyskową dla wirtualnych maszyn, a dwa serwery połączone w klaster zapewniają ciągłość działania środowiska na wypadek awarii jednego z nich. Trzeci serwer dodatkowy ma za zadanie replikować wirtualne serwery na wypadek awarii całego środowiska (klastra).

W wyniku przeprowadzonych oględzin dwóch serwerów znajdujących się w Urzędzie ustalono, że na obu serwerach zajętość dysków wynosiła odpowiednio: 732,71 GB i 582,37 GB, a wolna przestrzeń dyskowa odpowiednio: 2 992,54 GB i 3 142,88 GB, co stanowi odpowiednio 80,33 i 84,37% wolnej przestrzeni na poszczególnych voluminach macierzy dyskowej.

(akta kontroli str. 127, 633-645, 850-854)

13. W Urzędzie kluczowym elementem infrastruktury jest serwerownia zlokalizowana w budynku Urzędu Miasta Józefowa. Posiadała ona odpowiednie zabezpieczenia techniczne. W rejestrze czynności przetwarzania danych znajduje się opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 RODO.

(akta kontroli str. 11, 836-837)

Stwierdzone nieprawidłowości

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

1. Stwierdzono, że według stanu na dzień 2 sierpnia 2024 r., jedna spośród dziewięciu osób, które w okresie od 1 stycznia 2023 r. do 30 lipca 2024 r. zakończyły zatrudnienie w Urzędzie, nadal posiadała aktywne konto w systemie informatycznym Groszek. Było to niezgodne z § 19 ust. 2 pkt 5 rozporządzenia KRI[16], 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

[16] Przed 23 maja 2024 r. odpowiednio z § 20 ust. 2 pkt 5 starego rozporządzenia KRI.

zadań osób zaangażowanych w proces przetwarzania informacji. Ponadto ustalono, że w przypadku ośmiu pracowników, których konta zostały zablokowane, nie można było stwierdzić, kiedy to zablokowanie nastąpiło i że dokonywano modyfikacji na tych kontach.

Kierownik Referatu Informatyki wyjaśnił, że *przeoczono wyłączenie tego konta w systemie dziedzinowym, ale konto domenowe tego użytkownika jest zablokowane i bez zalogowania się do domeny nie ma możliwości zalogowania się do systemu Groszek*. W kwestii braku możliwości ustalenia, kiedy zablokowano konta użytkownikom, Kierownik Referatu Informatyki wyjaśnił, że *nie ma wiedzy, kiedy wyłączono konta tych pracowników w domenie i dlaczego dokonywano modyfikacji na tych kontach. Prawdopodobnie te konta mogły być włączane w celu skopiowania plików z profili tych użytkowników*.

Ponadto ustalono, że we wszystkich badanych przypadkach nie zostały sporządzone formalne wnioski o zamknięcie kont/odebranie uprawnień przez przełożonego. Kierownik Referatu Informatyki wyjaśnił, że *informacje o odejściu pracownika z pracy i konieczności odebrania uprawnień i zamknięciu kont dostępowych powinny być przekazywane Administratorowi Systemu Informatycznemu zgodnie z pkt. 3 IZSI, tj. Procedury zarządzania uprawnieniami do pracy w systemie informatycznym Urzędu, będącej załącznikiem nr 6 do Polityki Ochrony Danych Osobowych. W celu usprawnienia procesu zamykania kont w systemach teleinformatycznych procedura ta zostanie uzupełniona o formalny wniosek o zamknięcie konta i odebrania uprawnień pracownikowi, któremu wygasa stosunek pracy*.

Burmistrz wyjaśnił, że *przeoczono konieczność uzupełnienia wprowadzonej Polityki Ochrony Informacji o formalny wniosek o zamknięcie konta i odebranie uprawnień pracownikowi, któremu wygasa stosunek pracy. Dotychczas taki wniosek był składany telefonicznie przez bezpośredniego przełożonego pracownika, któremu wygasał stosunek pracy. Polityka Bezpieczeństwa Informacji zostanie uzupełniona o wyżej wymieniony formalny wniosek*.

(akta kontroli str. 855-864, 977-982)

2. W wyniku oględzin trzech systemów[17] informatycznych zarządzanych przez Urząd stwierdzono, że nie zostały spełnione wymagania dla haseł dostępu użytkowników do tych systemów określone w pkt 4 IZSI pn. „Stosowane metody i środki uwierzytelniania w systemie oraz procedury związane z ich zarządzaniem i użytkowaniem". Procedura ta określała wymogi dotyczące złożoności hasła oraz okresów, po jakim hasło powinno być zmienione.

W przypadku systemu Sygnity długość hasła określono na osiem znaków, podczas gdy IZSI przewidywała 12 znaków, małe, duże litery oraz cyfry. Ponadto ustawiono parametry w ten sposób, że umożliwiały wpisanie dowolnego ciągu ośmiu liter lub cyfr, podczas gdy system umożliwiał ustawienie większej złożoności hasła.

Oględziny systemu Info-System Groszek wykazały, że parametry dotyczące haseł wymuszają zmianę hasła co 30 dni, a minimalna długość hasła to 8 znaków, hasło powinno także zawierać znaki inne niż litery. Administrator nie ustawił w systemie parametru „Hasło powinno zawierać znak specjalny oraz duże i małe litery", a także nie ustawił minimalnej długości hasła na 12 znaków, co wymagane było IZSI. Oględziny wykazały też, że system umożliwia zmianę hasła po wpisaniu dowolnego ciągu ośmiu liter lub liczb. Powyższe było również niezgodne z § 19 ust. 2 pkt 7 rozporządzenia KRI.

Kierownik Referatu Informatyki wyjaśnił, że *żeby się dostać do ww. systemów, użytkownik i tak musi się zalogować do domeny Urzędu*. Ponadto wyjaśnił, że

[17] Systemy: SIDAS EZD, Sygnity oraz Groszek.

możliwość zmiany ustawień zwiększających poziom złożoności haseł dostępowych do programu została przeoczona.

W trakcie kontroli NIK stwierdzono, że powyższa nieprawidłowość została usunięta w przypadku ww. systemów, dlatego NIK nie formułuje wniosku pokontrolnego w tym zakresie.

(akta kontroli str. 120-121, 827-835)

3. W wyniku oględzin dwóch stanowisk pracy, gdzie obywatele załatwiają sprawy z zakresu wydawania dowodów osobistych, stwierdzono że w przypadku jednego stanowiska pracy monitor był ustawiony w sposób umożliwiający klientom Urzędu wgląd do treści na nich wyświetlanych, w tym do danych osobowych Było to niezgodne z § 19 ust. 2 pkt 7 rozporządzenia KRI. Kierownik Referatu Ewidencji Ludności i Urzędu Stanu Cywilnego wyjaśniła, że *lokalizacja stanowiska pracy wymusza przesuwanie monitora. W chwili uruchamiania i korzystania z monitora pracownik ustawia go pod właściwym kątem. Z chwilą zakończenia pracy przy monitorze jest on wygaszany. Specyfika zadań na stanowisku pracy i ich skrupulatność nie pozwala na korzystanie z dwóch monitorów jednocześnie*.

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

(akta kontroli str. 825)

4. W dwóch spośród czterech badanych umów nie zawarto zapisów mówiących o zobowiązaniu wykonawcy do zachowania tajemnicy informacji, do jakich może mieć dostęp w związku z realizowaniem umowy, co było niezgodne z § 20 ust. 2 pkt 10 starego rozporządzenia KRI [18].

Burmistrz wyjaśnił, że *umowy nr 398/2023 z 1 czerwca 2023 r. i nr 686/2023 z 12 grudnia 2023 r. dotyczą dostaw sprzętu komputerowego i nie są umowami serwisowymi. Zgodnie z zapisem § 19 ust. 2 pkt 10 KRI wymóg zawarcia w umowach zapisów gwarantujących odpowiedni poziom bezpieczeństwa dotyczy umów serwisowych.*

Zdaniem NIK, brak w umowach ww. zapisów świadczy o niezabezpieczeniu interesów Urzędu na wypadek niezachowania poufności informacji uzyskanych w związku z realizacją umowy. NIK wskazuje, że w ramach umowy zakupu świadczony jest również serwis gwarancyjny, w ramach którego wykonawca jest zobowiązany usuwać błędy oprogramowania, dlatego zamawiający powinien zagwarantować w umowie możliwość reagowania i podejmowania określonych czynności w takim przypadku wobec wykonawcy.

(akta kontroli str. 904-982)

5. Kopie zapasowe danych były przechowywane w miejscu wytwarzania danych w siedzibie Urzędu, co stanowi naruszenie § 19 ust. 2 pkt 12 lit. b) KRI.

Odnośnie przyczyn przechowywania danych w miejscu ich wytwarzania, Kierownik Referatu Informatyki wyjaśnił, że *obecne warunki lokalowe Urzędu pozwalają na takie usytuowanie środowiska produkcyjnego oraz kopii zapasowych. Niemniej jednak planowany jest zakup macierzy dyskowej w ramach projektu grantowego „Cyberbezpieczny Samorządu", która ma być przeznaczona do przechowywania dodatkowych kopii zabezpieczających poza głównym budynkiem Urzędu.*

Burmistrz wyjaśnił, że *z uwagi na to, że Urząd Miasta Józefowa posiada jedną serwerownię, brak jest możliwości wyniesienia urządzeń, na których przechowuje się kopie zapasowe z miejsca lokalizacji systemu produkcyjnego. W ramach programu*

[18] Od 23 maja 2024 r. wymóg taki określa § 19 ust. 2 pkt 10 rozporządzenia KRI.

grantowego „Cyberbezpieczny Samorząd" zaplanowano zakup dodatkowej macierzy dyskowej, na której będą przechowywane backup'y danych poza serwerownią Urzędu.

NIK wskazuje, że kopie zapasowe nie mogą być przechowywane w miejscu wytwarzania danych, ponieważ w przypadku awarii (zalania, pożaru) zniszczeniu ulegną zarówno dane źródłowe, jak i ich kopia.

(akta kontroli str. 836-849, 899-903, 977-982)

OCENA CZĄSTKOWA

W Urzędzie, w okresie objętym kontrolą, podejmowano działania w zakresie zapewnienia bezpieczeństwa informacji, m.in. poprzez zabezpieczenie serwerowni Urzędu przed nieuprawnionym dostępem, nadawanie uprawnień pracownikom adekwatnie do realizowanych przez nich zadań, uniemożliwienie zainstalowania przez pracowników nieautoryzowanego oprogramowania, zarządzanie pojemnością wykorzystywanych systemów informatycznych w sposób zapewniający właściwą wydajność systemów. Wprowadzono również procedury dotyczące przekazywania sprzętu komputerowego podmiotom zewnętrznym, tworzenia i testowania kopii zapasowych oraz zasady pracy zdalnej.

Stwierdzone w tym obszarze nieprawidłowości dotyczyły głównie niezapewnienia przechowywania kopii zapasowych badanych systemów informatycznych poza miejscem wytwarzania danych, niespełnienia przyjętych wymagań dla haseł dostępu w dwóch systemach informatycznych, a także braku w dwóch badanych umowach serwisowych zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

OBSZAR

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

1. W Urzędzie w okresie objętym kontrolą została przeprowadzona „Analiza zagrożeń i ryzyka przy przetwarzaniu danych osobowych", obejmująca analizę ryzyka utraty integralności, poufności lub dostępności informacji, co było zgodne z § 20 ust. 2 pkt 3 rozporządzenia KRI.

(akta kontroli str. 223-426)

2. W Urzędzie sposób postępowania w przypadku wystąpienia incydentu naruszenia ochrony danych osobowych został opisany w przyjętej w ramach Polityki ochrony danych osobowych „Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Miasta Józefowa". Procedura uwzględniała postanowienia art. 33 i 34 RODO.

Burmistrz poinformował, że *w dniu 31 lipca 2024 roku zgłoszono do Urzędu Ochrony Danych Osobowych naruszenie danych polegające na możliwym ujawnieniu danych osobowych tj. imienia, nazwiska oraz numeru PESEL osób będących obecnymi lub byłymi pracownikami Urzędu wykazanymi w protokole pokontrolnym ZUS. Podjęto skuteczne działania naprawcze w tym zakresie*.

(akta kontroli str. 60-76)

3. W okresie od 1 stycznia 2023 r. do 6 września 2024 r. odbyły się szkolenia obejmujące większość pracowników przeprowadzone przez IOD w zakresie ochrony danych z elementami cyberbezpieczeństwa. W okresie objętym kontrolą w Urzędzie nie opracowano harmonogramu szkoleń dla pracowników związanych z przetwarzaniem informacji. Burmistrz poinformował, że *harmonogram szkoleń nie został opracowany ze względu na trudności dopasowania takiego harmonogramu do wszystkich komórek organizacyjnych Urzędu*.

Zdaniem NIK, istotne jest opracowanie harmonogramu szkoleń na dany rok z zakresu bezpieczeństwa informacji, szczególnie, że we wniosku o grant w projekcie

Cyberbezpieczny Samorząd wskazano, że pracownicy nie są objęci programem szkoleniowym w zakresie cyberbezpieczeństwa i że planowane jest zlecenie opracowania kompleksowego programu szkoleniowego oraz zakup platformy szkoleniowej w celu zapewnienia regularnego podnoszenia poziomu świadomości cyberbezpieczeństwa dla pracowników Urzędu oraz dla kadry zarządzającej i służb IT w zakresie planowanych do zastosowania środków bezpieczeństwa w ramach projektu grantowego.

(akta kontroli str. 689-748, 977-982)

4. W Urzędzie w okresie objętym kontrolą przeprowadzono „Audyt bezpieczeństwa informacji w Urzędzie Miasta Józefowa" w zakresie zasad odnoszących się do bezpieczeństwa informacji i danych oraz efektywności wprowadzonych rozwiązań w zakresie zarządzania uprawnieniami pracowników i zawierania odpowiednich umów serwisowych. W dokumencie sformułowano jedno zalecenie dotyczące podjęcia działań zmierzających do wdrożenia na poziomie Urzędu systemowego rozwiązania dotyczącego zarządzania uprawnieniami do pracy w systemach informatycznych wykorzystywanych w Urzędzie. Opracowano również „Analizę zagrożeń i ryzyka przy przetwarzaniu danych osobowych", gdzie sformułowano zalecenia odnośnie zarządzania bezpieczeństwem informacji.

(akta kontroli str. 598-609)

Stwierdzone nieprawidłowości

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

OCENA CZĄSTKOWA

W Urzędzie, w okresie objętym kontrolą, podjęto działania w celu zapobiegania incydentom bezpieczeństwa informacji, tj. zorganizowano szkolenia pracowników, przeprowadzono audyt z zakresu bezpieczeństwa informacji, a także wprowadzono procedurę w zakresie zgłaszania incydentów naruszenia bezpieczeństwa informacji.

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 polityk ciągłości działania oraz opracowanie i wdrożenie planów zapewnienia ciągłości działania i planów odtworzeniowych w zakresie systemów informatycznych.
3. Zapewnienie niezwłocznego i trwałego odbierania byłym pracownikom Urzędu uprawnień do systemów informatycznych.
4. Uzupełnienie procedury dotyczącej zarządzania uprawnieniami do pracy w systemie informatycznym Urzędu o formalny wniosek w zakresie zamknięcia konta i odebranie uprawnień pracownikowi, któremu wygasa stosunek pracy.
5. Zawieranie w umowach o świadczenie usług informatycznych postanowień gwarantujących odpowiedni poziom bezpieczeństwa informacji.
6. Przechowywanie kopii zapasowych poza miejscem ich wytwarzania.

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, 19 września 2024 r.

Najwyższa Izba Kontroli
Departament Administracji Publicznej
Bogdan Skwarka
Dyrektor

/podpisano elektronicznie/

Kontroler
Tomasz Kwitowski
Doradca techniczny

/podpisano elektronicznie/