NAJWYŻSZA IZBA KONTROLI

DELEGATURA WE WROCŁAWIU

LWR.410.13.2.2024

Pan
Tomasz Kiliński
Burmistrz Miasta Nowa Ruda
Urząd Miejski w Nowej Rudzie
Rynek 1
57-400 Nowa Ruda

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 Nowej Rudzie, Rynek 1, 57-400 Nowa Ruda[1].
Kierownik jednostki kontrolowanej	Tomasz Kiliński, Burmistrz Miasta Nowa Ruda od 21 października 2018 r.[2].
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
KontrolerKontroler	Waldemar Zimoch, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LWR/84/2024 z dnia 31 maja 2024 r.

(akta kontroli: str. 1-3)

[1] Dalej: Urząd.
[2] Dalej: Burmistrz.
[3] Czynności kontrolne zakończono 29 sierpnia 2024 r.
[4] Dz. U. z 2022 r. poz. 623; dalej: ustawa o NIK.

II. Ocena ogólna[5] kontrolowanej działalności

OCENA OGÓLNA

Urząd nie zawsze prawidłowo i rzetelnie realizował zadania związane z zapewnieniem bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych.

Podstawą oceny ogólnej były oceny cząstkowe, dotyczące obszarów, które zostały poddane kontroli. W szczególności w badanym okresie w Urzędzie nie było w pełni wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji[6] w rozumieniu § 19 ust. 1 w związku 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[7]. Urząd nie posiadał również jednolitej dokumentacji w zakresie polityki bezpieczeństwa informacji. Jednocześnie w tym okresie stosowano dokumentację składającą się na Politykę Ochrony Danych Osobowych w Urzędzie[8], uwzględniającą 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 (ogólne rozporządzenie o ochronie danych)[9].

W okresie objętym kontrolą prowadzono analizę ryzyka w związku z potrzebą zachowania ciągłości działania systemów informatycznych. Zidentyfikowane zostały kluczowe elementy infrastruktury i usługi IT, lecz nie nadano odpowiednich procentowych ważności kluczowym elementom, a także nie opisano planów naprawczych w przypadku wystąpienia awarii. Urząd zapewnił właściwe rozwiązania zapobiegające możliwości instalacji nieautoryzowanego oprogramowania na urządzeniach służbowych oraz uniemożliwiające dostęp do danych na urządzeniach mobilnych. Jednocześnie wszystkie zweryfikowane umowy serwisowe posiadały zapisy gwarantujące odpowiedni poziom bezpieczeństwa. W Urzędzie opracowano plany ciągłości działania i plany odtworzeniowe, należy jednak podkreślić, że powinny one zawierać bardziej szczegółowe zapisy i wskazane byłoby uszczegółowienie dokumentacji w tym zakresie.

W trakcie kontroli stwierdzono szereg nieprawidłowości polegających na: **[1]** braku nadania zbiorom danych odpowiedniej ważności w procesie identyfikowania danych podlegających zabezpieczeniu, **[2]** nieprzeprowadzeniu przeglądu stanu bezpieczeństwa danych osobowych w terminie wymaganym regulacjami wewnętrznymi, **[3]** niezapoznaniu się większości pracowników z postanowieniami Regulaminu użytkownika komputerów przenośnych, **[4]** nieprzeprowadzaniu testów i treningów związanych z planami zapewnienia ciągłości działania, **[5]** niedokonywaniu przeglądu i aktualizacji dokumentacji zawierającej elementy polityki bezpieczeństwa informacji, **[6]** nieposiadaniu pełnych informacji o zasobach informatycznych Urzędu, **[7]** niezablokowaniu kont w systemach IT byłym pracownikom Urzędu, **[8]** ustaleniu wymogów dla haseł w systemach IT niezgodnie z wymogami stosowanej polityki haseł, **[9]** użytkowaniu pomieszczenia serwerowni w sposób niezapewniający odpowiedniej ochrony, **[10]** nieprawidłowym przechowywaniu nośników danych z kopiami zapasowymi, **[11]** nierealizowaniu szkoleń z zakresu bezpieczeństwa informacji, oraz **[12]** wykonywaniu okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji z naruszeniem zasad niezależności i obiektywności.

---

[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] Dalej: PODO.
[9] Dz. Urz. UE L 119/1 z 4 maja 2016 r., str. 1, ze zm.; dalej: RODO.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[10] kontrolowanej działalności

OBSZAR

1. Organizacja bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych

Opis stanu faktycznego

1.1. Urząd posiadał łącznie 15 systemów (rejestrów, programów), za pomocą których przetwarzał zbiory różnych danych. W Urzędzie zidentyfikowano zbiory tych danych, jednak nie przypisano im odpowiedniego poziomu ochrony, zgodnie z ich wagą, co zostało opisane w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli: str. 4-14)

1.2. W Urzędzie nie było w pełni wdrożonego SZBI w rozumieniu § 19 ust. 1 rozporządzenia KRI, co opisano w sekcji *Stwierdzone nieprawidłowości*.

Urząd nie posiadał również jednolitej dokumentacji odnośnie polityki bezpieczeństwa informacji, a jej elementy znajdowały się w innych dokumentach, tj.:

- zarządzeniem nr 124/18 Burmistrz Miasta Nowa Ruda wprowadził 8 czerwca 2018 r. Regulamin Ochrony Danych Osobowych w Urzędzie Miejskim w Nowej Rudzie[11]. W Regulaminie tym zawarto m.in.: [1] zasady bezpiecznego użytkowania sprzętu IT, dysków, programów, [2] procedury rozpoczęcia, zawieszenia oraz zakończenia pracy w systemach IT, [3] politykę haseł, [4] zasady wynoszenia nośników z danymi poza Urząd, [5] zasady korzystania z Internetu. Jednocześnie Załącznikiem nr 1 do tego dokumentu był Regulamin użytkowników komputerów przenośnych;
- postanowieniem nr 15/18 Burmistrza Miasta Nowa Ruda z 31 sierpnia 2018 r. wprowadzono w Urzędzie Instrukcję zarządzania RODO oraz Instrukcję zarządzania Systemami Informatycznymi. Elementami Instrukcji zarządzania RODO były m.in. procedury: [1] metod i środków uwierzytelniających, [2] napraw w serwisach zewnętrznych, [3] niszczenia danych na nośnikach elektronicznych i papierowych, [4] postępowania z nośnikami i sprzętem poza Urzędem, [5] nadawania uprawnień do przetwarzania danych osobowych. Ponadto dokument ten zawierał plan ciągłości działania oraz zasady tworzenia kopii zapasowych.

Koordynację i kontrolę realizacji zadań, w ramach Regulaminu, a także wskazanego wyżej postanowienia, powierzono Inspektorowi Ochrony Danych Osobowych[12]. W wyżej wymienionych dokumentach nie wskazano wprost ich właściciela odpowiadającego za ich opracowanie, przegląd i modyfikację. Jedynie ich wykonanie powierzono Koordynatorowi Zespołu ds. Informatyki.

Ponadto w ramach bezpieczeństwa fizycznego postanowieniem nr 21/21 z 31 grudnia 2021 r. Burmistrz wprowadził Politykę kluczy w Urzędzie, a nadzór nad jego wykonaniem również powierzył IOD.

Badanie 28 teczek osobowych pracowników Urzędu wykazało, że w 25 przypadkach brak było pisemnego oświadczenia o treści: „*Zapoznałem się z treścią Regulaminu użytkownika komputerów przenośnych i zobowiązuję się do przestrzegania zasad w nim zawartych*", co zostało opisane w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli: str. 15-60)

[10] 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.
[11] Dalej: Regulamin.
[12] Dalej: IOD.

1.3. W dniu 31 grudnia 2021 r., zarządzeniem nr 246/21, Burmistrz wprowadził PODO. Nadzór nad wykonaniem tego zarządzenia powierzono IOD, a realizację zapisów – wszystkim pracownikom Urzędu, stosownie do wykonywanych przez nich zadań. Dokument ten zawierał m.in.: ocenę skutków (analizę ryzyka), opis operacji przetwarzania, instrukcję postępowania z incydentami oraz zapisy na temat szkoleń, upoważnień i przeprowadzania audytu. Pracowników zapoznano z postanowieniami PODO.

(akta kontroli: str. 61-80)

1.4. W okresie objętym kontrolą w Urzędzie przeprowadzono analizę ryzyka związanego z potrzebą zachowania ciągłości działania systemów informatycznych. W ramach przeprowadzonej 27 grudnia 2023 r. - *Analizy Ryzyka Ogólnego i Oceny Skutków dla Przetwarzania Danych* (DPIA), wymieniono m.in. aspekty naruszenia bezpieczeństwa informacji takie jak: kradzież nośników lub dokumentów, podsłuch, sfałszowane oprogramowanie, czy też awarie techniczne. W dokumencie tym wymieniono również listę zagrożeń oraz określono prawdopodobieństwo i skutki zajścia danego zagrożenia. W ramach obowiązujących regulacji wewnętrznych, nie przeprowadzono jednak ponownego przeglądu stanu bezpieczeństwa danych osobowych przetwarzanych w Urzędzie, który należało wykonać nie dłużej niż po sześciu miesiącach, co zostało opisane w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli: str. 81-97)

1.5. Urząd w kontrolowanym okresie nie wprowadził dokumentu o nazwie polityka ciągłości działania. Należy jednak nadmienić, że w Instrukcji zarządzania RODO, stanowiącej załącznik do postanowienia nr 15/18 Burmistrza Miasta Nowa Ruda z dnia 31 sierpnia 2018 r. znalazły się zapisy dotyczące odtworzenia systemów informatycznych po awarii krytycznej oraz na wypadek braku zasilania w sieci komputerowej, a także utraty dostępu do sieci Internet.

(akta kontroli: str. 54-55)

1.6. W Instrukcji zarządzania RODO w ograniczonym zakresie zamieszczono elementy planu zapewnienia ciągłości działania i planu odtworzeniowego. W Procedurze II tej instrukcji, w części - *Zasady postępowania przy odtworzeniu systemu informatycznego w lokalizacji podstawowej* - określono bowiem jaka osoba zajmuje się urządzeniami podstawowymi, jaki jest przewidywany czas uruchomienia, a przypadku braku osoby upoważnionej kto ją zastępuje.

Należy podkreślić, że plan zapewnienia ciągłość działania oraz plany odtworzeniowe powinny zawierać bardziej szczegółowe wytyczne rozbite na poszczególne elementy, tj. zasilanie i topologia sieci, klastry i macierze dyskowe, systemy kopii zapasowych, czy też systemy serwerów wirtualnych, a także opis działania dotyczący urządzeń brzegowych. Zatem wskazane byłoby uszczegółowienie dokumentacji w tym zakresie.

(akta kontroli: str. 59, 295-297)

1.7. W Urzędzie nie przeprowadzano testów i treningów związanych z planami zapewnienia ciągłości działania, co opisano w sekcji *Stwierdzone nieprawidłowości*

(akta kontroli: str.302-303)

1.8. W Urzędzie nie dokonywano przeglądu i aktualizacji dokumentacji, która zawierała w sobie elementy związane z polityką bezpieczeństwa informacji, co opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli: str. 15-60)

1.9. W Urzędzie zostali wyznaczeni pracownicy odpowiedzialni za bezpieczeństwo informacji oraz zapewnienie ciągłości działania. Czynnościami tymi zajmowali się IOD oraz Koordynator w Zespole ds. Informatyki. Przypisano im m.in. takie obowiązki jak:

- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie wykonania tych zaleceń;
- pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych;
- nadzór nad sprawnym funkcjonowaniem systemu informatycznego w Urzędzie;
- administracja i nadzór nad bezpieczeństwem sieci lokalnej;
- nadzór nad bezpieczeństwem sieci i serwerów;
- archiwizowanie systemów operacyjnych.

(akta kontroli: str. 126-139)

1.10. W Urzędzie wyznaczono osobę na stanowisko IOD zgodnie z art. 37 ust. 1 i 5 RODO oraz art. 8 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[13]. Osoba wybrana na to stanowisko posiadała odpowiednie wykształcenie i kwalifikacje, a jej zakres obowiązków obejmował m.in. takie zadania jak:

- nadzór nad realizacją przepisów RODO;
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie wykonania tych zaleceń;
- współpraca z organem nadzorczym;
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO oraz, w stosownych przypadkach, prowadzenie konsultacji we wszelkich innych sprawach.

(akta kontroli: str. 126-139)

1.11. W okresie objętym kontrolą IOD pełniła swoją funkcję w Urzędzie w sposób niezależny, zgodnie z wymogami określonymi w art. 38 ust. 3 RODO.

IOD wykonywała zadania, które nie podlegały instrukcjom oraz naciskom dotyczącym wykonywania obowiązków związanych z ochroną danych osobowych, co pozwalało na obiektywne i bezstronne wykonywanie tych obowiązków. Jednocześnie IOD oświadczyła, że nie jest zaangażowana w inne działania, które mogłyby prowadzić do konfliktu interesów, a wykonywane przez nią funkcje nie są powiązane z działaniami, które mogłyby wpływać na wykonywane obowiązki. Wyjaśniła również, że posiada odpowiednie zasoby oraz dostęp do informacji niezbędnych do pełnienia powierzonej roli, w tym wsparcie zarządu i dostęp do niezbędnych narzędzi, aby skutecznie realizować zadania związane z ochroną danych osobowych.

(akta kontroli: str.140)

1.12. Urząd zgłosił 2 marca 2021 r. dwie osoby odpowiedzialne za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, zgodnie z art. 21 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[14]. Jednocześnie Urząd nie posiadał jednoznacznych dokumentów stwierdzających fakt wyznaczenia ww. osób i tym samym dotrzymania 14 dniowego terminu zgłoszenia, wynikającego z art. 22 ust. 1 pkt 5 ustawy o ksc.

[13] Dz. U. z 2019 r. poz. 1781.
[14] Dz. U. z 2024 r. poz. 1077, ze zm.; dalej: ustawa o ksc.

Główny specjalista – informatyk, wyjaśnił, że ww. osoby zostały wybrane poprzez telefoniczne polecenie służbowe, a zgłoszenia dokonano niezwłocznie do CSIRT NASK[15].

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 Burmistrza.

(akta kontroli: str. 141-145, 457)

1.13. Urząd nie posiadał formalnej i jednolitej polityki bezpieczeństwa informacji. Wprowadzono Regulamin, w którym zamieszczono bardzo okrojone zasady lub procedury wewnętrzne obejmujące swoim zakresem elementy z obszaru polityki bezpieczeństwa. W dokumencie tym zawarto m.in.:

- zasady bezpiecznego użytkowania sprzętu IT, dysków, programów.
- procedurę rozpoczęcia, zawieszenia oraz zakończenia pracy w systemach IT;
- politykę haseł;
- zasady wynoszenia nośników z danymi poza Urząd;
- zasady korzystania z Internetu.

Dokument ten nie zawierał wymogu sporządzenia innych odrębnych dokumentów wykonawczych, stanowiących uszczegółowione procedury, polityki czy instrukcji.

(akta kontroli: str. 15-97)

1.14. Do utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację, w Urzędzie wykorzystywano specjalistyczne oprogramowanie. Funkcjonowało ono już od lutego 2019 r., a pomimo tego zostało wdrożone na poziomie 70%, co opisano w sekcji *Stwierdzone nieprawidłowości*.

Użytkowane oprogramowanie pozwalało na automatyczne wykrywanie sieci i monitorowanie m.in. komputerów stacjonarnych i przenośnych oraz zainstalowanych na nich aplikacji. Dane zgromadzone w tym programie dotyczyły użytkowników sprzętu, wszystkich elementów sprzętu komputerowego, oprogramowania oraz części drukarek i urządzeń peryferyjnych. Każdy zinwentaryzowany element posiadał odrębny rekord w tej bazie i był opisany za pomocą atrybutów. W ramach zakupu oprogramowania uzyskano 100 licencji. Na dzień przeprowadzenia czynności kontrolnych system pozwalał przeprowadzić inwentaryzację komputerów (stacjonarnych i przenośnych) na poziomie 98,0% zasobów (98 z 100 licencji).

W toku przeprowadzonych oględzin na próbie 10 komputerów, w tym pięciu laptopów i pięciu komputerów stacjonarnych oraz jednej drukarki, stwierdzono, że system inwentaryzacyjny wskazywał aktualne dane m.in. w zakresie zainstalowanego oprogramowania, sprzętu, konfiguracji systemu oraz osoby odpowiedzialnej/użytkownika. W przypadku gdy urządzenie nie było aktualnie podłączone do sieci, program informował o ostatniej zarejestrowanej konfiguracji oraz wskazywał jak długo urządzenie nie działało, nie było podłączone do sieci lokalnej urzędu.

(akta kontroli: str. 260-294, 400-414 ,430)

1.15. Urząd wziął udział w konkursie grantowym w ramach Projektu *Cyberbezpieczny Samorząd* o numerze FERC.02.02-CS.01-001/23, Fundusze Europejskie na Rozwój

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

Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe. Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa. Wniosek o dofinansowanie projektu *Poprawa cyberbezpieczeństwa w Gminie Miejskiej Nowa Ruda*[16] został złożony w dniu 1 grudnia 2023 r. na kwotę 850 000,00 zł[17]. W dniu 4 stycznia 2024 r. wnioskodawca otrzymał informację, że wniosek uzyskał pozytywną ocenę formalno-merytoryczną, a w dniu 15 kwietnia 2024 r. podpisał umowę.

W ramach uzyskanego dofinansowania Projektu zaplanowano między innymi:

- przeprowadzenie audytu bezpieczeństwa informacji;
- sporządzenie Polityki Bezpieczeństwa Informacji oraz SZBI;
- przeprowadzenie szkolenia na temat cyberbezpieczeństwa i przetwarzania informacji celem podniesienia świadomości oraz zwiększenia wiedzy pracowników w przedmiotowym temacie;
- zakupienie licencji na program antywirusowy;
- przedłużenie wsparcia i aktualizację urządzeń sieciowych;
- przedłużenie wsparcia oraz aktualizację systemu do inwentaryzacji;
- przedłużenie wsparcia oraz aktualizację programu do wykonywania kopii baz danych serwerów;
- zakup instalacji i uruchomienie serwerowni w innej lokalizacji niż obecna, co pozwoli na rozproszenie baz danych oraz wymianę sprzętu, który pracuje już bez wsparcia i aktualizacji producentów (serwerów, macierzy, przełączników, UPS-ów[18]).

Główny specjalista – informatyk wyjaśnił, że wszystkie zakupione elementy w ramach otrzymanych funduszy w znaczącym stopniu poprawią cyberbezpieczeństwo w Urzędzie na kolejne lata, gdyż w obecnej sytuacji budżet nie pozwalał na wydatki w ramach wyżej wymienionych zagadnień w tak obszernym zakresie.

Jako element pomiaru poprawy cyberbezpieczeństwa w wyniku realizacji Projektu przewidziano ewaluację według kryteriów „Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego". Przed rozpoczęciem Projektu wypełniono ankietę, w której określono stan obecny w zakresie ośmiu obszarów cyberbezpieczeństwa[19] oraz planowane zmiany w związku z realizacją Projektu.

(akta kontroli: str. 146-195, 459)

Stwierdzone nieprawidłowości

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

1. W Urzędzie, w procesie identyfikowania zbiorów danych podlegających zabezpieczeniu, nie nadano zbiorom danych odpowiedniej ważności, a tym samym poziomu ochrony, co zdaniem NIK było działaniem nierzetelnym.

Główny specjalista – informatyk wyjaśnił, że Urząd nie dokonał „oflagowania posiadanych baz", ponieważ ewidencja ludności (najważniejsza dla Urzędu baza) była częścią oprogramowania, w którego skład wchodziło 14 modułów zasilanych danymi z tejże bazy.

NIK wskazuje, że nie był to jedyny zbiór danych w posiadaniu Urzędu, należało więc przypisać wszystkim zbiorom danych, podlegającym zabezpieczeniu, odpowiedni poziom ochrony, zgodny z ich wagą. Informacje takie klasyfikuje się

[16] Dalej: Projekt.
[17] Dofinansowanie 100%, brak zaangażowania własnych środków Urzędu.
[18] Zasilacz awaryjny, zasilacz bezprzerwowy, zasilacz UPS (ang. uninterruptible power supply – zasilacz bezprzerwowy).
[19] Były to: [1] Zarządzanie, [2] System Zarządzania Bezpieczeństwem Informacji, [3] Ochrona, [4] Zdarzenia i Monitoring, [5] Reagowanie, [6] Odtwarzanie, [7] Infrastruktura i [8] Telekomunikacja.

bowiem z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację.

(akta kontroli: str. 4-14, 430)

2. W Urzędzie nie było w pełni wdrożonego SZBI, co stanowiło naruszenie § 19 ust. 1 rozporządzenia KRI.

Główny specjalista – informatyk wyjaśnił, że braki tej dokumentacji spowodowane są niewystarczającymi środkami na jej stworzenie. Dodał przy tym, że zostanie ona stworzona w ramach Projektu, który będzie realizował Urząd.

(akta kontroli: str. 15-60, 415)

3. W 25 teczkach osobowych (na 28 badanych ogółem) brak było oświadczenia o treści: *Zapoznałem się z treścią Regulaminu użytkownika komputerów przenośnych i zobowiązuję się do przestrzegania zasad w nim zawartych*, mimo takiego obowiązku, wynikającego z zarządzenia nr 124/18 Burmistrza Miasta Nowa Ruda z dnia 8 czerwca 2018 r., wprowadzającego ten Regulamin.

IOD wyjaśniła, że wszyscy pracownicy pracujący na komputerach przenośnych zapoznają się z tym regulaminem, niestety nie wszyscy złożyli pisemne oświadczenie wynikające z zapoznaniem się z tym dokumentem, co było niedopatrzeniem.

(akta kontroli: str. 15-28, 298)

4. Urząd nie przeprowadził przeglądu stanu bezpieczeństwa danych osobowych przetwarzanych w Urzędzie, w okresie sześciu miesięcy od wykonanej 27 grudnia 2023 r. *Analizy Ryzyka Ogólnego i Oceny Skutków dla Przetwarzania Danych* (DPIA). Zawarta w tym dokumencie deklaracja określała jasno, iż Administrator w celu utrzymania założonego poziomu bezpieczeństwa danych osobowych przetwarzanych w organizacji powinien przeprowadzać jego przegląd nie rzadziej niż raz na sześć miesięcy.

IOD wyjaśniła, że zaistniała sytuacja nastąpiła przez przeoczenie, a Urząd uznał, że efektywniejsze będzie przeprowadzenie tej analizy przez podmiot zewnętrzny w ramach Projektu, który ma być realizowany.

(akta kontroli: str. 81-97)

5. Urząd nie przeprowadzał testów i treningów związanych z planami zapewnienia ciągłości działania, co było działaniem nierzetelnym.

Główny specjalista – informatyk wyjaśnił, że nie ma dokumentacji takich testów i wskazał, że po ujawnieniu tej nieprawidłowości rozpoczęto elektroniczne dokumentowanie przeprowadzanych testów.

NIK podkreśla, że norma ISO 22301[20] wskazuje, że w przypadku planu zapewnienia ciągłości działania oraz planów odtworzeniowych istotne jest ich cykliczne testowanie w celu uzyskania potwierdzenia, że w sytuacji wystąpienia incydentu zadziałają one prawidłowo. Nie jest co prawda możliwe zasymulowanie w pełni zaistniałej katastrofy, np. zalania, pożaru budynku. Dlatego też plany te powinny być testowane jedynie w możliwym zakresie. Istotne przy tym jest zidentyfikowanie słabych punktów tych planów w trakcie prowadzonych ćwiczeń i ich ciągłe doskonalenie, a przy tym dokumentowanie tych działań.

(akta kontroli: str. 81-97, 302-303)

6. W Urzędzie nie dokonywano przeglądu i aktualizacji dokumentacji, która zawierała w sobie elementy związane z polityką bezpieczeństwa informacji, co było niezgodne z § 19 ust. 2 pkt 1 rozporządzenia KRI.

[20] Norma ISO 22301 Bezpieczeństwo i odporność. Systemy zarządzania ciągłością działania. Wymagania.

IOD przyznała, że nie dokonano przeglądów dokumentów przez niedopatrzenie. Zadeklarowała także, że w związku z powyższym podejmie wszelkie działania mające na celu usunięcie nieprawidłowości; zostanie przeprowadzony odpowiedni przegląd i będzie wykonana odpowiednia dokumentacja.

(akta kontroli: str. 15-97, 424)

7. Urząd nie posiadał pełnych informacji o zasobach informatycznych obejmujących ich rodzaj i konfigurację, co naruszało § 19 ust. 2 pkt 2 rozporządzenia KRI. Mimo posiadania od lutego 2019 r. właściwego do tego celu oprogramowania, wdrożono go w Urzędzie tylko na poziomie 70%. Do systemu nie wprowadzono bowiem w całości posiadanego sprzętu, a braki dotyczyły m.in. serwerów czy też drukarek.

Główny specjalista – informatyk wyjaśnił, że uzupełnienie danych wymaga dużego nakładu pracy, aby być na bieżąco z wprowadzonymi zmianami i nowymi możliwościami dedykowanej aplikacji.

Powyższa nieprawidłowość została usunięta do dnia zakończenia kontroli w Urzędzie.

(akta kontroli: str. 260-294, 400-414,430)

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli ocenia negatywnie działania Urzędu w zakresie organizacji bezpieczeństwa informacji oraz zapewnienia ciągłości działania. W Urzędzie nie było bowiem w pełni wdrożonego SZBI w rozumieniu § 19 ust. 1 rozporządzenia KRI. Urząd nie posiadał również jednolitej dokumentacji odnośnie polityki bezpieczeństwa informacji, a wprowadzone w Regulaminie w tym zakresie uregulowania były niepełne. Nie prowadzono także przeglądu i aktualizacji posiadanej dokumentacji w zakresie bezpieczeństwa informacji. W Urzędzie opracowano plany ciągłości działania i plany odtworzeniowe, należy jednak podkreślić, że powinny one zawierać bardziej szczegółowe zapisy i wskazane byłoby uszczegółowienie dokumentacji w tym zakresie. W okresie objętym kontrolą nie prowadzono testów i treningów związanych z planami zapewnienia ciągłości działania. Prawidłowo zidentyfikowano co prawda zbiory danych podlegających zabezpieczeniu, jednakże nie nadano im odpowiedniego poziomu ochrony, zgodnie z ich ważnością.

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

Opis stanu faktycznego

2.1. Urząd posiadał wdrożoną procedurę dotyczącą zabezpieczenia przed złośliwym oprogramowaniem polegającą na blokowaniu we wszystkich komputerach portów USB. W ramach przeprowadzonych oględzin zweryfikowano pięć komputerów stacjonarnych i stwierdzono, że użytkownicy posiadają jedynie przyznane lokalnie uprawnienia oraz że nie ma możliwości zainstalowania nieautoryzowanego oprogramowania. Było to zgodne z § 19 ust. 2 pkt 4 rozporządzenia KRI.

Urząd posiadał na stanie dwa tablety oraz 21 służbowych telefonów komórkowych. Tablety znajdowały się na stanie Straży Miejskiej i nie były używane, brak było również na nich oprogramowania z dostępem do zasobów Urzędu. Główny specjalista informatyk wyjaśnił, że telefony służbowe są zabezpieczone standardowymi aplikacjami i służą tylko jako urządzenia do komunikacji oraz wykonywania zdjęć.

(akta kontroli: str. 196-200)

2.2. Urząd zatrudniał 92 osoby uczestniczące, w ramach wykonywania swoich obowiązków służbowych, w procesie przetwarzania informacji. Nadanie uprawnień do dostępu do systemów IT oraz ich zmiana/odebranie następowało na podstawie

informacji mailowej, wysyłanej do informatyków lub ustnie. Nie stosowano w Urzędzie sformalizowanego wniosku o nadanie/cofnięcie/zmianę uprawnień.

W ramach przeprowadzonej kontroli dokonano weryfikacji dotyczącej adekwatności uprawnień do systemów komputerowych i zasobów dyskowych pracowników Urzędu, wynikających z zakresu ich obowiązków[21]. We wszystkich badanych przypadkach nie stwierdzono by posiadane przez nich uprawnienia wykraczały poza zakresy czynności. Było to zgodne z § 19 ust. 2 pkt 4 rozporządzenia KRI.

(akta kontroli: str. 201-256)

2.3. W okresie od 1 stycznia 2023 do 18 lipca 2024 r. w Urzędzie zakończyło zatrudnienie sześć osób. W ramach przeprowadzonej kontroli dokonano weryfikacji odebrania wszelkich uprawnień tym osobom. Ustalono, że w przypadku dwóch byłych pracowników ich konta w systemach były nadal aktywne, co opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli: str. 196-197)

2.4. Nadawanie uprawnień użytkownikom, tworzenie identyfikatorów, przydział haseł, czy też częstotliwość ich zmiany określono w Regulaminie. Wdrożono także usługę katalogową Active Directory[22] jako podstawową usługę, w oparciu o którą funkcjonował system logowania użytkowników do stacji roboczych. System obiegu dokumentów, jak i cały użytkowany pakiet oprogramowania firmy RADIX nie został jednak zintegrowany z usługą AD, co wymagało od użytkownika ponownego logowania się do aplikacji.

W Urzędzie określono zasady budowy hasła do poszczególnych systemów informatycznych określając minimalną liczbę znaków oraz ich złożoność. Należy jednak podkreślić, że występowała jedynie integracja loginu do poszczególnych systemów obsługiwanych przez użytkownika, natomiast nie wszystkie systemy wymuszały w ustalonych okresach czasowych zmianę hasła. Sprawdzanie stosownych zabezpieczeń technicznie w systemach IT dokonane na przykładzie trzech systemów wykazało, że żaden z nich nie wymuszał zmiany hasła i jego złożoności, co opisano w sekcji S*twierdzone nieprawidłowości*.

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

(akta kontroli: str. 260-294)

2.5. Oględziny pięciu stanowisk pracy realizujących zadania w Punkcie Obsługi Klienta, posiadające dostęp do ogólnopolskiej aplikacji *Źródło* wykazały, że monitory usytuowane były w sposób uniemożliwiający wgląd do danych przez osoby nieuprawnione, co było zgodne z § 19 ust. 2 pkt 7 rozporządzenia KRI.

(akta kontroli: str. 428)

2.6. W Urzędzie wprowadzono Regulamin użytkownika komputerów przenośnych. Zawarto w nim informacje m.in. w zakresie: przewożenia sprzętu, jego zabezpieczenia fizycznego, zalecanego działania w trakcie kradzieży, robienia kopii oraz sposobu ochrony danych zawartych w tym sprzęcie. Każdy użytkownik sprzętu przenośnego przed rozpoczęciem jego użytkowania miał obowiązek zapoznać się z wyżej wymienionym regulaminem i potwierdzić zapoznanie się z jego postanowieniami. Było to zgodne z § 19 ust. 2 pkt 8 rozporządzenia KRI.

(akta kontroli: str. 29-32)

[21] Na próbie 15 wybranych pracowników.
[22] Dalej: AD.

2.7. Komputery przenośne w Urzędzie były szyfrowane, a połączenie z zasobami Urzędu było skonfigurowane bezpiecznie. Spełniało to wymogi § 19 ust. 2 pkt 9 i 11 rozporządzenia KRI.

(akta kontroli: str. 260-294)

2.8. Serwerownia znajdowała się w wydzielonym pomieszczeniu w budynku głównym Urzędu. Dostęp do niej miały osoby z Zespołu do Spraw Informatyki, pracownicy Straży Miejskiej oraz pracownicy zaplecza socjalnego. Pomieszczenie to było klimatyzowane, a w czasie oględzin klimatyzacja była sprawna. Sprzęt informatyczny w serwerowni był podłączony do sieci elektrycznej dedykowanej, posiadającej własne zabezpieczenia. Rozdzielnica elektryczna zasilania obwodów dedykowanych serwerowni była zabezpieczona przed bezpośrednim dostępem osób nieuprawnionych, a w ramach zasilania zapasowego (podtrzymanie pracy urządzeń) wykorzystywane były UPS-y. W pomieszczeniu serwerowni znajdował się rejestr wejść/wyjść, natomiast w trakcie oględzin stwierdzono ryzyko związane z potencjalnymi zagrożeniami fizycznymi lub środowiskowymi dla tego pomieszczenia, co opisano w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli: str. 258-259)

2.9. W okresie objętym kontrolą obowiązywało jedenaście umów zawartych przez Urząd na zakup lub serwis sprzętu informatycznego i oprogramowania. Szczegółowe badanie czterech z nich wykazało, że w umowach tych zawarto zapisy gwarantujące zachowanie odpowiedniego poziomu bezpieczeństwa informacji. Zapisy te znajdowały się w dodatkowych umowach powierzenia danych osobowych do każdej z tych umów. Było to zgodne z § 19 ust. 2 pkt 10 rozporządzenia KRI.

(akta kontroli: str. 305-399, 437)

2.10. Sprzęt komputerowy w dużej mierze był serwisowany przez informatyków Urzędu. W sytuacjach, gdy komputer znajdował się w trakcie obejmującej go gwarancji, a nie było możliwości jego naprawy na miejscu, przed jego wysłaniem do serwisu wymontowywany był dysk twardy z danymi. Komputery, które posiadały gwarancję z opcją naprawy u klienta, były naprawiane w Urzędzie w asyście informatyka, natomiast komputery, które były przekazywane do innych jednostek, pozbawiano nośników danych.

Główny specjalista - informatyk wyjaśnił, że dyski twarde z komputerów przekazanych, czy też uszkodzonych, przechowywane były w Urzędzie i oczekiwały na wykonanie kasacji przez wyspecjalizowaną firmę.

(akta kontroli: str. 436)

2.11. W Załączniku nr 6 do postanowienia nr 12/2018 Burmistrza Miasta Nowa Ruda z dnia 10 lipca 2018 r. znajdowała się procedura tworzenia kopii zapasowych. W jej ramach określono czas przechowywana kopii zapasowych, dostęp do tych kopii, a także określono zasady nadzoru nad weryfikacją poprawności ich sporządzenia oraz zasady ich utylizacji. W procedurze tej wskazano również, że kopie zapasowe przechowywane powinny być w innym pomieszczeniu niż serwerownia.

(akta kontroli: str. 52-60, 258-259)

2.12. Zapisy w procedurze tworzenia kopii zapasowych określały także rodzaj nośników na jakich należy sporządzać kopie i sposób postępowania z nimi. Każdy nośnik miał być opisany datą jej sporządzenia. Wszystkie nośniki należało zaewidencjonować w *Rejestrze nośników komputerowych zawierających dane osobowe*. Należy podkreślić, że procedura tworzenia kopii nie zawierała zapisów dotyczących harmonogramu tworzenia kopii, a Urząd nie posiadał również w swoich zasobach innego dokumentu wskazującego na obowiązujący harmonogram tworzenia kopii zapasowych systemów komputerowych w Urzędzie.

Jak stwierdzono w trakcie oględzin[23] kopie zapasowe (bezpieczeństwa) były wykonywane na dostępnych zasobach dyskowych znajdujących się w serwerowni Urzędu. Nie wykonywano przy tym tych kopii na dyskach zewnętrznych, co opisano w sekcji *Stwierdzone nieprawidłowości*. W systemie do tworzenia kopii odnotowano, że kopie wykonywane były każdego dnia roboczego o tej samej godzinie.

(akta kontroli: str. 295-297, 429, 431-435)

2.13. Procedury obowiązujące w urzędzie nie przewidywały monitorowania pojemności nośników pamięci serwerów. W Załączniku nr 2 do postanowienia nr 12/2018 opisano jedynie plany awaryjne dotyczące odtworzenia systemu informatycznego po awarii krytycznej, na wypadek braku zasilania w sieci komputerowej oraz na wypadek utraty dostępu do sieci Internet. Z przeprowadzonych oględzin wynikało, że w Urzędzie znajdowały się trzy serwery fizyczne i 11 serwerów wirtualnych. Przeprowadzony w toku oględzin test zajętości czterech serwerów wykazał poszczególne zajętości, wynoszące: Serwer nr 1 – 78%, Serwer nr 2 – 92%, Serwer nr 3 – 93%, Serwer nr 4 – 30%.

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.

Główny specjalista - informatyk wyjaśnił, że niezwłocznie rozproszone zostaną zasoby serwerów 2 i 3 na serwery, na których zajętość dyskowa jest niższa niż 80%. Ponadto na potrzeby monitorowania, Urząd był w trakcie wdrażania dedykowanej aplikacji, do której za pomocą „agentów" dodaje się poszczególne serwery. Komunikaty o problemach będą wysyłane na adres mailowy informatyków.

(akta kontroli: str. 52-60, 260-294)

2.14. Urząd dokonał identyfikacji kluczowych elementów infrastruktury i usług IT w procesie zapewnienia ciągłości działania. W tym zakresie w Załączniku Nr 2 do postanowienia nr 12/2018 opisano pobieżnie postępowanie w przypadku awarii serwera, w przypadku braku zasilania w sieci komputerowej, czy też w przypadku braku dostępu do sieci Internet. Nie uwzględniono jednak przy tym wszystkich etapów takiej procedury polegających na nadaniu odpowiednich procentowych ważności kluczowym elementom, a także opisaniu planów naprawczych w przypadku wystąpienia awarii, co opisano w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli: str. 52-60)

Stwierdzone nieprawidłowości

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

1. Analiza polegająca na weryfikacji odebrania wszelkich uprawnień w systemach IT osobom już nie pracującym w Urzędzie wykazała, że w dwóch przypadkach (na sześć sprawdzanych) konta byłych pracowników były nadal aktywne, co było niezgodne z art. 19 ust. 2 pkt 5 rozporządzenia KRI.

   Główny specjalista - informatyk oświadczył, że nieprawidłowość ta spowodowana była przeoczeniem, a uchybienie to zostało niezwłocznie usunięte po ujawnieniu błędu.

   (akta kontroli: str. 196-197, 425)

2. Trzy poddane sprawdzeniu systemy informatyczne użytkowane przez Urząd nie wymuszały zmiany hasła i jego złożoności, co było niezgodne z pkt 6 polityki haseł Regulaminu. Jednocześnie umożliwiało to stosowanie nieadekwatnych

[23] 12 lipca 2024 r.

haseł dostępu do tych systemu w odniesieniu do istotności zawartych w nich informacji i było niezgodne z § 19 ust. 2 pkt 7 lit. c rozporządzenia KRI.

Główny specjalista - informatyk wyjaśnił, że nadawał stałe hasła każdemu użytkownikowi i nie posiadał wiedzy czy użytkownik dokonał zmiany hasła i w jakim zrobił to terminie. Dodał również, że niezwłocznie zostanie połączone logowanie do modułów systemów z AD, co spowoduje automatyzację zmiany haseł w wymaganym okresie przez użytkowników systemów.

Nieprawidłowość ta została usunięta w trakcie trwania kontroli.

(akta kontroli: str. 260-262)

3. W części pomieszczenia serwerowni znajdowały się materiały łatwopalne (segregatory, kartony, pudła itp.), które zostały przez informatyków niezwłocznie usunięte. Ponadto część zastosowanych zabezpieczeń fizycznych serwerowni, w niewystarczającym stopniu chroniła to pomieszczenie, co zwiększało ryzyko ujawnienia, modyfikacji, usunięcia lub zniszczenia informacji, będących w posiadaniu Urzędu. Było to niezgodne z § 19 ust. 2 pkt 9 rozporządzenia KRI.

Główny specjalista - informatyk wyjaśnił, że przyczyną braku zabezpieczeń był brak środków finansowych na zakup poszczególnych elementów zabezpieczeń.

(akta kontroli: str. 258-259, 431)

4. W trakcie wykonywania oględzin w serwerowni stwierdzono, że urządzenie z kopiami systemów IT Urzędu znajduje się w tym samym pomieszczeniu (serwerowni), co było niezgodne z *Procedurą tworzenia kopii zapasowych*, która wskazywała inne pomieszczenie, w którym mają być przechowywane nośniki z kopiami systemów i danych. Nie wykonywano przy tym kopii na dyskach zewnętrznych. Było to niezgodne § 19 ust. 2 pkt 12 lit. b rozporządzenia KRI, tj. zwiększało ryzyko utraty informacji w wyniku awarii.

Główny specjalista - informatyk wyjaśnił, że Urząd planuje pozyskać dodatkowe pomieszczenie znajdujące się w sąsiednim budynku, co umożliwiłoby alokację replikacji kopii baz danych. Tymczasowo przeniesiono urządzenie z kopiami systemów IT do innego pomieszczenia.

(akta kontroli: str. 258-259, 429)

5. W ramach identyfikacji kluczowych elementów infrastruktury i usług IT w procesie zapewnienia ciągłości działania, Urząd nie nadał im odpowiednich procentowych ważności, a także nie opisał planów naprawczych w przypadku wystąpienia ich awarii, czy to za pośrednictwem czynników zewnętrznych, czy też wewnętrznych, co było działaniem nierzetelnym.

Główny specjalista – informatyk przyznał, że brak było tych elementów i dodał, że dołożone zostaną wszelkie starania, aby na etapie tworzenia analizy ryzyka nie popełnić zaistniałych błędów.

(akta kontroli: str. 52-60, 301)

OCENA CZĄSTKOWA

Wdrożone i wykorzystywane w Urzędzie rozwiązania organizacyjne i techniczne nie zapewniały w pełni bezpieczeństwa informacji. Urząd zapewnił właściwe rozwiązania zapobiegające możliwości instalacji nieautoryzowanego oprogramowania na urządzeniach służbowych oraz uniemożliwiające dostęp do danych na urządzeniach mobilnych. Ponadto wszystkie zweryfikowane umowy serwisowe posiadały zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji.

Zidentyfikowane zostały kluczowe elementy infrastruktury i usługi IT, lecz nie nadano im odpowiednich procentowych ważności, a także nie opisano planów naprawczych w przypadku wystąpienia ich awarii. Nie zabezpieczono w wystarczający sposób nośników danych, na których przechowywane były kopie zapasowe. Ponadto

pomieszczenie serwerowni było wykorzystywane w sposób niezapewniający odpowiedniej ochrony przeciwpożarowej oraz przeciwwłamaniowej. W dwóch przypadkach nie zablokowano kont w systemach informatycznych, osobom, które zakończyły zatrudnienie. Brak było wystarczających wymogów dla haseł w ramach użytkowanych przez Urząd systemów informatycznych. Należy podkreślić, że Urząd w trakcie kontroli NIK wyeliminował nieprawidłowości związane z uprawnieniami, hasłami dostępu i przechowywaniem materiałów łatwopalnych w pomieszczeniu serwerowni.

OBSZAR

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

3.1. W okresie objętym kontrolą Urząd przeprowadził analizę ryzyka integralności, poufności i dostępności, zatwierdzoną przez Burmistrza w dniu 27 grudnia 2023 r. Jej elementy zawierała Analiza Ryzyka Ogólnego oraz Ocena Skutków Dla Przetwarzania Danych (DPIA). Dokument ten uwzględniał realizowane zadania, zidentyfikowane ryzyka z nimi związane, ocenę prawdopodobieństwa i skutku danego ryzyka oraz skalę tego ryzyka, osobę odpowiedzialną za dane ryzyko oraz plan postępowania z danym ryzykiem. Poziom ryzyka we wszystkich komórkach organizacyjnych oszacowano jako niski i w związku z tym akceptowalny oraz niewymagający podejmowania dalszego postępowania.

(akta kontroli: str. 81-97)

3.2. We wprowadzonym Regulaminie, zgodnie z § 19 ust. 2 pkt 13 rozporządzenia KRI, ustalono w Urzędzie sposób postępowania w przypadku naruszenia ochrony danych osobowych. W dokumencie tym wskazano sytuacje stanowiące naruszenie bezpieczeństwa informacji oraz zasady postępowania w przypadku ich stwierdzenia lub podejrzenia przez pracowników Urzędu ich wystąpienia. W ramach instrukcji wymieniono incydenty wymagające powiadomienia oraz ich typy.

IOD oświadczyła, że w okresie objętym kontrolą w Urzędzie nie wystąpiły incydenty w zakresie bezpieczeństwa informacji.

(akta kontroli: str. 15-80)

3.3. W Urzędzie w latach 2023-2024 przeprowadzano jedynie szkolenia z ochrony danych osobowych i bezpieczeństwa informacji dla każdego nowozatrudnionego pracownika Urzędu. W ramach tego szkolenia każdy pracownik zaznajamiał się z zabezpieczeniami informatycznymi i internetowymi, a także poczty elektronicznej oraz sprzętu mobilnego, tj.: laptopów i nośników wynoszonych na zewnątrz poza Urząd.

W okresie objętym kontrolą nie realizowano szkoleń z zakresu bezpieczeństwa informacji dla wszystkich pracowników przetwarzających informacje, pomimo że obowiązek ich przeprowadzania wynikał z § 19 ust. 2 pkt 6 rozporządzenia KRI, co opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli: str. 417-423)

3.4. W dniach 2-13 października 2023 w Urzędzie przeprowadzono okresowy audyt wewnętrzny, o którym mowa w § 19 ust. 2 pkt 14 rozporządzenia KRI. Audyt przeprowadziły dwie osoby bezpośrednio odpowiedzialne w Urzędzie za nadzór i zakres badanego obszaru, tj.: IOD oraz Główny specjalista informatyk, co naruszało zasady niezależności oraz obiektywności audytu i zostało opisane w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli: str. 98-125)

Stwierdzone nieprawidłowości

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

1. W latach 2023 – 2024 w Urzędzie nie realizowano szkoleń z zakresu bezpieczeństwa informacji, pomimo, że obowiązek ich przeprowadzania wynikał z § 19 ust. 2 pkt 6 rozporządzenia KRI.

   IOD wyjaśniła, że wszyscy nowo przyjęci pracownicy przechodzą odpowiednie szkolenia, natomiast w uzyskanej w ramach Projektu dotacji przewidziano szkolenia w ramach bezpieczeństwa informacji dla wszystkich pracowników zatrudnionych w Urzędzie.

   NIK wskazuje, że szkolenia osób zaangażowanych w proces przetwarzania informacji, zgodnie z cytowanym wyżej przepisem rozporządzenia KRI, powinny obejmować szczególnie takie zagadnienia jak: zagrożenia bezpieczeństwa informacji; skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna oraz stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzeń i oprogramowania minimalizującego ryzyko błędów ludzkich. Zatem samo przeszkolenie nowoprzyjętych pracowników z zakresu PBI jest niewystarczające.

   (akta kontroli: str. 417-423)

2. Audyt wewnętrzny, o którym mowa w § 19 ust. 2 pkt 14 rozporządzenia KRI był wykonany przez pracowników Urzędu zatrudnionych odpowiednio na stanowisku IOD oraz Głównego specjalisty - informatyka. W związku z faktem, że w zakresach obowiązków tych osób znajdowały się obszary dotyczące ochrony danych osobowych, czy też zarządzania systemami informatycznymi, audytowali oni obszary, za które bezpośrednio odpowiadali. Naruszało to zasady niezależności i obiektywności audytu określone w Standardach audytu wewnętrznego dla jednostek sektora finansów publicznych[24] oraz w pkt 9.2 lit. e normy ISO/IEC 27001[25].

   Główny specjalista – informatyk wyjaśnił, że w związku z brakiem funduszy audyt wewnętrzny wykonano w formie samooceny, a wykonując audyt posiłkowano się szablonem audytu z lat poprzednich.

   (akta kontroli: str. 98-125, 300, 304)

OCENA CZĄSTKOWA

W Urzędzie w sposób rzetelny przeprowadzono analizę ryzyka utraty integralności, poufności oraz dostępności informacji, wdrożono postępowanie w sytuacjach wystąpienia lub podejrzenia incydentu w zakresie bezpieczeństwa informacji. Zapewniono również przy przyjęciu do pracy szkolenia pracownikom zaangażowanym w proces przetwarzania informacji, jednakże nie przeprowadzano w kontrolowanym okresie szkoleń dla wszystkich pracowników Urzędu. W 2023 r. przeprowadzono okresowy, coroczny audyt wewnętrzny z zakresu bezpieczeństwa informacji przez pracownika IOD oraz Głównego specjalistę - informatyka, co naruszało zasady niezależności oraz obiektywności audytu.

IV. Uwagi i wnioski

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

Uwagi

NIK zwraca uwagę, że charakter, waga i skala stwierdzonych nieprawidłowości wskazują na potrzebę wzmocnienia przez Burmistrza działań podejmowanych w obszarze kontroli zarządczej, o której mowa w art. 68 ust. 1 ustawy z dnia 27

[24] Komunikat Ministra Rozwoju i Finansów z dnia 12 grudnia 2016 r. w sprawie standardów audytu wewnętrznego dla jednostek sektora finansów publicznych (Dz. Urz. MRiF poz. 28).
[25] Norma ISO/IEC 27001 - Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania; dalej: norma ISO/IEC 27001.

sierpnia 2009 r. o finansach publicznych[26], w celu zapewnienia zgodnego z prawem, terminowego i efektywnego realizowania celów i zadań Urzędu w zakresie związanym z zapewnieniem bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych.

Wnioski

1. Wprowadzenie i wdrożenie kompletnego Systemu Zarządzania Bezpieczeństwem Informacji, wraz z Polityką Bezpieczeństwa Informacji.
2. Zapewnienie nadania zbiorom danych odpowiedniej ważności w procesie identyfikowania danych podlegających zabezpieczeniu, a tym samym poziomu ochrony.
3. Uzupełnienie brakujących oświadczeń o zapoznaniu się pracowników z Regulaminem użytkowania komputerów przenośnych.
4. Przeprowadzenie przeglądu stanu bezpieczeństwa w ramach analizy ryzyka w Urzędzie.
5. Przeprowadzanie testów i treningów związanych z planami zapewnienia ciągłości działania.
6. Bieżące aktualizowanie dokumentacji składającej się na SZBI w zakresie dotyczącym zmieniającego się otoczenia.
7. Odpowiednie zabezpieczenie pomieszczeń infrastruktury informatycznej (serwerowni).
8. Przechowywanie nośników danych z kopiami zapasowymi w sposób zapewniający odpowiednią ochronę danych przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami.
9. Przypisywanie procentowych ważności i opisywanie planów naprawczych w przypadku wystąpienia awarii kluczowych elementów infrastruktury i usług IT, w ramach ich identyfikacji w procesie zapewnienia ciągłości działania.
10. Przeprowadzenie szkoleń dla pracowników Urzędu w zakresie bezpieczeństwa informacji.
11. Przeprowadzenie audytu wewnętrznego dotyczącego bezpieczeństwa informacji z zachowaniem zasadny niezależności i obiektywności.

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.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

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

[26] Dz. U. z 2023 r. poz. 1270, ze zm.

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.

Wrocław, 19 września 2024 r.

Kontroler
Waldemar Zimoch
Główny specjalista kontroli państwowej

.....
podpis

Najwyższa Izba Kontroli
Delegatura we Wrocławiu
Dyrektor
z up. p.o. Wicedyrektor
Artur Urban

.....
podpis