NAJWYŻSZA IZBA KONTROLI

DELEGATURA WE WROCŁAWIU

LWR.410.13.5.2024

Pan
Janusz Chodasewicz
Burmistrz Miasta Kamienna Góra

Urząd Miasta Kamienna Góra
pl. Grunwaldzki 1
58-400 Kamienna Góra

WYSTĄPIENIE POKONTROLNE

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

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miasta Kamienna Góra[1], pl. Grunwaldzki 1, 58-400 Kamienna Góra.
Kierownik jednostki kontrolowanej	Janusz Chodasewicz, Burmistrz Miasta Kamienna Góra[2], od 23 listopada 2018 r.
Zakres przedmiotowy kontroli	Rozwiązania organizacyjne i techniczne w zakresie zapewnienia bezpieczeństwa przetwarzania informacji oraz zapewnienia ciągłości działania w urzędzie i ich stosowanie.
Okres objęty kontrolą	Od 1 stycznia 2023 r. do dnia zakończenia 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
Kontrolerzy	1. Piotr Kociołek, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LWR/82/2024 z 28 maja 2024 r. 2. Cezary Mazik, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LWR/95/2024 z 26 czerwca 2024 r.

(akta kontroli: str. 1-6)

[1] Dalej: Urząd.
[2] Dalej: Burmistrz.
[3] Czynności kontrolne zakończono 17 lipca 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.

W okresie objętym kontrolą stosowano dokumentację składającą się na System Zarządzania Bezpieczeństwem Informacji[6] i Politykę Ochrony Danych[7], uwzględniającą wymogi odpowiednio rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[8] oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[9].

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

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

W toku kontroli stwierdzono jednak nieprawidłowości w każdym z trzech kontrolowanych obszarów, polegające na: **[1]** nierzetelnym sporządzeniu dokumentacji związanej z zapewnieniem ciągłości działania systemów informatycznych, **[2]** nadmiarowym udostępnieniu wszystkim pracownikom Urzędu szczegółowych zasad zarządzania środowiskiem informatycznym, **[3]** nie w pełni rzetelnej aktualizacji SZBI, **[4]** niesporządzeniu wewnętrznych regulacji dotyczących pracy zdalnej, przewidzianych w SZBI, **[5]** użytkowania pomieszczenia serwerowni w sposób niezapewniający odpowiedniej ochrony przeciwpożarowej, **[6]** nieprawidłowym przechowywaniu nośników danych z kopiami zapasowymi, **[7]** udzieleniu pracownikom dostępu do systemów informatycznych bez stosownego upoważnienia lub ze zbyt ogólnym upoważnieniem, **[8]** niezablokowaniu kont w systemach IT byłym pracownikom Urzędu, **[9]** ustaleniu wymogów dla haseł w jednym z systemów informatycznych niezgodnie z wymogami SZBI, **[10]** braku w dwóch umowach serwisowych zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji, oraz **[11]** nieprzeprowadzeniu w 2023 r. okresowego, corocznego audytu wewnętrznego z zakresu bezpieczeństwa informacji.

[5] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[6] Dalej: SZBI.
[7] Dalej: POD.
[8] Dz. U. poz. 773, dalej: rozporządzenie KRI.
[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. W Urzędzie zidentyfikowano zbiory danych, które są w nim przetwarzane i podlegają zabezpieczeniu. Dla każdego z tych zbiorów sporządzono kartę rejestru czynności przetwarzania (74 zbiory danych), bądź kartę kategorii czynności przetwarzania (dwa zbiory danych). W kartach tych wskazano informacje, o których mowa odpowiednio w art. 30 ust. 1 oraz ust. 2 RODO, w tym m.in.: administratora danych, podmiot przetwarzający, kategorię danych, czas ich przetwarzania, nazwę systemu/oprogramowania, w którym są one przetwarzane[11] oraz opis zastosowanych technicznych i organizacyjnych środków bezpieczeństwa tych danych.

(akta kontroli: str. 342-344, 390-394)

1.2. W Urzędzie opracowano i wdrożono SZBI[12], o którym mowa w § 19 ust. 1 rozporządzenia KRI. Składał się on z:

- Polityki Bezpieczeństwa Informacji[13];
- Polityki Bezpieczeństwa Informacji w zakresie zarządzania systemem informatycznym[14];
- Polityki Bezpieczeństwa Informacji w zakresie postępowania w sytuacjach naruszenia bezpieczeństwa informacji[15];
- Planu ciągłości działania w sytuacji awarii systemu informatycznego[16];
- Procedury zarządzania ryzykiem bezpieczeństwa informacji[17].

Dokumentacja ta została zatwierdzona przez Burmistrza i przedstawiona do zapoznania się i stosowania wszystkim pracownikom Urzędu. Nadzór nad SZBI powierzono[18] Inspektorowi Ochrony Danych[19] oraz Administratorom Systemów Informatycznych[20], którzy byli odpowiedzialni za jego przygotowanie, wdrożenie, przeglądy i modyfikacje.

(akta kontroli: str. 74-203, 458, 463)

1.3. Zgodnie z art. 24 ust. 2 RODO, wprowadzono[21] w Urzędzie POD, opisującą zasady przetwarzania danych osobowych w celu spełniania wymagań RODO. POD określała m.in. osoby pełniące funkcje związane z zapewnieniem właściwej ochrony danych osobowych, zasady dopuszczania pracowników Urzędu do przetwarzania tych danych, procedurę udostępniania danych osobowych oraz środki organizacyjne, techniczne oraz fizyczne, stosowane w celu zapewnienia poufności, integralności i rozliczalności przetwarzania danych.

---

[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] Nazwę systemu/oprogramowania, w którym przetwarzane są dane wskazano w kartach rejestru czynności przetwarzania.
[12] Wprowadzony zarządzeniami Burmistrza: nr 167/2022 z 28 kwietnia 2022 r. i nr 133/2024 z 23 maja 2024 r.
[13] Dalej: PBI.
[14] Dalej: PBI-ZSI.
[15] Dalej: PBI-NBI.
[16] Dalej: Plan ciągłości działania.
[17] Dalej: Procedura zarządzania ryzykiem.
[18] Zgodnie z § 5 zarządzenia Burmistrza nr 167/2022 z 28 kwietnia 2022 r. i § 4 zarządzenia Burmistrza nr 133/2024 z 23 maja 2024 r.
[19] Dalej: IOD.
[20] Dalej: ASI.
[21] Zarządzeniem Burmistrza nr 31/2022 z 2 lutego 2022 r.

Dokumentacja ta została zatwierdzona przez Burmistrza i przedstawiona do zapoznania się i stosowania wszystkim pracownikom Urzędu, a nadzór nad nią powierzono IOD[22].

(akta kontroli: str. 204-227, 458, 464)

1.4. W okresie objętym kontrolą przeprowadzono[23] w Urzędzie analizę ryzyka w celu zidentyfikowania i oceny potencjalnych zagrożeń, które mogą wpłynąć na ciągłość działania systemów informatycznych Urzędu oraz opracowania środków zaradczych[24]. W ramach tej analizy zidentyfikowano sześć zagrożeń[25], którym przypisano odpowiedni poziom wpływu oraz prawdopodobieństwa i określono poziom ryzyka. W trzech przypadkach poziom ten oceniono jako wysoki (ryzyka krytyczne). Dla wszystkich zidentyfikowanych zagrożeń określono środki zaradcze. Analiza ta została sporządzona przez Informatyka Urzędu, jednak nie poddano jej zatwierdzeniu przez Burmistrza, co opisano w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli: str. 349-351)

1.5. Rolę polityki ciągłości działania w Urzędzie wypełniała PBI-ZSI, będąca integralną częścią SZBI. Opisano w niej środki i metody stosowane w zarządzaniu oraz eksploatacji systemów informatycznych, w celu ich odpowiedniego zabezpieczenia i zapewnienia ciągłości działania. W polityce tej m.in. zidentyfikowano posiadane aktywa informatyczne, opisano sposób ich zabezpieczenia, określono sposób tworzenia i przechowywania kopii bezpieczeństwa danych, dokonywania przeglądów sprzętu, raportowania ciągłości działania i postępowania w sytuacjach awaryjnych. PBI-ZSI została (wraz z innymi dokumentami składającymi się na SZBI) zakomunikowana wszystkim pracownikom Urzędu w całości, łącznie z opisem m.in. urządzeń, ich lokalizacji, budowy sieci informatycznej i zastosowanych zabezpieczeń technicznych, która to część powinna być udostępniona wyłącznie pracownikom odpowiedzialnym za ten zakres, o czym szerzej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli: str. 163-182, 458, 463)

1.6. Działania zapewniające przywrócenie zdolności realizacji działań Urzędu w przypadku awarii systemu informatycznego zostały określone w Planie ciągłości działania. W dokumencie tym wskazano opis działań w przypadku wystąpienia awarii, czynności do podjęcia, zadania do wykonania i osoby odpowiedzialne. W planie tym nie przewidziano scenariuszy innych niż awaria systemu, mimo zidentyfikowania w analizie ryzyka (o której mowa w pkt 1.4 niniejszego wystąpienia pokontrolnego) sześciu zagrożeń ciągłości działania, w tym trzech krytycznych. Powyższe szerzej opisano w sekcji *Stwierdzone nieprawidłowości.*

Nie określono w Planie ciągłości działania także akceptowalnego czasu przywrócenia ciągłości działania systemów informatycznych Urzędu. Jak wyjaśnił Burmistrz, czas przywrócenia systemów do działania został wykazany w raporcie z testowania Planu ciągłości działania, przeprowadzonego 15 września 2023 r.

(akta kontroli: str. 191-194, 349-351, 356-357, 456, 459)

1.7. Urząd w okresie objętym kontrolą przeprowadził testowanie przyjętego Planu ciągłości działania. Test ten został wykonany 15 września 2023 r. i polegał na sprawdzeniu skuteczności procedur awaryjnych w przypadku awarii głównego serwera baz danych Urzędu, na podstawie scenariusza testowania, przygotowanego

[22] Zgodnie z § 3 zarządzenia Burmistrza nr 31/2022 z 2 lutego 2022 r.
[23] 5 czerwca 2023 r.
[24] Dalej: Analiza ryzyka w związku z potrzebą zachowania ciągłości działania.
[25] Tj.: [1] awarie sprzętu, [2] przerwy w dostawie prądu, [3] ataki cybernetyczne, [4] błędy ludzkie, [5] katastrofy naturalne i [6] przerwy w łączności sieciowej.

przez Informatyka Urzędu. Z przeprowadzonego testu sporządzono raport, w którym opisano przebieg testu, jego wyniki i ich analizę, a także wnioski i rekomendacje oraz działania korygujące. Przeprowadzenie kolejnego testu zaplanowano na wrzesień 2024 r.

(akta kontroli: str. 354-357)

1.8. Zgodnie z § 19 ust. 2 pkt 1 rozporządzenia KRI, dokonywano w Urzędzie przeglądu i aktualizacji dokumentacji składającej się na SZBI, a także POD. Przeglądu takiego dokonywał IOD, co najmniej raz w roku kalendarzowym[26].

W wyniku przeprowadzonych przeglądów dokonywano aktualizacji SZBI – zarządzeniami Burmistrza: [1] nr 339/2022 z 8 września 2022 r., [2] nr 183/2023 z 6 lipca 2023 r. i [3] nr 76/2024 z 6 marca 2024 r. Ponadto, w związku z wejściem w życie 23 maja 2024 r. nowego rozporządzenia KRI, wprowadzono tego dnia nową wersję SZBI[27].

Niemniej, mimo dokonywanych przeglądów i aktualizacji SZBI, nie były one prowadzone w pełni rzetelnie, ponieważ dokumentacja ta zawierała nieaktualne zapisy, o czym szerzej w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli: str. 228-238)

1.9. Zgodnie z obowiązującymi w Urzędzie regulacjami, nadzór nad SZBI powierzono IOD oraz ASI. Zakres obowiązków ASI został określony zarządzeniem Burmistrza nr 504/2017 z 1 września 2017 r.[28] (oraz w PBI) i obejmował m.in.: zarządzanie i administrowanie bazami danych, podejmowanie działań w celu właściwego zabezpieczenia danych, bieżące monitorowanie systemu informatycznego, realizację decyzji odnośnie do nadawania osobom uprawnień do danych, udział w procesie reagowania na incydenty w zakresie bezpieczeństwa, przeprowadzanie szkoleń dla pracowników oraz wykonywanie zadań związanych z tworzeniem, przechowywaniem i sprawdzaniem kopii bezpieczeństwa danych. Powyższym zarządzeniem powołano na ASI dwóch pracowników Urzędu (Informatyków), którzy pisemnie potwierdzili przyjęcie powierzonej funkcji[29]. W zakresie obowiązków tych osób na stanowisku Informatyka wskazano z kolei m.in. zarządzanie systemem informatycznym Urzędu, zabezpieczanie ciągłości funkcjonowania infrastruktury informatycznej czy analizę zasobów sprzętu komputerowego i oprogramowania.

Powyższe osoby posiadały odpowiednie kompetencje w zakresie powierzonych obowiązków, potwierdzone posiadanym wykształceniem oraz przebytymi szkoleniami.

(akta kontroli: str. 149, 321-332, 340-341)

1.10. Na podstawie art. 37 ust. 1 RODO i art. 8 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[30], Burmistrz wyznaczył[31] jedną osobę, będącą pracownikiem Urzędu, do pełnienia funkcji IOD w Urzędzie i jednostkach mu podległych[32]. Osoba ta posiadała odpowiednie kwalifikacje do pełnienia tej funkcji, potwierdzone świadectwem ukończenia studiów podyplomowych w zakresie „Inspektor ochrony danych osobowych". Zakres obowiązków IOD obejmował zadania

[26] Co było dokumentowane podpisem w prowadzonych rejestrach przeglądów, odpowiednio SZBI i POD.
[27] Zarządzeniem Burmistrza nr 133/2024 z 23 maja 2024 r.
[28] W sprawie powołania i określenia zadań Administratora Bezpieczeństwa Informacji i Administratora Systemów Informatycznych w Urzędzie Miasta Kamienna Góra.
[29] Dokument ten został włączony do ich akt osobowych.
[30] Dz. U. z 2019 r. poz. 1781.
[31] Zarządzeniem Burmistrza nr 231/2018 z 16 lipca 2018 r.
[32] Miejski Ośrodek Pomocy Społecznej w Kamiennej Górze, Miejska Biblioteka Publiczna w Kamiennej Górze, Muzeum Tkactwa w Kamiennej Górze, Centrum Kultury w Kamiennej Górze i Miejskie Centrum Kultury Fizycznej w Kamiennej Górze.

związane z ochroną i zabezpieczeniem danych osobowych, w tym m.in. zadania określone w art. 39 ust. 1 RODO.

(akta kontroli: str. 333-341)

1.11. Zgodnie z Regulaminem organizacyjnym Urzędu[33], IOD podlegał bezpośrednio Burmistrzowi, co było zgodne z art. 38 ust. 3 RODO, w którym wskazano, że IOD podlega bezpośrednio najwyższemu kierownictwu administratora danych lub podmiotu przetwarzającego.

W zakresie obowiązków pracownika pełniącego funkcję IOD nie wskazano czynności innych, niż związanych z pełnioną funkcją i ochroną danych osobowych, wobec czego spełniono wymagania z art. 36 ust. 6 RODO, tj. zapewniono, że realizowane przez IOD zadania i obowiązki nie powodowały konfliktu interesów.

(akta kontroli: str. 18, 337-339)

1.12. Zgodnie z art. 21 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[34], zarządzeniem Burmistrza nr 71/2021 z 18 lutego 2021 r. wyznaczono Informatyka Urzędu, pełniącego funkcję ASI, jako osobę odpowiedzialną za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Dane wyżej wymienionej osoby zostały przekazane do CSIRT-NASK[35] 19 lutego 2021 r., tj. w terminie zgodnym z art. 22 ust. 1 pkt 5 ustawy o ksc[36].

Nie skorzystano natomiast z uprawnienia określonego w art. 21 ust. 2 i 3 ustawy o ksc, tj. nie wyznaczono jednej osoby odpowiedzialnej za utrzymywanie wyżej wymienionych kontaktów w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jednostki organizacyjne Miasta Kamienna Góra oraz jednostki podległe i nadzorowane przez Burmistrza. Do wyżej wymienionych jednostek przekazano 14 kwietnia 2021 r. pismo IOD[37], przypominające o obowiązku wynikającym z art. 21 ust. 1 ustawy o ksc.

(akta kontroli: str. 292-296)

1.13. Obowiązująca w Urzędzie PBI nie zawierała wymogu sporządzenia odrębnych dokumentów wykonawczych, stanowiących uszczegółowione procedury, polityki czy instrukcje. Wymóg taki natomiast zawierała PBI-ZSI, w której wskazano, iż Administrator Danych Osobowych[38] (funkcję tę pełnił Burmistrz) jest odpowiedzialny za wdrożenie wewnętrznej regulacji (zarządzenia) dotyczącej pracy zdalnej w Urzędzie, która powinna zawierać m.in. zasady porozumienia się pracodawcy i pracownika wykonującego pracę zdalną, zasady kontroli wykonywania pracy przez pracownika wykonującego pracę zdalną, zasady kontroli przestrzegania wymogów w zakresie bezpieczeństwa i ochrony informacji oraz zasady instalacji, inwentaryzacji, konserwacji aktualizacji oprogramowania i serwisu, powierzonych pracownikowi urządzeń. Powyższe zarządzenie nie zostało sporządzone, o czym szerzej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli: str. 150-182)

1.14. Zgodnie z § 19 ust. 2 pkt 2 rozporządzenia KRI, w Urzędzie utrzymywano aktualność inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. W tym celu wykorzystywano oprogramowanie dedykowane do danych kategorii sprzętu, tj. do urządzeń

[33] Wprowadzonym zarządzeniem Burmistrza nr 276/2019 z 22 lipca 2019 r., ze zm.
[34] Dz. U. z 2024 r. poz. 1077, dalej: ustawa o ksc.
[35] Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy.
[36] Tj. w terminie 14 dni od dnia wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
[37] Znak IOD.142.3.1.2021.
[38] Dalej: ADO.

podłączonych do usługi *Active Directory*[39] (komputery i serwery), do drukarek, macierzy dyskowych oraz urządzenia UTM, pełniącego funkcje m.in. routera i firewall. Oprogramowanie to pozwalało na wykrywanie i monitorowanie urządzeń – każdy element posiadał odrębny rekord w bazie, wraz ze wskazaniem m.in. aktualnej konfiguracji, zainstalowanego oprogramowania, stanu urządzenia oraz użytkownika odpowiedzialnego za sprzęt. Przeprowadzone w trakcie oględzin[40] badanie obejmujące próbę celowo wybranych 14 urządzeń[41] wykazało, że wyżej wymienione oprogramowanie wskazywało aktualne dane na ich temat, w tym aktualną konfigurację i zainstalowane oprogramowanie.

(akta kontroli: str. 400-401)

1.15. Urząd przystąpił do Programu „Cyberbezpieczny Samorząd"[42], realizowanego przez Centrum Projektów Polska Cyfrowa w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027. Umowa o powierzenie grantu[43] o wartości 838,9 tys. zł[44] została podpisana 6 maja 2024 r., a czas jej realizacji ustalono na 24 miesiące od dnia wejścia w życie. W ramach tej umowy zaplanowano zakup sprzętu informatycznego, w tym: serwera domenowego, serwerów NAS[45], urządzeń sieciowych (switch, UTM[46]) oraz kluczy sprzętowych do dwuetapowej weryfikacji tożsamości dla pracowników Urzędu, a także oprogramowania do systemu DLP[47] i kompleksowego zarządzania infrastrukturą informatyczną. W ramach umowy przewidziano także środki na przeprowadzenie szkolenia dla pracowników oraz wykonanie audytu SZBI przez firmę zewnętrzną.

Jako element pomiaru poprawy cyberbezpieczeństwa w wyniku realizacji tego 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[48] oraz planowane zmiany w związku z realizacją Projektu, w tym przede wszystkim wdrożenie nowych systemów bezpieczeństwa: SIEM[49], DLP, NAC[50], WAF[51], PAM[52], DAM[53], MDM[54], CMDB[55] oraz narzędzia wspierającego analizę ryzyka.

(akta kontroli: str. 250-291)

Stwierdzone nieprawidłowości

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

1. Analiza ryzyka w związku z potrzebą zachowania ciągłości działania z 5 czerwca 2023 r. nie została poddana zatwierdzeniu przez Burmistrza.

---

[39] Usługa umożliwiająca centralne zarządzanie tożsamościami i dostępem użytkowników komputerów, dalej: AD.
[40] Z 26 czerwca 2024 r.
[41] W tym 10 komputerów stacjonarnych, jednego laptopa, jednego serwera, jednej drukarki oraz jednego urządzenia UTM.
[42] Dalej: Projekt.
[43] Nr FERC.02.02-CS.01-001/23/0712/ FERC.02.02-CS.01-001/23/2024.
[44] Kwota grantu bez udziału własnego gminy miejskiej Kamienna Góra, pokrywa 100% wartości projektu.
[45] Serwer NAS (ang. *Network Attached Storage*) – sieciowa pamięć masowa.
[46] Urządzenie UTM (ang. *Unified Threat Management*), to zintegrowane rozwiązanie do zarządzania zagrożeniami, które umożliwia ochronę sieci.
[47] Ang. *Data Loss Prevention* – system zapobiegania utracie danych.
[48] Były to: [1] Zarządzanie, [2] System Zarządzania Bezpieczeństwem Informacji, [3] Ochrona, [4] Zdarzenia i Monitoring, [5] Reagowanie, [6] Odtwarzanie, [7] Infrastruktura i [8] Telekomunikacja.
[49] Ang. *Security Information and Event Management* – system zarządzania informacjami i zdarzeniami zabezpieczeń.
[50] Ang. *Network Access Control* – system kontroli dostępu do sieci.
[51] Ang. *Web Application Firewall* – zapora aplikacji www.
[52] Ang. *Privileged Access Management* – system zarządzania dostępem uprzywilejowanym.
[53] Ang. *Database Access Management* – system zarządzania dostępem do baz danych.
[54] Ang. *Mobile Device Management* – system zarządzania urządzeniami mobilnymi.
[55] Ang. *Configuration Management Data Base* – system zarządzania bazą konfiguracji.

Według wyjaśnień Burmistrza, został on zapoznany z powyższą analizą i zaakceptował ją ustnie.

Najwyższa Izba Kontroli wskazuje, że proces zarządzania ryzykiem powinien być dokumentowany (Standard B „Standardów kontroli zarządczej dla sektora finansów publicznych"[56]). Dotyczy to również akceptacji przedmiotowej Analizy ryzyka przez Burmistrza jako kierownika jednostki odpowiedzialnego za zapewnienie funkcjonowania adekwatnej, skutecznej i efektywnej kontroli zarządczej.

(akta kontroli: str. 349-351, 455-458)

2. PBI-ZSI została zakomunikowana wszystkim pracownikom Urzędu w całości, łącznie z dokładnym opisem m.in. urządzeń, ich lokalizacji, budowy sieci informatycznej i zastosowanych zabezpieczeń technicznych. Stwarza to ryzyko, że informacje zawarte w tym dokumencie mogą zostać wykorzystane do przełamania ustanowionych zabezpieczeń. Było to niezgodne z § 19 ust. 2 pkt 7 oraz § 19 ust. 2 pkt 11 rozporządzenia KRI, które obligują kierownictwo podmiotów publicznych do zapewnienia właściwej ochrony przetwarzanych informacji oraz ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji. Ponadto stanowiło to naruszenie zasad określonych w załączniku A normy ISO 27001 punkt A.5.1.1, według której szczegóły techniczne zawarte w PBI winne zostać udostępnione wyłącznie odpowiedzialnym pracownikom (nie podlegają one publikacji).

Burmistrz wyjaśnił, że pracownicy zostali zapoznani z PBI-ZSI w całości, gdyż stanowiła ona integralną część SZBI, a każdy pracownik, który otrzymuje upoważnienie do przetwarzania danych osobowych, jednocześnie zostaje zobowiązany do zachowania tajemnicy przetwarzanych danych oraz o sposobie ich zabezpieczenia. Burmistrz dodał, że PBI-ZSI poddana zostanie analizie, a dane związane ze szczegółowymi zasadami zarządzania środowiskiem informatycznym zostaną zanonimizowane i nie będą dostępne dla wszystkich pracowników, a tylko dla osób upoważnionych w tym zakresie, tj. ASI, IOD i ADO.

(akta kontroli: str. 160, 169-178, 455-463, 482-483)

3. Plan ciągłości działania przewidywał wyłącznie jeden scenariusz, tj. na wypadek awarii systemu[57], mimo zidentyfikowania w Analizie ryzyka w związku z potrzebą zachowania ciągłości działania sześciu zagrożeń, mogących wpłynąć na ciągłość działania systemów informatycznych, w tym trzech krytycznych, co było działaniem nierzetelnym.

Jak wyjaśnił Burmistrz, system informatyczny jest kluczowym elementem działania organizacji, więc jego awaria może mieć najpoważniejsze skutki i skupienie się na tym scenariuszu wynikało z jego priorytetowego znaczenia dla zachowania ciągłości działania.

Zdaniem NIK Plan ciągłości działania powinien obejmować postępowanie w zakresie wszystkich zidentyfikowanych ryzyk w przypadku ich wystąpienia.

(akta kontroli: str. 191-194, 349-351, 482-484)

4. Nierzetelnie przeprowadzano w okresie objętym kontrolą przeglądy i aktualizacje SZBI. PBI-ZSI zawierała bowiem zapisy dotyczące przechowywania kopii zapasowych na nośnikach optycznych (płytach DVD), podczas gdy praktyka taka

[56] Załącznik do komunikatu nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych (Dz. Urz. Min. Fin. Nr 15, poz. 84).
[57] Zagrożenie o wysokim poziomie ryzyka (krytyczne).

nie była w Urzędzie stosowana[58]. Zapis ten nie został zmieniony, mimo dokonywania corocznych przeglądów i aktualizacji SZBI.

Według wyjaśnień Burmistrza, kopii zapasowych nie przechowuje się na nośnikach optycznych, gdyż przestały one spełniać minimalne wymagania techniczne z uwagi na zbyt małą pojemność. Brak zmiany zapisów w tym zakresie w PBI-ZSI Burmistrz wyjaśnił natomiast dynamicznym rozwojem infrastruktury teleinformatycznej Urzędu.

NIK zwraca uwagę, że w związku ze zmieniającym się otoczeniem należy zapewnić okresową aktualizację regulacji wewnętrznych, tak by odpowiadały one stosowanej praktyce i zachodzącym zmianom w infrastrukturze informatycznej Urzędu.

(akta kontroli: str. 172-174, 228-232, 456, 460)

5. Nie sporządzono wewnętrznych regulacji, dotyczących pracy zdalnej w Urzędzie, mimo iż wymagały tego zapisy obowiązującej PBI-ZSI.

Jak wyjaśnił Burmistrz, nie wdrożono powyższych regulacji, ponieważ w Urzędzie nie została wprowadzona możliwość wykonywania pracy zdalnej, a zapisy w PBI-ZSI zostały wprowadzone z uwagi na możliwość składania wniosków o taką formę pracy, przewidzianą w ustawie z dnia 26 czerwca 1974 r. Kodeks pracy[59]. Burmistrz dodał, iż w przypadku dopuszczenia w Urzędzie do wykonywania pracy zdalnej, wprowadzone zostaną odpowiednie regulacje w tym zakresie.

NIK nie podziela argumentacji wynikającej z wyjaśnień Burmistrza. Opracowanie i wdrożenie dokumentów wykonawczych, które przewidziano w dokumentacji składającej się na SZBI, ma na celu ustanowienie odpowiednich zabezpieczeń w zakresie bezpieczeństwa informacji i z uwagi na swój systemowy charakter nie powinno być uzależnione od aktualnej polityki Urzędu dotyczącej wykonywania pracy zdalnej. Ponadto należy wskazać, że obowiązek sporządzenia przedmiotowej regulacji został nałożony przez samą jednostkę kontrolowaną, bez wskazania warunku dopuszczenia wykonywania w niej pracy zdalnej.

(akta kontroli: str.180-181, 455, 458-459)

OCENA CZĄSTKOWA

Działania Urzędu w zakresie organizacji bezpieczeństwa informacji oraz zapewnienia ciągłości działania systemów informatycznych nie zawsze były prowadzone w sposób rzetelny. Prawidłowo zidentyfikowano zbiory danych podlegających zabezpieczeniu oraz opracowano i przyjęto do stosowania dokumentację składającą się na SZBI i POD, uwzględniającą wymogi odpowiednio rozporządzenia KRI i RODO. Właściwie określono oraz zapewniono niezbędne zasoby osobowe i techniczne w celu zapewnienia bezpieczeństwa informacji. Prowadzono także Analizę ryzyka w związku z potrzebą zachowania ciągłości działania systemów informatycznych, ustanowiono politykę ciągłości działania i Plan ciągłości działania oraz poddawano go testowaniu. Niemniej, powyższa analiza nie została zatwierdzona przez Burmistrza jako właściciela zidentyfikowanych w niej ryzyk, a plan zapewnienia ciągłości działania obejmował scenariusz związany z tylko jednym zagrożeniem, mimo zidentyfikowania sześciu w analizie ryzyka. Ponadto stwierdzone nieprawidłowości dotyczyły udostępnienia szczegółowych zasad zarządzania środowiskiem informatycznym wszystkim pracownikom Urzędu, nierzetelnej aktualizacji SZBI, gdyż dokumentacja ta zawierała nieaktualne zapisy oraz niesporządzenia regulacji wewnętrznych dotyczących pracy zdalnej, mimo takiego wymogu wprowadzonego w PBI-ZSI.

[58] Co zostało stwierdzone w trakcie oględzin z 25 czerwca 2024 r.
[59] Dz. U. z 2023 r. poz. 1465, ze zm.

OBSZAR

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

Opis stanu faktycznego

2.1. Przyjęte w Urzędzie rozwiązanie, polegające na nieprzyznawaniu użytkownikom uprawnień administracyjnych do systemu operacyjnego, zapobiegało możliwości instalowania nieautoryzowanego oprogramowania przez pracowników Urzędu na komputerach służbowych. Przeprowadzone w ramach oględzin[60] badanie dziesięciu komputerów wykazało, że żaden z testowanych użytkowników nie posiadał uprawnień do instalacji oprogramowania. Było to zgodne z § 19 ust. 2 pkt 4 rozporządzenia KRI.

Według wyjaśnień Burmistrza, na tabletach służbowych instalowane były administracyjne konta Google, do których dostępu nie mają użytkownicy sprzętu, wobec czego zablokowana była możliwość samodzielnej instalacji oprogramowania. Z kolei przyznane pracownikom służbowe telefony nie były przeznaczone do przetwarzania informacji – nie instalowano na nich aplikacji wykorzystywanych w Urzędzie.

(akta kontroli: str. 453-454, 456, 459)

2.2. Zgodnie z procedurą nadawania, odbierania i modyfikacji uprawnień w systemach informatycznych, zawartą w PBI-ZSI, uprawnienia do poszczególnych obszarów przetwarzania nadawał ADO, a stosowny wniosek (w formie papierowej) kierowany był przez kierownika komórki organizacyjnej do IOD oraz ASI.

Badanie losowo wybranej próby 15 pracowników Urzędu (na łącznie 65 pracowników uczestniczących w procesie przetwarzania informacji) wykazało, że uprawnienia tych pracowników w systemach informatycznych nie wykraczały poza zakres określony w zakresach obowiązków służbowych. Dla każdego pracownika sporządzono wniosek o nadanie uprawnień, zatwierdzony przez: przełożonego pracownika, ASI, IOD i ADO. Poza dwoma przypadkami, wskazane we wnioskach systemy informatyczne były zgodne z systemami, do których nadano pracownikowi uprawnienia[61]. W czterech przypadkach z kolei wskazano we wniosku jeden z badanych systemów, jednak bez określenia konkretnych jego modułów do których miał być uzyskany dostęp. Powyższe zostało szerzej opisane w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli: str. 169, 402-410)

2.3. W okresie objętym kontrolą, pracę w Urzędzie zakończyło 13 pracowników. Wnioski o odebranie im uprawnień w systemach informatycznych sporządzone zostały w terminie do trzech dni po zakończeniu zatrudnienia[62]. Niemniej, oględziny[63] trzech systemów i usługi AD wykazały, że konta ośmiu byłych pracowników pozostawały aktywne, o czym więcej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli: str. 384-385, 402-404, 411)

2.4. Obowiązujące w Urzędzie zasady nadawania haseł, zawarte w PBI-ZSI, wprowadzały dla nich wymagania określające minimalną liczbę znaków oraz ich złożoność.

W ramach oględzin trzech systemów i usługi Active Directory[64] stwierdzono, że w jednym z systemów[65] wymagania dla haseł dostępu określały długość hasła na

[60] Z 8 lipca 2024 r.
[61] Co stwierdzono na podstawie oględzin z 26 czerwca 2024 r.
[62] W dwóch przypadkach nie sporządzano przedmiotowego wniosku, gdyż osoby te nie wykonywały zadań w systemach informatycznych.
[63] Z 26 czerwca 2024 r.
[64] Dalej: AD.
[65] Służącym do elektronicznego obiegu dokumentów.

mniejszą niż wymagana PBI-ZSI liczba znaków, o czym szerzej w sekcji *Stwierdzone nieprawidłowości*.

Identyfikatory (loginy) użytkowników w wyżej wymienionych systemach miały formę imienną, poza kontami administracyjnymi, użytkowanymi wyłącznie przez informatyków.

(akta kontroli: str. 172, 400-401)

2.5. Oględziny[66] pięciu stanowisk obsługi klienta[67] wykazały, że monitory usytuowane były w sposób uniemożliwiający wgląd do wyświetlanych danych przez osoby nieuprawnione. Powyższe spełniało wymogi § 19 ust. 2 pkt 7 rozporządzenia KRI.

(akta kontroli: str. 453-454)

2.6. W Urzędzie opracowano zasady korzystania ze służbowych komputerów przenośnych poza miejscem pracy, które stanowiły załącznik do PBI, co było zgodne z § 19 ust. 2 pkt 8 rozporządzenia KRI. Pracownicy byli zobowiązani do potwierdzenia zapoznania się z nimi poprzez złożenie podpisu na dokumencie.

Zgodnie z powyższymi zasadami, pracownicy m.in. nie mogli przechowywać prywatnych danych na komputerach oraz mieli zakaz korzystania z publicznych sieci Wi-Fi. Zasady te nie zawierały natomiast uregulowań związanych z pracą zdalną, o których mowa w pkt 1.13 niniejszego wystąpienia pokontrolnego.

(akta kontroli: str. 158, 162)

2.7. Zgodnie z wyjaśnieniami Burmistrza, komputery przenośne były zabezpieczone przed dostępem osób nieuprawnionych poprzez oprogramowanie szyfrujące dyski twarde oraz indywidualny login i hasło przypisane do użytkownika.

(akta kontroli: str. 455-456, 459)

2.8. Serwerownia Urzędu zlokalizowana była w odrębnym, klimatyzowanym pomieszczeniu, do którego dostęp mieli informatycy, a wejścia były rejestrowane. Posiadała ona wydzieloną instalację elektryczną oraz systemy zabezpieczeń dostępu. Niemniej, pomieszczenie to użytkowano w sposób mogący powodować zagrożenie pożarowe, o czym szerzej w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli: str. 396-399)

2.9. W okresie objętym kontrolą obowiązywało osiem umów zawartych przez Urząd na zakup lub serwis sprzętu informatycznego i oprogramowania. Szczegółowe badanie czterech z nich wykazało, że w dwóch umowach nie zawarto zapisów gwarantujących zachowanie odpowiedniego poziom bezpieczeństwa informacji, co opisano w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli: str. 412-452)

2.10. Nie opracowano w Urzędzie formalnej procedury dotyczącej przekazywania sprzętu informatycznego poza jednostkę, określającej postępowanie służb informatycznych w sytuacji wydania urządzeń komputerowych zewnętrznemu serwisowi lub jego zbycia. Jak wyjaśnił Burmistrz, sytuacje takie są bardzo rzadkie (sprzęt IT nie jest wysyłany do zewnętrznego serwisu), a w przypadku, gdy mają miejsce – z przekazywanego sprzętu usuwane są wszelkie dane, poprzez wyjmowanie z urządzeń nośników pamięci (dysków twardych).

(akta kontroli: str. 456, 459-460)

2.11. Zasady stanowiące politykę kopii zapasowych zostały opisane w PBI-ZSI. Określały one sposób archiwizacji danych (tworzenia kopii zapasowych), miejsce

[66] Z 8 lipca 2024 r.

[67] Czterech w Wydziale Urząd Stanu Cywilnego i Ewidencja Ludności oraz jednego w Wydziale Organizacyjnym – Biurze Obsługi Klienta.

i okres ich przechowywania oraz osoby mające do nich dostęp. Ponadto określono sposób postępowania z nośnikami wyłączonymi z użytkowania i zasady testowania kopii bezpieczeństwa.

(akta kontroli: str. 172-174)

2.12. W toku oględzin[68] ustalono, że kopie zapasowe danych tworzone były zgodnie z zasadami, określonymi w PBI-ZSI, tj. codziennie w sposób automatyczny, na serwery archiwizacyjne (macierze dyskowe), z czego jeden znajdował się w pomieszczeniu serwerowni, a drugi poza tym pomieszczeniem. Służące do tego celu oprogramowanie automatycznie przeprowadzało test poprawności wykonanej kopii. Przeprowadzony w trakcie oględzin test na odzyskiwanie danych z wybranej kopii zapasowej[69] zakończył się poprawnym przywróceniem danych.

Serwer archiwizacyjny przechowywany poza pomieszczeniem serwerowni nie został jednak należycie zabezpieczony przed dostępem osób nieupoważnionych, o czym szerzej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli: str. 396-399)

2.13. W Urzędzie nie przyjęto formalnej procedury monitorowania pojemności nośników pamięci masowych, wykorzystywanych w serwerach. W toku oględzin[70] ustalono, że posiadane oprogramowanie umożliwiało taki monitoring w sposób automatyczny, jednak nie było ono wykorzystywane przez informatyków. Według oświadczenia Informatyka Urzędu, ze względów praktycznych, prowadzili oni ręczne monitorowanie dysków. Przeprowadzony w trakcie oględzin test zajętości dysków twardych na trzech serwerach wykazał, że zajętość wynosiła odpowiednio 5,7%, 69,7% i 90,7%. Jak wyjaśnił Burmistrz, serwer na którym zajętość wynosiła 90,7% był najstarszym serwerem w Urzędzie, przeznaczonym do wyłączenia. Służył on wyłącznie do przechowywania plików roboczych pracowników, które nie są strategiczne dla ciągłości działania Urzędu, a ilość danych na tym serwerze podlegała dynamicznym zmianom.

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

(akta kontroli: str. 396-399, 457, 461)

2.14. W ramach zapewnienia ciągłości działania Urzędu zidentyfikowano[71] kluczowe elementy infrastruktury IT oraz kluczowe usługi IT, wykorzystywane w jednostce. Informacje te zostały wykorzystane do testowania Planu ciągłości działania, przeprowadzonego 15 września 2023 r. W wyniku tego testu określono czas przywrócenia poszczególnych systemów oraz procesów do działania, który wyniósł od pięciu do 30 minut.

(akta kontroli: str. 352-357)

Stwierdzone nieprawidłowości

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

1. Według stanu na 26 czerwca 2024 r. dwóch pracowników (na 15 objętych badaniem) posiadało dostęp do systemu informatycznego, którego nie wskazano we wniosku o nadanie im dostępu. Ponadto we wnioskach o nadanie dostępu dla czterech pracowników wskazano system bez określenia jego konkretnych modułów. Było to niezgodne z § 19 ust. 2 pkt 4 rozporządzenia KRI, zgodnie

[68] Z 25 czerwca 2024 r.
[69] Baza danych systemu dziedzinowego z 1 kwietnia 2024 r.
[70] Z 25 czerwca 2024 r.
[71] Co zostało udokumentowane analizą z 7 czerwca 2023 r.

z którym należy zapewnić, by osoby zaangażowane w proces przetwarzania informacji posiadały stosowne uprawnienia.

Burmistrz wyjaśnił, że omyłkowo nie wpisano poszczególnych systemów we wnioskach dla wskazanych pracowników i dokonano już aktualizacji tych wniosków.

(akta kontroli: str. 402-410, 456, 461)

2. Nie dokonano zablokowania/usunięcia kont w systemach informatycznych Urzędu ośmiu (na łącznie 13) pracowników, którzy zakończyli zatrudnienie w okresie objętym kontrolą[72]. Konta te pozostawały aktywne, mimo złożenia wniosków o odebranie uprawnień powyższym pracownikom. Było to niezgodne z § 19 ust. 2 pkt 5 rozporządzenia KRI.

Według wyjaśnień Burmistrza, konta nie zostały wyłączone z uwagi na duże obłożenie pracą informatyków. Burmistrz dodał, że z uwagi na to, iż są to systemy lokalne, do wskazanych systemów pracownicy mogli zalogować się tylko na sprzęcie informatycznym zlokalizowanym w Urzędzie.

Powyższe konta zostały zablokowane w trakcie dokonywania oględzin 26 czerwca 2024 r.

(akta kontroli: str. 402-404, 456, 460)

3. W jednym z trzech sprawdzanych systemów informatycznych Urzędu, ustalone wymagania dla haseł dostępu określały długość hasła na mniejszą liczbę znaków niż określona w PBI-ZSI jako minimalna. Umożliwiało to stosowanie nieadekwatnych haseł dostępu do systemu w odniesieniu do istotności ochrony informacji i było niezgodne z § 19 ust. 2 pkt 7 lit. c rozporządzenia KRI.

Burmistrz wyjaśnił, że wymagania dla haseł określone w przedmiotowym systemie zostały zaprojektowane przez jego producenta. Jednocześnie Burmistrz przyznał, że było to niezgodne z PBI-ZSI i zostało już zmienione.

(akta kontroli: str. 400-401, 457, 461)

4. Pomieszczenie serwerowni było użytkowane w sposób niezapewniający odpowiedniego poziomu ochrony przeciwpożarowej, z uwagi na przechowywanie w nim pudeł z kartonu, będącego materiałem łatwopalnym. Było to niezgodne z § 19 ust. 2 pkt 9 rozporządzenia KRI i nie spełniało zaleceń określonych w pkt 11.2.1 Polskiej Normy PN-ISO/IEC 27002.

Według wyjaśnień Burmistrza, w kartonowych pudłach znajdował się nowy sprzęt teleinformatyczny, który zostanie w najbliższym czasie rozdysponowany według zapotrzebowania.

NIK zwraca uwagę, że pomieszczenie serwerowni powinno być użytkowane w sposób minimalizujący ryzyko zniszczenia informacji przechowywanych na serwerach, wobec czego nie powinno być wykorzystywane w celach magazynowych, szczególnie z użyciem materiałów łatwopalnych, takich jak karton.

(akta kontroli: str. 396-399, 457, 461)

5. W dwóch umowach serwisowych[73] (na cztery objęte badaniem), podpisanych z podmiotami zewnętrznymi, nie zawarto zapisów gwarantujących zachowanie odpowiedniego poziomu bezpieczeństwa informacji, co było niezgodne z § 19 ust. 2 pkt 10 rozporządzenia KRI.

[72] Według ustaleń oględzin z 26 czerwca 2024 r.

[73] Umowy nr: [1] 15/04/2021 z 28 kwietnia 2021 r. na aktualizację oprogramowania PKZP wraz z usługami serwisowymi i [2] 2/VII/2022/ZIF z 6 lipca 2022 r. na dostawę sprzętu z oprogramowaniem.

Burmistrz wyjaśnił, że nie znajdowano uzasadnienia, aby w umowach zawierać zapisy określające poziom bezpieczeństwa informacji, gdyż umowa nr 15/04/2021 dotyczyła jedynie zakupu licencji na oprogramowanie, które jest lokalne i w żaden sposób nie łączy się, ani nie przekazuje danych do producenta, który przygotowuje jedynie pliki aktualizacyjne. Natomiast umowa nr 2/VII/2022/ZIF z 6 lipca 2022 r. dotyczyła jedynie dostawy sprzętu wraz z oprogramowaniem, a wszelkie serwisy oraz naprawy w ramach gwarancji przewiduje się wykonywać w siedzibie Urzędu, a gdyby z jakiegoś powodu koniecznym było przekazanie sprzętu na zewnątrz, byłby on przekazany bez nośników danych.

NIK zwraca uwagę, że wymóg zawierania w umowach przedmiotowych zapisów określony jest w przepisach prawa, które Urząd zobowiązany jest przestrzegać. Ponadto wskazać należy, że pracownik zewnętrzny w czasie napraw gwarancyjnych bądź opieki autorskiej może mieć dostęp do danych także w siedzibie Urzędu i nie wyklucza to złamania obowiązujących w nim zasad bezpieczeństwa informacji oraz powstania szkody lub naruszenia poufności aktywów informacyjnych.

(akta kontroli: str. 413-428, 457, 461-462)

6. Serwer archiwizacyjny (macierz dyskowa), na którym przechowywane były kopie zapasowe danych Urzędu, nie został należycie zabezpieczony przed dostępem osób nieupoważnionych, gdyż znajdował się on bezpośrednio na biurku w pomieszczeniu informatyków, do którego dostęp posiadali inni pracownicy Urzędu. Nie zapewniono tym samym odpowiedniej ochrony danych przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, co było niezgodne z § 19 ust. 2 pkt 7 rozporządzenia KRI.

Jak wyjaśnił Burmistrz, przedmiotowy serwer znajdował się w pomieszczeniu informatyków tymczasowo, z uwagi na przeprowadzanie koniecznej rekonfiguracji i konserwacji. Standardowo znajduje się on w pomieszczeniu, które jest odpowiednio zabezpieczone przed dostępem osób nieupoważnionych, a zmiana lokalizacji na czas konserwacji była spowodowana tymczasowym ograniczeniem dostępu do tamtego pomieszczenia.

Zdaniem NIK, nawet w sytuacji tymczasowego przechowywania serwera w miejscu innym niż docelowe, należało zapewnić jego ochronę przed dostępem osób nieuprawnionych.

(akta kontroli: str. 396-399, 485-486)

OCENA CZĄSTKOWA

Wdrożone i wykorzystywane w Urzędzie rozwiązania organizacyjne i techniczne nie zapewniały w pełni bezpieczeństwa informacji. Prawidłowo zidentyfikowane zostały kluczowe elementy infrastruktury i usługi IT, a Urząd zapewnił właściwe rozwiązania zapobiegające możliwości instalacji nieautoryzowanego oprogramowania na urządzeniach służbowych oraz uniemożliwiające dostęp do danych na urządzeniach mobilnych.

Pomieszczenie serwerowni było jednak wykorzystywane w sposób niezapewniający odpowiedniej ochrony przeciwpożarowej, mimo stosowania w nim zabezpieczeń fizycznych w celu ochrony przeciwwłamaniowej i przeciwpożarowej.

Ustalono zasady tworzenia i przechowywania kopii zapasowych, które były tworzone regularnie i poddawane testowaniu. Niemniej, nie zabezpieczono w wystarczający sposób nośników danych, na których przechowywane były kopie zapasowe.

Nadawanie i odbieranie uprawnień pracownikom do pracy w systemach informatycznych odbywało się w oparciu o wdrożoną w Urzędzie procedurę, jednak w dwóch przypadkach pracownicy mieli dostęp do systemów informatycznych bez

stosownego upoważnienia, a w czterech przypadkach nie wskazano, do którego modułu systemu dziedzinowego pracownik posiadał upoważnienie. Ponadto, nie zablokowano kont w systemach informatycznych ośmiu pracowników, którzy zakończyli zatrudnienie w Urzędzie.

Pozostałe stwierdzone nieprawidłowości dotyczyły niewystarczających wymogów dla haseł w jednym z systemów informatycznych oraz braku w dwóch umowach serwisowych zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

OBSZAR

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

3.1. Zgodnie z przyjętą Procedurą zarządzania ryzykiem, w 2023 r. przeprowadzono w Urzędzie coroczną analizę ryzyka bezpieczeństwa informacji, zatwierdzoną przez Burmistrza 31 października 2023 r. Na ww. analizę składały się: [1] arkusze identyfikacji ryzyka w komórce organizacyjnej, zawierające realizowane przez daną komórkę zadania, zidentyfikowane ryzyka oraz zastosowane środki organizacyjne i techniczne wprowadzone w celu minimalizacji tego ryzyka i utraty bezpieczeństwa informacji oraz [2] arkusze identyfikacji oceny ryzyka bezpieczeństwa informacji w poszczególnych komórkach organizacyjnych Urzędu, w których wskazano: 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. 195-203, 297-320)

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

Według wyjaśnień Burmistrza, w okresie objętym kontrolą nie wystąpiły incydenty w zakresie bezpieczeństwa informacji.

(akta kontroli: str. 183-190, 342-344)

3.3. W Urzędzie przeprowadzano szkolenia z ochrony danych osobowych i bezpieczeństwa informacji dla każdego nowozatrudnionego pracownika Urzędu. W okresie objętym kontrolą przeprowadzono 11 takich szkoleń, prowadzonych przez IOD, a ich zakres tematyczny obejmował m.in.: [1] podstawowe pojęcia z zakresu ochrony danych, [2] role i obowiązki ADO, IOD i ASI, [3] podstawy przetwarzania danych, [4] naruszenia ochrony danych i obowiązek ich zgłaszania, [5] wewnętrzne regulacje dotyczące ochrony danych, w tym POD i SZBI, [6] środki techniczne i organizacyjne służące bezpieczeństwu informacji. Spełniało to warunki określone w § 19 ust. 2 pkt 6 rozporządzenia KRI.

Ponadto, 13 czerwca 2024 r. przeprowadzono[74] szkolenie z zakresu ochrony danych osobowych i bezpieczeństwa informacji dla wszystkich pracowników Urzędu.

(akta kontroli: str. 72, 342-345, 358-375)

[74] Przez IOD i ASI.

3.4. W okresie objętym kontrolą nie przeprowadzono okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji, o czym szerzej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli: str. 69, 72-73, 239-249)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:

Nie przeprowadzono w 2023 r. okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji, co było niezgodne z § 19 ust. 2 pkt 14 rozporządzenia KRI, zgodnie z którym kierownictwo podmiotu powinno zapewnić przeprowadzenie takiego audytu nie rzadziej niż raz na rok. Ostatni audyt w ramach realizacji powyższego obowiązku został przeprowadzony od 1 do 8 lipca 2022 r.
Jak wyjaśnił Burmistrz, w związku z planami przystąpienia do projektu „Cyberbezpieczny Samorząd", zakładano przeprowadzenie powyższego audytu w ramach tego projektu, gdyż pierwotny termin składania wniosków przypadał na 30 września 2023 r. W związku z kolejnymi przesunięciami terminu na złożenie wniosku, nie udało się tego zamierzenia zrealizować w 2023 r.

NIK wskazuje, że obowiązek przeprowadzenia przedmiotowego audytu wynika z przepisów prawa i jego realizacja nie może być uzależniona od udziału w projektach związanych z pozyskaniem środków zewnętrznych.

(akta kontroli: str. 69, 72-73, 239-249, 343, 348)

OCENA CZĄSTKOWA

W Urzędzie w sposób rzetelny prowadzono okresowe analizy ryzyka utraty integralności, poufności oraz dostępności informacji, wdrożono procedurę postępowania w sytuacjach wystąpienia lub podejrzenia incydentu w zakresie bezpieczeństwa informacji, a także zapewniono szkolenia pracowników zaangażowanych w proces przetwarzania informacji. Niemniej, nie przeprowadzono w 2023 r. okresowego, corocznego audytu wewnętrznego z zakresu bezpieczeństwa informacji.

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 i 2 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych[75], 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. Zapewnienie pisemnego zatwierdzania przez Burmistrza przeprowadzanych w Urzędzie analiz ryzyka wykonanych w związku z potrzebą zachowania ciągłości działania.
2. Zapewnienie uwzględnienia w Planie ciągłości działania, scenariuszy obejmujących wszystkie zidentyfikowane krytyczne (o wysokim poziomie ryzyka) zagrożenia ciągłości działania.
3. Zapewnienie udostępniania informacji o szczegółowych zasadach zarządzania środowiskiem informatycznym tylko upoważnionym w tym zakresie pracownikom.

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

4. Zaktualizowanie dokumentacji składającej się na SZBI w zakresie zmieniającego się otoczenia.
5. Zapewnienie wprowadzenia wewnętrznych regulacji dotyczących pracy zdalnej w Urzędzie, stosownie do wymagań PBI-ZSI.
6. Usunięcie z serwerowni materiałów łatwopalnych, w tym kartonowych pudeł.
7. Zawieranie w umowach serwisowych zapisów gwarantujących zachowanie odpowiedniego poziomu bezpieczeństwa informacji.
8. Przechowywanie nośników danych z kopiami zapasowymi w sposób zapewniający odpowiednią ochronę danych przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami.
9. Zapewnienie przeprowadzania audytu wewnętrznego z zakresu bezpieczeństwa informacji co najmniej raz na rok.

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 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 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.

Wrocław, 12 sierpnia 2024 r.

Najwyższa Izba Kontroli
Delegatura we Wrocławiu
p.o. Dyrektor
Marcin Kaliński

Kontroler
Piotr Kociołek
Starszy inspektor kontroli państwowej

..... *podpis*

..... *podpis*