NAJWYŻSZA IZBA KONTROLI
DELEGATURA W KATOWICACH

LKA.410.14.5.2024

Pani
Katarzyna Zyga
Wójt
Gminy Zbrosławice

Urząd Gminy Zbrosławice
ul. Oświęcimska 2
42-674 Zbrosławice

WYSTĄPIENIE POKONTROLNE

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

I. Dane identyfikacyjne

Jednostka kontrolowana

Urząd Gminy Zbrosławice[1], 42-674 Zbrosławice, ul. Oświęcimska 2.

Kierownik jednostki kontrolowanej

Katarzyna Zyga, Wójt Gminy, od 7 maja 2024 r.

W okresie objętym kontrolą funkcję kierownika jednostki poprzednio pełnił Wiesław Olszewski, Wójt Gminy Zbrosławice, od 19 listopada 2018 r. do 6 maja 2024 r.

Zakres przedmiotowy kontroli

Rozwiązania organizacyjne i techniczne w zakresie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego.

Okres objęty kontrolą

Od 1 stycznia 2023 r. do dnia zakończenia kontroli w 2024 r., tj. do dnia 4 września 2024 r. (także za okresy wcześniejsze w zakresie uczestnictwa w programie Cyfrowa Gmina).

Podstawa prawna podjęcia kontroli

Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[2]

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli
Delegatura w Katowicach

Kontrolerzy

1. Lucyna Mol, Główny specjalista kontroli państwowej, upoważnienie do kontroli nr LKA/124/2024 z 5 czerwca 2024 r.
2. Szymon Gruca, Główny specjalista kontroli państwowej, upoważnienie do kontroli nr LKA/165/2024 z 24 lipca 2024 r.

(akta kontroli str. 1-8)

[1] Dalej*: Urząd*.

[2] Dz. U. z 2022 r. poz. 623, dalej: ustawa o NIK.

II. Ocena ogólna[3] kontrolowanej działalności

OCENA OGÓLNA

W Urzędzie podejmowano działania mające na celu zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych.

Przyjęto i wdrożono system zarządzania bezpieczeństwem informacji wraz z dokumentami składającymi się na ten system, w tym politykę bezpieczeństwa informacji, instrukcję zarządzania systemem informatycznym, plan ciągłości działania oraz zasady pracy zdalnej. Zidentyfikowano kluczowe elementy infrastruktury IT oraz nadano im poziom wrażliwości. Powołanemu Inspektorowi Ochrony Danych Osobowych[4] zagwarantowano niezależne wykonywanie obowiązków. Administratorowi Systemów Informatycznych[5] przypisano odpowiedzialność za zapewnienie bezpieczeństwa informacji oraz ciągłości działania. Wyznaczono także osobę do utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Pracowników Urzędu zapoznano z procedurami składającymi się na system zarządzania bezpieczeństwem informacji, zapewniono im także szkolenia z zakresu ochrony danych osobowych oraz szkolenie z zakresu cyberbezpieczeństwa. Przeprowadzono audyt z zakresu bezpieczeństwa informacji. W celu poprawy cyberbezpieczeństwa, Urząd przystąpił do programu „Cyberbezpieczny Samorząd".

Pracownikom uniemożliwiono instalację na komputerach dowolnego oprogramowania. Usytuowanie monitorów na stanowiskach pracy uniemożliwiało wgląd do danych przez osoby nieuprawnione. Pomieszczenie serwerowni było zabezpieczone w sposób ograniczający ryzyko nieuprawnionego dostępu z zewnątrz. W umowach na serwis i dostawę urządzeń ujmowano zapisy dotyczące zachowania poufności informacji uzyskanych w związku z realizacją umów. Przeprowadzono, w okresie objętym kontrolą, kilkukrotne testowanie odtwarzania kopii zapasowych. Prawidłowo odtworzono również kopie zapasowe podczas badania realizowanego przy udziale NIK.

Stwierdzone w toku kontroli nieprawidłowości dotyczyły m.in.:

- wdrożenia regulacji istotnych dla systemu bezpieczeństwa informacji dopiero po dziesięciu miesiącach od otrzymania rekomendacji audytora w tym zakresie, tj.: wykazu systemów informatycznych z określonym poziomem krytyczności, wykazu usług i elementów infrastruktury istotnej z punktu widzenia zachowania ciągłości działania, procedur dotyczących kopii zapasowych obejmujących m.in. ich przechowywanie i częstotliwość ich sporządzania, regulacji wewnętrznych związanych z systemem dostępu do pomieszczeń Urzędu, co było niezgodne z §19 ust. 1 i ust. 2 pkt 1 rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[6] i nierzetelne;
- przechowywania kopii zapasowych w miejscu wytwarzania danych, co było niezgodne z §19 ust. 2 pkt 12 lit. b i e rozporządzenia KRI;
- niedokonania bezzwłocznego blokowania dostępu do systemów informatycznych ośmiu spośród 15 objętych badaniem pracowników, którzy zakończyli pracę w Urzędzie co było niezgodne z §19 ust. 2 pkt 5 rozporządzenia KRI;

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

[4] Dalej: *IODO*.

[5] Dalej: *ASI*.

[6] Dz.U. z 2024 r. poz. 773, dalej: rozporządzenie KRI.

– rezygnacji z wymuszenia okresowej zmiany haseł w odniesieniu do dwóch z trzech objętych badaniem programów komputerowych, pomimo przyjętych regulacji wewnętrznych w tym zakresie.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[7] kontrolowanej działalności

OBSZAR

1. Organizacja bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych

Opis stanu faktycznego

1.1 W Urzędzie zidentyfikowano kategorie danych, które były przez Urząd przetwarzane[8]. W Urzędzie opracowano także wykaz programów stosowanych do przetwarzania danych osobowych[9].W wykazie tym nie przypisano programom poziomu ochrony (wrażliwości i krytyczności). Do 30 września 2023 r. w Urzędzie nie zidentyfikowano usług i elementów infrastruktury istotnych z punktu widzenia zachowania ciągłości działania krytycznych systemów informatycznych.

19 stycznia 2023 r. audytor przedstawił sprawozdanie z przeprowadzenia zadania audytowego: audyt bezpieczeństwa informacji zapewnienie ciągłości działania systemów teleinformatycznych. Jednym z celów zadania była identyfikacja dobrych praktyk oraz słabości systemowych w celu przedstawienia uwag i wniosków usprawniających zarządzanie ciągłością działania systemów teleinformatycznych. Jako zalecenie audytor przedstawił m.in.: sporządzenie wykazu systemów informatycznych, z określonym poziomem ich krytyczności; sporządzenie wykazu usług i elementów infrastruktury istotnych z punktu widzenia zachowania ciągłości działania krytycznych systemów informatycznych; rozważenie opracowania listy zdarzeń powodujących przerwy w ciągłości działania, opracowanie zasad przechowywania kopii zapasowych w innej lokalizacji oraz częstotliwości wykonywania tych kopii. Audytor rekomendował także wprowadzenie w planie ciągłości działania systemu dostępu do pomieszczeń.

Wykaz systemów, usług elementów infrastruktury teleinformatycznej wykorzystywanych do realizacji zadań i usług publicznych wraz z przypisaniem stopnia krytyczności, wykaz zdarzeń powodujących przerwy w ciągłości działania oraz procedury dotyczące kopii zapasowych opracowano na podstawie zaktualizowanego planu ciągłości działania, wprowadzonego zarządzeniem Wójta z 30 listopada 2023 r.[10] System dostępu do pomieszczeń uregulowany został zarządzeniem Wójta z 29 listopada 2023 r.[11] Dokumenty te stanowiły realizację rekomendacji poaudytowych przedstawionych Wójtowi 19 stycznia 2023 r., tj. odpowiednio 314 i 313 dni po otrzymaniu zaleceń, co opisano w sekcji *stwierdzone nieprawidłowości*.

(akta kontroli str. 58-59, 82-86, 136-138, 383-385, 443-446)

1.2 W Urzędzie opracowano, ustanowiono i wdrożono politykę bezpieczeństwa informacji oraz instrukcję zarządzania systemem informatycznym[12]. Dokumenty te przedstawione zostały do zapoznania się i stosowania wszystkim pracownikom.

[7] 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.

[8] Opisane w rejestrze czynności przetwarzania. Dokument wprowadzony zarządzeniem nr OR.0050.99.2019 z 8 kwietnia 2019 r.

[9] Wykaz stanowił załącznik nr 2 do polityki bezpieczeństwa informacji wprowadzonej zarządzeniem nr OR.0050.493.2018 z 17 grudnia 2018 r.

[10] Nr. OR.0050.373.2023.

[11] Nr OR.120.6.2023.

[12] Zarządzeniem nr OR.0050.493.2018 Wójta Gminy Zbrosławice z dnia 17 grudnia 2018 r.

Administrator Danych Osobowych[13] odpowiadał za przestrzeganie zasad ustanowionych w tych dokumentach oraz przeprowadzenie corocznego audytu bezpieczeństwa. Wprowadzony został także plan ciągłości działania[14], instrukcja postępowania z kluczami oraz zabezpieczenia pomieszczeń i budynków Urzędu[15]. Plan ciągłości działania nie przewidywał zapoznania z jego treścią wszystkich pracowników. Natomiast instrukcja postępowania z kluczami udostępniona została do zapoznania pracownikom. Instrukcja ta wprowadzona została 313 dni po otrzymaniu zaleceń poaudytowych.

(akta kontroli str. 22-61, 79, 89-96, 429-439)

1.3 W obszarze ochrony danych osobowych, poza zapisami polityki bezpieczeństwa informacji, wprowadzono także instrukcję postępowania w sytuacjach naruszenia ochrony danych osobowych[16], zasady przeprowadzania analizy ryzyka w obszarze ochrony danych osobowych[17] wzór rejestru wszystkich kategorii czynności przetwarzania[18] oraz rejestr czynności przetwarzania[19]. Instrukcja postępowania w sytuacjach naruszenia ochrony danych osobowych zakomunikowana została pracownikom Urzędu.

(akta kontroli str. 24-33, 64-75, 78-79, 82-86)

1.4 W wyniku zaleceń audytowych dokonano przeglądu i aktualizacji planu ciągłości działania[20]. Jako element planu wprowadzono wykaz systemów informatycznych, usług infrastruktury teleinformatycznej[21], a także wykaz zdarzeń powodujących przerwy w ciągłości działania[22]. W dokumentach tych określono m.in. poziom krytyczności zdarzeń/usług, ich wpływ na organizację oraz czas przywrócenia poszczególnych systemów. Określono także częstotliwość wykonywania kopii zapasowych.

(akta kontroli str. 58-62)

1.5 W Urzędzie nie opracowano dokumentu o nazwie „Polityka ciągłości działania". Opracowano natomiast i wdrożono plan ciągłości działania[23]. Dokument ten obejmował także działania odtworzeniowe.

(akta kontroli str. 46-61)

1.6 W okresie od 28 października 2019 r. do 29 listopada 2023 r. plan ciągłości działania wskazywał, że procedura określona w planie obejmuje wszystkie zasoby

---

[13] Dalej: *ADO*.

[14] Na podstawie zarządzenia nr OR.0050.323.2019 Wójta Gminy Zbrosławice z 28 października 2019 r. w sprawie wprowadzenia planu ciągłości działania w Urzędzie Gminy Zbrosławice, zastąpionego zarządzeniem nr OR.0050.373.2023 z dnia 30 listopada 2023 r.

[15] Na podstawie zarządzenia nr OR.120.6.2023 Wójta Gminy Zbrosławice z 29 listopada 2023 r. w sprawie wprowadzenia Instrukcji postępowania z kluczami oraz zabezpieczenia pomieszczeń i budynków Urzędu Gminy Zbrosławice.

[16] Na podstawie zarządzenia nr OR.0050.494.2018 Wójta Gminy Zbrosławice z dnia 17 grudnia 2018 r.

[17] Na podstawie zarządzenia nr OR.0050.481.2018 Wójta Gminy Zbrosławice z dnia 10 grudnia 2018 r. w sprawie przyjęcia zasad przeprowadzania analizy ryzyka w obszarze ochrony danych osobowych w Urzędzie Gminy Zbrosławice.

[18] Wprowadzony zarządzeniem nr OR.0050.99.2019 z 8 kwietnia 2019 r.

[19] Wprowadzony zarządzeniem nr OR.0050.167.2018 z 21 maja 2018 r.

[20] Wprowadzony zarządzeniem nr OR.0050.373.2023 z 30 listopada 2023 r.

[21] W dokumencie wskazano systemy informatyczne wraz z określeniem m.in. poziomu krytyczności usługi pod względem bezpieczeństwa, czasu przywrócenia systemu oraz częstotliwości wykonywania kopii zapasowych skali systemu i powiązania z innymi systemami.

[22] W dokumencie zidentyfikowano zewnętrzne i wewnętrzne czynniki powodujące przerwy w ciągłości dziania wraz z wpływem działania, stopniem krytyczności oraz potencjalnymi metodami likwidacji.

[23] Wprowadzony zarządzeniem nr OR.0050.323.2019 z 28 października 2019 r. i zastąpiony zarządzeniem OR.0050.373.2023 z 30 listopada 2023 r.

infrastruktury teleinformatycznej. Przy czym w planie nie określono jakimi zasobami dysponuje Urząd, a także nie ustalono akceptowalnego czasu przywrócenia ciągłości działania systemów informatycznych. W aktualizacji planu ciągłości działania obowiązującej od 30 listopada 2023 r., stanowiącej realizację zaleceń poaudytowych, wprowadzono wykaz systemów i usług elementów infrastruktury teleinformatycznej używanej do realizacji zadań wraz z przypisaniem danym systemom m.in. stopnia krytyczności oraz czasu niezbędnego do odtworzenia/przywrócenia systemu po awarii lub innego incydentu, a także częstotliwości wykonywania kopii zapasowych. Wskazano tryb organizacji lokalizacji zastępczej.

Naczelnik Wydziału Informatyki wskazał, że w aktualizacji planu ciągłości działania opisano funkcjonujące wcześniej mechanizmy, które nie zostały sformalizowane.

(akta kontroli str. 58-61, 442)

1.7 W okresie objętym kontrolą przeprowadzono trzy testy dotyczące ciągłości działania. Prowadzone testy polegały na próbie odzyskania kompletnego obrazu serwera, do osobnej maszyny wirtualnej oraz uruchomienie jej bez środowiska sieciowego. Testy przeprowadzone 8 sierpnia 2023 r. i 19 lutego 2024 r. nie wykazały błędów i nieprawidłowości. Podczas testowania prowadzonego od 25 czerwca do 27 czerwca 2024 r. wystąpiły problemy z odtwarzaniem. Po zmianie konfiguracji przeprowadzono dalsze testy, pozytywnie zakończone.

(akta kontroli str. 62-63)

1.8 Zapewniono aktualizację regulacji stanowiących element polityki bezpieczeństwa informacji. 30 listopada 2023 r. przyjęty został zaktualizowany plan ciągłości działania. Wprowadzono, także 29 listopada 2023 r. instrukcję postępowania z kluczami oraz zabezpieczenia pomieszczeń i budynków Urzędu. Dokumenty te wprowadzone zostały prawie rok po otrzymaniu rekomendacji audytowych wskazujących na słabości systemu bezpieczeństwa informacji.

W planie ciągłości działania stanowiącym załącznik do zarządzenia nr OR.0050.373.2023 z 30 listopada 2023 r. nie wskazano osób odpowiedzialnych za prawidłową i terminową realizację działań przewidzianych w tym planie[24], co opisano w sekcji *stwierdzone nieprawidłowości*.

(akta kontroli str. 52-61, 89-96, 362-385, 409)

1.9 W Urzędzie za bezpieczeństwo informacji oraz zapewnienie ciągłości działania odpowiedzialny był Naczelnik Wydziału Informatyki. Zgodnie z zakresem obowiązków[25], Naczelnik zobowiązany był m.in. do utrzymania sprawności i ciągłości działania systemów informatycznych oraz nadzoru nad cyberbezpieczeństwem systemów informatycznych Urzędu. Naczelnik miał niezbędne wykształcenie kierunkowe oraz uczestniczył w szkoleniach z zakresu informatyki i cyberbezpieczeństwa.

(akta kontroli str. 103-110)

1.10 W Urzędzie wyznaczono IODO[26], który miał odpowiednie kwalifikacje zawodowe do pełnienia tej funkcji. Do obowiązków IODO należało m.in. aktualizacja procedur realizacji obowiązków związanych z przetwarzaniem danych osobowych, dokonywanie oceny skutków przetwarzania danych osobowych pod kątem

[24] Obejmujących działania zapewniające przywrócenie zdolności realizacji działalności oraz częstotliwość testowania.

[25] Zakres obowiązków zaakceptowany przez Naczelnika 27 marca 2024 r. oraz poprzedzający go zakres obowiązków z 1 lutego 2018 r.

[26] Na podstawie zarządzenia nr OR.0050.226.2018 Wójta Gminy Zbrosławice z dnia 21 czerwca 2018 r.

związanego z nim ryzyka, monitorowanie przestrzegania RODO, zgłaszanie naruszenia bezpieczeństwa do organu nadzoru oraz osób, których dane dotyczą.

(akta kontroli str. 103, 111-120)

1.11 Zarządzeniem o wyznaczeniu IODO[27] ustalono jego bezpośrednią podległość Wójtowi Gminy, zgodnie z art. 38 ust. 3 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[28].

(akta kontroli str. 103)

1.12 Wójt Gminy 31 grudnia 2021 r. wyznaczył osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych realizowanych przez Urząd Gminy. Dane te przekazane zostały w terminie wynikającym z art. 22 ust. 1 pkt 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[29] do CSIRT NASK.

(akta kontroli str. 121, 388)

1.13 W Urzędzie opracowano plany, procedury i instrukcje, które wraz z polityką bezpieczeństwa informacji stanowiły system zarządzania bezpieczeństwem informacji. Dokumenty te obejmowały: instrukcję zarządzania systemem informatycznym, plan ciągłości działania, procedurę tworzenia kopii zapasowych, zasady przeprowadzania analizy ryzyka w obszarze danych osobowych, instrukcję dotycząca sposobu i trybu przetwarzania informacji niejawnych oznaczonych klauzulą „zastrzeżone" i „poufne", instrukcję postępowania w sytuacji naruszenia danych osobowych, instrukcję postępowania z kluczami oraz zabezpieczenia pomieszczeń i budynków Urzędu. Instrukcja postępowania z kluczami oraz zabezpieczenia pomieszczeń i budynków Urzędu oraz procedura tworzenia kopii zapasowych zbiorów danych oraz sposobu, miejsca i okresu przechowywania opracowane zostały po 313 dniach od otrzymania zaleceń audytowych w tym zakresie.

(akta kontroli str. 122, 461-462)

1.14 Na podstawie badania dziesięciu komputerów, jednego serwera, dwóch laptopów, routera i jednej drukarki stwierdzono[30], że jednostka posiada informacje o zasobach informatycznych, które obejmują m.in. ich rodzaj i konfigurację było to zgodne z §19 ust. 2 pkt 2 rozporządzenia KRI. Oprogramowanie inwentaryzujące zasoby informatyczne wykorzystywane przez Urząd monitorowało także aktywność w sieci oraz przypisanie danej osoby do konkretnego urządzenia. Naczelnik Wydziału Informatyki wyjaśnił, że zasoby informatyczne przypisano do osób, które korzystają z danego sprzętu, przy czym te osoby nie mają przypisanej formalnej odpowiedzialności za konkretny sprzęt. Odpowiedzialność/dbałość za mienie, w tym sprzętu Urzędu wynika z zakresu obowiązku pracowników.

(akta kontroli str. 123-142)

1.15 Urząd przystąpił do programu „Cyberbezpieczny Samorząd" realizowanego ramach Europejskiego Funduszu Rozwoju Regionalnego (EFRR), programu Fundusze Europejskie na Rozwój Cyfrowy (FERC)[31]. Umowa o powierzenie grantu

[27] §3 zarządzenia nr OR.0050.226.2018 Wójta Gminy Zbrosławice z dnia 21 czerwca 2018 r.

[28] Dz.Urz.UE.L 119 z 04.05.2016, str. 1, ze zm.

[29] Dz.U. z 2024 r. poz. 1077.

[30] Dobranych w sposób celowy według osądu kontrolera.

[31] W ramach naboru FERC.02.02-CS.01-001/23.

zawarta została 15 lipca 2024 r. Wartość projektu wynosiła 913,9 tys. zł, z tego dofinansowanie 840,8 tys. zł. Urząd zobowiązał się zrealizować projekt w terminie 24 miesięcy od zawarcia umowy, jednak nie dłużej niż do 30 czerwca 2026 r. W zakresie technicznym projektu przewidziano zakup m.in.: serwerów wraz z licencjami[32], macierzy dyskowej wraz z dyskami, biblioteki taśmowej, oprogramowania do realizacji kopii zapasowych, zasilania awaryjnego UPS dla serwerów, agregatu prądotwórczego, urządzenia UTM. W zakresie kompetencyjnym przewidziano szkolenia: z zakresu cyberbezpieczeństwa dla pracowników, systemu zarządzania bezpieczeństwem informacji dla kadry kierowniczej oraz dla administratora sieci.

Jak wyjaśnił Naczelnik Wydziału Informatyki, realizacja grantu w istotny sposób przyczyni się do poprawy cyberbezpieczeństwa Urzędu.

(akta kontroli str. 143-219, 411, 447-450)

Stwierdzone nieprawidłowości

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

1. Urząd do końca listopada 2023 r. nie zidentyfikował usług i elementów infrastruktury istotnych z punktu widzenia zachowania ciągłości działania oraz zdarzeń powodujących przerwy w ciągłości działania, nie opracował procedur związanych z kopiami zapasowymi m.in. w zakresie przechowywania i częstotliwości ich sporządzania, nie ustalił systemu dostępu do pomieszczeń Urzędu. Wdrożenie tych regulacji było objęte wnioskami audytora przedstawionymi Wójtowi 19 stycznia 2023 r. Zalecenia audytora, istotne z punktu widzenia systemu bezpieczeństwa informacji, zrealizowane zostały po upływie 313 dni od ich otrzymania, tj. wprowadzono dopiero 29 listopada 2023 r. instrukcję postępowania z kluczami oraz zabezpieczenia pomieszczeń i budynków Urzędu, a 30 listopada 2023 r. wprowadzono zaktualizowany plan ciągłości działania.

   (akta kontroli str. 52-63, 89-102, 362-385)

Zgodnie z §19 ust. 1 rozporządzenia KRI, podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. W myśl § 19 ust. 2 pkt 1 tego rozporządzenia zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.

(akta kontroli str. 52-61, 63)

Były Wójt Gminy nie przedstawił przyczyn ww. nieprawidłowości.

(akta kontroli str. 468)

2. Niewskazanie w planie ciągłości działania stanowiącym załącznik do zarządzenia nr OR.0050.373.2023 z 30 listopada 2023 r. osób odpowiedzialnych za prawidłową i terminową realizację działań przewidzianych w tym planie, co było działaniem nierzetelnym.

W planie ciągłości działania w pkt 6 – działania zapewniające przywrócenie zdolności realizacji działalności określono m.in. działania, czynności operacyjne, zasoby niezbędne do przywrócenia zdolności jednostki. W pkt 7.2 – częstotliwość testowania określono opis testu, częstotliwość, termin realizacji oraz oczekiwany wynik. W ww.

[32] Dla Urzędu, Gminnego Zespołu Obsługi Placówek Oświatowych, Gminnego Ośrodka Pomocy Społecznej.

punktach planu nie wskazano jednakże osób odpowiedzialnych za te czynności, mimo odniesienia w pkt 4.3 planu, że za prawidłowe i terminową realizację działań przewidzianych w planie odpowiedzialne są osoby wskazane w kolumnie „Odpowiedzialni".

(akta kontroli str. 53-56)

Były Wójt Gminy nie przedstawił przyczyn ww. nieprawidłowości.

(akta kontroli str. 468)

OCENA CZĄSTKOWA

W Urzędzie wdrożono politykę bezpieczeństwa informacji oraz dokumentację wykonawczą, w tym plan ciągłości działania. Jednakże aktualizacje dokumentacji wykonawczej opracowane zostały dopiero po 313 dniach po otrzymaniu rekomendacji audytu, wskazujących na słabości systemu bezpieczeństwa informacji.

OBSZAR

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

Opis stanu faktycznego

2.1 Na podstawie oględzin dziesięciu komputerów (trzech laptopów oraz siedmiu komputerów stacjonarnych) ustalono, że na wszystkich badanych komputerach niemożliwe było zainstalowanie oprogramowania testowego na kontach ich użytkowników. System wyświetlał monit o podanie hasła administratora. Było to zgodne z §19 ust. 2 pkt 12 lit. c rozporządzenia KRI.

(akta kontroli str. 220)

Naczelnik Wydziału Informatyki wyjaśnił, że telefony służbowe wykorzystywane są wyłącznie do rozmów, kontaktu tekstowego oraz wykonywania zdjęć podczas wizji lokalnych, nie są podłączone do wewnętrznej sieci Urzędu i nie są zabezpieczone w sposób systemowy przed instalacją dowolnego oprogramowania. Jak wskazał Naczelnik przy zatrudnieniu, wszyscy pracownicy składają oświadczenie i zobowiązują się do przestrzegania zasad dotyczących sprzętu służbowego, m.in. korzystania ze sprzętu IT oraz oprogramowania wyłącznie do wykonywaniem obowiązków pracowniczych, wykorzystywania jedynie legalnego oprogramowania pochodzącego od pracodawcy. Ponadto Naczelnik wyjaśnił, że Gmina udostępnia radnym służbowe tablety, które wykorzystywane są do udziału w sesjach oraz głosowania. Dystrybuowane dane są zabezpieczone indywidualnym dla każdego radnego loginem i hasłem, przekazywane dane nie są wrażliwe/poufne (mają status informacji publicznej).

W umowach na użyczenie tabletu zawarto zapisy o zobowiązaniu do nieinstalowania na tablecie żadnego oprogramowania, nie uruchamiania na tablecie oprogramowania innego, niż zainstalowane przez użyczającego.

(akta kontroli str. 12, 221-223, 442)

2.2 Analiza przyznawania uprawnień do systemów informatycznych przeprowadzona na próbie badawczej 15 pracowników Urzędu[33], wykonujących zadania w systemach informatycznych, wykazała że 12 spośród tych pracowników przyznano te uprawnienia na podstawie wniosków o nadanie uprawnień - zgodnie z realizowanymi czynnościami. Uprawnienia dla dwóch osób odpowiadały zakresowi realizowanych zadań, jednakże przyznane zostały bez formalnego wniosku o nadanie tych uprawnień określonego w załączniku nr 1 do instrukcji zarządzania systemem

[33] Według stanu na dzień oględzin: pięciu naczelników wydziałów, dwóch kierowników, jeden zastępca naczelnika, trzech inspektorów i czterech głównych specjalistów.

informatycznym. Natomiast jednej osobie przyznano uprawnienia do systemu informatycznego, które nie odpowiadały zakresowi obowiązków tego pracownika i nie zostały uwzględnione we wniosku o ich nadanie, co opisano w sekcji *stwierdzone nieprawidłowości*.

(akta kontroli str. 234-247)

2.3 Analiza blokowania dostępu do systemów informatycznych przeprowadzona na próbie 15 pracowników, którzy zakończyli pracę w Urzędzie w okresie objętym kontrolą wykazała, że:

- jeden z tych pracowników nie miał konta w systemie[34],
- konta czterech byłych pracowników w dniu oględzin były zablokowane, przy czym nie było możliwe ustalenie kiedy blokada konta została ustanowiona, ze względu na nadpisanie pliku dziennika zdarzeń na kontrolerze domeny,
- siedmiu pracownikom, po zakończeniu pracy zablokowano konta w terminach od 18 do 212 dni po zakończeniu pracy w Urzędzie, z tego trzem pracownikom zresetowano hasło w dniu złożenia wniosku o odebranie uprawnień, u dwóch nie było możliwe ustalenie czy przed zamknięciem konta dokonano resetu hasła, w dwóch przypadkach nie zostały złożone formalne wnioski o odebranie uprawnień[35].
- konta trzech byłych pracowników w dniu oględzin były nadal aktywne.

Powyższe opisano w sekcji *stwierdzone nieprawidłowości*.

(akta kontroli str. 234, 246, 407-411)

2.4 W ramach kontroli dokonano oględzin trzech systemów informatycznych[36], pod kątem wymagań dla haseł dostępu do tych systemów. Jeden z trzech objętych badaniem programów, gdzie logowanie odbywało się poprzez integrację z systemem do zarządzania zbiorem użytkowników w sieci, złożoność hasła oraz częstotliwość jego zmiany była wymuszana zgodnie z instrukcją zarządzania systemem informatycznym. Jeden z programów wymuszał złożoność hasła, natomiast nie wymuszał częstotliwości tej zmiany. Jeden nie wymuszał zarówno złożoności hasła[37], jak i częstotliwości jego zmiany określonej w instrukcji zarządzania systemem informatycznym. Powyższe opisano w sekcji *stwierdzone nieprawidłowości*.

Oględziny systemów nie wykazały nietypowych loginów tj. takich których w prosty sposób nie można przypisać do użytkownika.

(akta kontroli str. 248-249)

2.5 Usytuowanie monitorów na stanowiskach pracy realizujących zadania z wykorzystaniem aplikacji „Źródło" uniemożliwiało wgląd do danych przez osoby nieuprawnione, zgodnie z §19 ust. 2 pkt 7 rozporządzenia KRI.

(akta kontroli str. 250-252)

2.6 W Urzędzie, w okresie objętym kontrolą, obowiązywał regulamin/zasady wykonywania pracy zdalnej[38]. W regulaminie obowiązującym do 6 kwietnia 2023 r. określono m.in. że niedozwolone jest udostępnianie innym osobom danych służących o uwierzytelniania do systemów i/lub usług; korzystania z urządzeń, które nie zostały

[34] Osoba wykonująca zadania w ramach robót publicznych.

[35] Z tego nie został złożony wniosek o odebranie uprawnień byłemu Wójtowi.

[36] Tj. system elektronicznego obiegu dokumentów, kadrowo-płacowy i do prowadzenia rejestru mieszkańców i wyborców.

[37] Program nie ma takich funkcji.

[38] Przyjęty zarządzeniem nr OR.0050.325.2021 z 27 października 2021 r. i zastąpiony zarządzeniem nr OR.120.2.2023 z 7 kwietnia 2023 r.

zatwierdzone przez pracodawcę; udostępniania służbowego sprzętu lub sprzętu wykorzystywanego do realizowania zadań służbowych innym osobom. Pracownicy, którym przekazywano sprzęt informatyczny, na potrzeby pracy zdalnej, w protokole przekazania sprzętu zobowiązani byli do przestrzegania zaleceń bezpieczeństwa zawartych w tym regulaminie. W zasadach wykonywania pracy zdalnej obowiązujących od 7 kwietnia 2023 r. ujęto zapisy odnoszące się m.in. do kontroli przestrzegania wymogów bezpieczeństwa i ochrony informacji, w tym procedur ochrony danych osobowych[39]. Było to zgodne z §19 ust. 2 pkt 8 rozporządzenia KRI.

(akta kontroli str. 253-278, 317-327)

2.7 Zgodnie z wyjaśnieniem Naczelnika Wydziału Informatyki dane na dyskach komputerów przenośnych były szyfrowane, zabezpieczone loginem i hasłem, a użytkownicy mieli ograniczone konta.

(akta kontroli str. 12)

2.8 Pomieszczenie serwerowni było zabezpieczone w sposób ograniczający ryzyko nieuprawnionego dostępu z zewnątrz i wewnątrz. NIK zwraca jednakże uwagę, że obecne pomieszczenie przeznaczone na serwerownię może być niewystarczające do pełnienia tej funkcji ze względu na jego powierzchnię. Naczelnik Wydziału Informatyki wyjaśnił, że przy opracowaniu wniosku projektu „Cyberbezpieczny samorząd" zaplanowano utworzenie nowej serwerowni.

(akta kontroli str. 279-287, 409)

2.9 Na podstawie próby czterech umów obejmujących: serwis oprogramowania (dwie umowy) i dostawy urządzeń (dwie umowy), stwierdzono że umowach zawieranych z podmiotami zewnętrznymi zawarto zapisy dotyczące zachowania poufności informacji uzyskanych w związku z realizacją umowy. Powyższe było zgodne z §19 ust. 2 pkt 10 rozporządzenia KRI.

(akta kontroli str. 289-306)

2.10 W instrukcji zarządzania systemem informatycznym wskazano, że urządzenia, dyski lub inne informatyczne nośniki informacji, przeznaczone do napraw, gdzie wymagane jest zaangażowanie autoryzowanych podmiotów zewnętrznych, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez ADO lub ASI. Naczelnik Wydziału Informatyki wyjaśnił, że przy przekazywaniu sprzętu poza jednostkę, każdorazowo wymontowywano nośniki danych (dyski twarde) i przekazywany sprzęt nie zawierał żadnych danych.

(akta kontroli str. 44, 441)

2.11 Zasady tworzenia kopii zapasowych zbiorów danych i programów określono w części VII instrukcji zarządzania systemem informatycznym. Częstotliwość tworzenia kopii określono w załączniku nr 4 do planu ciągłości działania z 30 listopada 2023 r. Dostęp do kopii zapasowych miał ASI. Jak wyjaśnił Naczelnik Wydziału Informatyki kopie mają postać plików, które są automatycznie zastępowane przez mechanizm retencji. W przypadku baz danych i kopii na dysku USB, kopie są nadpisywane w sposób zautomatyzowany. Nośniki nie były niszczone. W okresie objętym kontrolą, w ramach planu ciągłości działania, przeprowadzono trzykrotne testowanie odtwarzania z kopii zapasowych.

Ponadto jak podał Naczelnik, przed wprowadzeniem planu ciągłości działania z 30 listopada 2023 r. funkcjonowały analogiczne procedury odnośnie do kopii

[39] Tj. kwestie komunikowania się z pracodawcą i innymi pracownikami przy użyciu służbowej poczty elektronicznej, korzystania z udostępnionych przez pracodawcę systemów informatycznych, stosowania środków organizacyjnych i technicznych niezbędnych do ochrony danych osobowych, przyjętych w organizacji (szyfrowanie, pseudonimizjację).

zapasowych, które ostatecznie zostały sformalizowane w ww. załączniku nr 4 do tego planu.

(akta kontroli str. 42-43, 63, 441-442)

2.12 Zapisy instrukcji zarządzania systemem informatycznym (część VII ust. 1) określały, że kopie zapasowe tworzy się w określonych systemach, w terminach stosownych do potrzeb. W załączniku nr 4 do planu ciągłości działania z 30 listopada 2023 r. określono częstotliwość tworzenia kopii zapasowych.

Na podstawie oględzin stwierdzono, że kopie zapasowe danych tworzone były zgodnie z częstotliwością określoną w załączniku nr 4 do planu ciągłości działania z 30 listopada 2023 r. Kopie obrazów maszyn wirtualnych (wykonywane codziennie) oraz kopia wykonana z poprzedniej kopii (tworzona raz w tygodniu) przechowywane były w pomieszczeniu serwerowni, tj. w miejscu wytwarzania danych. Kopie baz danych z systemu finansowego wykonywane były codziennie i zapisywane na urządzeniu umieszczonym w pomieszczeniu informatyków. Umieszczenie kopii zapasowych w serwerowni stanowiło naruszenie § 19 ust. 2 pkt 12 lit. b i e rozporządzenia KRI, co opisano w sekcji *stwierdzone nieprawidłowości*.

W ramach kontroli przeprowadzono próbne odzyskanie pliku z najstarszej kopii zapasowej. Odzyskany plik otworzył się prawidłowo.

(akta kontroli str. 62, 307-313)

2.13 Oględziny dwóch przestrzeni dyskowych serwera produkcyjnego wykazały, że zajętość miejsca na macierzach dyskowych wynosiła około 50%. Naczelnik Wydziału Informatyki wyjaśnił, że nie opracowano procedury dotyczącej monitorowania pojemności nośników pamięci, nie wdrożono także żadnych systemów monitorowania dostępnego miejsca na dyskach serwerów produkcyjnych. Natomiast jak wyjaśnił, na urządzeniach stosowanych do przechowywania kopii zapasowych ustawiono alarmy powodujące wysyłanie do administratora informacji po przekroczeniu 80% zajętości dysków.

(akta kontroli str. 314-316)

2.14 W ramach zapewnienia ciągłości działania Urzędu wprowadzonego 30 listopada 2023 r., ustalono wykaz systemów, usług elementów infrastruktury informatycznej używanej do realizacji zadań i usług publicznych oraz wykaz zdarzeń powodujących przerwy w ciągłości działania urzędu wraz z potencjalnymi metodami ich likwidacji. Określono także maksymalny czas przywrócenia poszczególnych systemów i procesów działania. Powyższe dokumenty wprowadzone zostały w wyniku realizacji rekomendacji audytowych.

(akta kontroli str. 58-61, 383-385)

Stwierdzone nieprawidłowości

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

1. Spośród 15 objętych próbą pracowników Urzędu uprawnienia do systemów informatycznych nadano:

a) jednemu pracownikowi w zakresie niezgodnym z zakresem realizowanych zadań i jednocześnie nie uwzględnionym w formalnym wniosku o nadanie tych uprawnień;

b) dwóm pracownikom z pominięciem formalnego wniosku określonego w części IV instrukcji zarządzania systemem informatycznym i załączniku nr 1 do tej instrukcji;

co było niezgodne z §19 ust. 2 pkt 4 rozporządzenia KRI oraz z częścią IV instrukcji zarządzania systemem informatycznym i załącznikiem nr 1 do tej instrukcji.

Naczelnik Wydziału Informatyki wyjaśnił, że udzielenie dostępu dwóm pracownikom nadane zostało na podstawie polecenia ustnego, w tym w jednym z tych przypadków w fazie wdrożenia programu[40]. W ślad za poleceniem miał zostać sporządzony pisemny wniosek, który nie wpłynął do Wydziału. Odnosząc się do jednego pracownika, którego zakres obowiązków nie odpowiadał nadanemu uprawnieniu, Naczelnik wyjaśnił, że popełnił błąd. Jednocześnie wskazał, że program do którego nadano uprawnienia temu pracownikowi uruchamiany był z udziału sieciowego, do którego pracownik nie miał nadanych uprawnień i nie mógł uruchomić tego programu.

(akta kontroli str. 40, 234-245, 386, 388, 407, 410)

NIK wskazuje, że polecenia ustne nie były wystarczające wobec obowiązujących w Urzędzie regulacji wewnętrznych, do których stosowania zobowiązani byli wszyscy pracownicy.

2. W stosunku do ośmiu spośród 15 objętych próbą byłych pracowników Urzędu (tj. 47%) nie dokonano bezzwłocznej zmiany uprawnień w systemach informatycznych, co stanowiło naruszenie §19 ust. 2 pkt 5 rozporządzenia KRI.

W dniu przeprowadzenia czynności kontrolnych[41], konta w systemie informatycznym:

- trzech byłych pracowników były aktywne, mimo skierowania wniosków o blokadę dostępu/zamknięcie konta w systemie;
- jednego byłego pracownika dokonano resetu hasła 30 dni po jego zakończeniu pracy w Urzędzie;
- czterech byłych pracowników zostały zamknięte w terminie od 54 do 212 dni po zakończeniu stosunku pracy. Przy czym w dwóch z tych przypadków nie było możliwe ustalenie, czy dokonano resetu hasła przed datą zamknięcia konta ze względu na nadpisanie pliku dziennika zdarzeń na kontrolerze domeny. Na jednym z kont dokonano resetu hasła 30 dni po zakończeniu stosunku pracy, a zamknięto to konto 102 dni od tej daty. Jedno z ww. kont zamknięte zostało 77 dni po zakończeniu pracy danego pracownika, ze względu na brak wniosku o odebranie uprawnień.

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

(akta kontroli str. 234, 246-247)

Naczelnik Wydziału Informatyki wyjaśnił, że w większości przypadków, kiedy następowała rotacja pracowników na stanowisku, wykonywano reset hasła użytkownika, co było jednoznaczne z zablokowaniem dostępu do całego systemu temu pracownikowi. Konta pozostawiane były jednak jako aktywne, aby osoba, która przejmowała zadania miała dostęp do części dokumentów i innych danych, niezbędnych do zachowania ciągłości pracy. Ponadto, Naczelnik wskazał, że w jednym przypadku przyczyną niezamknięcia konta (oraz braku resetu hasła) był brak wniosku o odebranie uprawnień pracownikowi. W pozostałych, przyczyną opóźnień był nadmiar obowiązków oraz brak zastępstwa na stanowisku informatyka.

Były Naczelnik Wydziału Gospodarki Komunalnej wyjaśnił, że niezłożenie wniosku o odebranie uprawnień pracownikowi związane było z nadmiarem obowiązków.

(akta kontroli str. 409-410, 465)

[40] Program wspomagający zarządzanie nieruchomościami.

[41] Tj. 19 lipca 2024 r.

3. Spośród trzech objętych badaniem systemów informatycznych, w dwóch nie ustanowiono wymogów dla haseł dostępu do tych systemów określonych w części V ust. 2 Instrukcji zarządzania systemem informatycznym.

Zgodnie z części V ust. 2 Instrukcji zarządzania systemem informatycznym, hasło użytkownika miało być zmieniane nie rzadziej niż 30 dni. Dwa objęte badaniem systemy informatyczne nie wymuszały zmiany hasła w terminach przyjętych w tej instrukcji, tj. w jednym przypadku program nie wymuszał zmiany hasła, w drugim wymuszenie okresowej zmiany hasła ustawione zostało na 180 dni.

(akta kontroli str. 40-41, 248)

Naczelnik Wydziału Informatyki wyjaśnił, że przyczyną rezygnacji z wymuszenia zmiany haseł oraz ustawienia wymuszenia hasła co 180 dni były liczne prośby o pilną pomoc w resetowaniu zapomnianego hasła, które były uciążliwe ze względu na natłok obowiązków związanych z samodzielnym wykonywaniem zadań. Naczelnik wyjaśnił dodatkowo, że aby korzystać z tych programów należało prawidłowo zalogować się do systemów informatycznych Urzędu, gdzie wymagane było podanie hasła o określonej złożoności, którego zmiana była wymuszana co 30 dni. Ponadto Naczelnik powołał się na rekomendacje CERT Polska dla haseł, które wskazują, że system nie powinien wymuszać okresowej zmiany hasła użytkownika[42].

(akta kontroli str. 411)

NIK wskazuje, że instrukcja zarządzania systemem informatycznym jest obowiązującym dokumentem Urzędu i obowiązki z niego wynikające winny być respektowane. Powyższe może również prowadzić do konstatacji, że niezbędnym jest dokonanie przeglądu tej instrukcji, pod kątem m.in. aktualności zapisów w niej zawartych odnoszących się do stosowanych metod i środków uwierzytelniania oraz procedur związanych z ich zarządzeniem i użytkowaniem.

4. Kopie zapasowe przechowywane były na serwerze archiwizacji znajdującym się miejscu wytwarzania danych, co stanowiło naruszenie § 19 ust. 2 pkt 12 lit. b i e rozporządzenia KRI.

W wyniku oględzin ustalono, że kopie zapasowe nie były tworzone na zewnętrznych nośnikach danych, a urządzenia przechowujące kopie utworzone w ramach kopii obrazów maszyn wirtualnych i kopii wykonanej z poprzedniej kopii znajdowały się w pomieszczeniu serwerowni, tj. miejscu wytwarzania danych.

Zgodnie z § 19 ust. 2 pkt 12 lit. b i e rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego na: minimalizowaniu ryzyka utraty informacji w wyniku awarii i zapewnieniu bezpieczeństwa plików systemowych.

(akta kontroli str. 307-321)

Naczelnik Wydziału Informatyki wyjaśnił, że aktualny stan ma charakter tymczasowy. Kopie przechowywane są w miejscu wytwarzania ze względu na remont pomieszczenia, w którym przechowywane były kopie. Po zakończeniu remontu kopie te zostaną przeniesione do innego pomieszczenia.

(akta kontroli str. 386, 388)

Zdaniem NIK, nawet czasowe umiejscowienie kopii zapasowych w miejscu wytwarzania stwarza ryzyko utraty informacji.

[42] https://cert.pl/posts/2022/01/kompleksowo-o-haslach/

OCENA CZĄSTKOWA

W Urzędzie wdrożono rozwiązania organizacyjne i techniczne zapewniające bezpieczeństwo informacji oraz ciągłość działania, jednakże nie w każdym przypadku przyjęte rozwiązania te były prawidłowo i rzetelnie realizowane. Stwierdzone w badanym obszarze nieprawidłowości dotyczyły: przechowywania w miejscu wytwarzania danych sporządzonych kopii zapasowych systemów, niedokonania bezzwłocznego odebrania uprawnień do systemów informatycznym pracownikom, którzy zakończyli stosunek pracy w Urzędzie oraz rezygnacji z wymuszenia okresowej zmiany hasła wbrew przyjętym regulacjom wewnętrznym.

OBSZAR

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

3.1 W 2018 r. opracowano analizę ryzyka utraty integralności, poufności i dostępności informacji w obszarze personelu, siedziby, organizacji, sprzętu, oprogramowania i sieci wraz ustaleniem poziomu ryzyka i reakcji na ryzyko.

IODO wyjaśnił, że w latach następnych przyjęto zasadę, iż analiza ryzyka miała być przeprowadzana corocznie lub w miarę potrzeb. Tematyka każdego roku dotyczyła innego obszaru działania urzędu. Analiza ryzyka przeprowadzana była przez IODO wraz z pracownikiem merytorycznym obszaru objętego analizą.

W 2023 r. przeprowadzono analizę ryzyka w obszarze ochrony danych osobowych, której wyniki zostały przekazane ADO. Jak wskazał IODO, kolejna analiza zostanie przeprowadzona do końca 2024 r.

(akta kontroli str. 424-425, 456-457)

3.2 Wprowadzono instrukcję postępowania w sytuacji naruszenia danych osobowych[43], z którą zapoznano wszystkich pracowników. Prowadzono także rejestr incydentów bezpieczeństwa oraz działań korygujących i zapobiegawczych. W 2023 r. odnotowano infekcję komputera: podejrzane pliki i ruch w sieci ukierunkowany na atak. Infekcja została usunięta. W wyniku tego incydentu informatyk przekazał pracownikom, w ramach przypomnienia, zasady bezpieczeństwa w systemie informatycznym. Pracownicy Urzędu zostali dodatkowo przeszkoleni z zakresu cyberbezpieczeństwa.

(akta kontroli str. 70-79, 333-347, 412, 418-419)

3.3 W okresie objętym kontrolą przeprowadzono jedno szkolenie w tematyce ochrony danych osobowych[44]. Szkolenie adresowane było dla pracowników Urzędu. Szkolenia w tematyce ochrony danych osobowych przeprowadzane były w każdym roku. W szkoleniu organizowanym w danym roku uczestniczyły osoby, które nie były objęte wcześniej takim szkoleniem. Na 64 pracowników administracyjnych zatrudnionych na dzień 31 grudnia 2023 r. przeszkolonych zostało 61 pracowników (tj. 95,3%). Trzy osoby nie objęte szkoleniem były długotrwale nieobecne.

IODO wyjaśnił, że po wejściu przepisów z zakresu ochrony danych osobowych wszyscy pracownicy zostali przeszkoleni z tej tematyki. Dodatkowo, co najmniej raz w roku organizowane było szkolenie dla nowych lub powracających po dłuższych nieobecnościach pracowników. IODO wskazał ponadto, że utrzymuje stały kontakt z pracownikami podczas wykonywania swoich obowiązków, a także w sposób ciągły

[43] Zarządzeniem nr OR.0050.494.2018 z 17 grudnia 2018 r.

[44] Zakres szkolenia obejmował m.in.: regulacje prawne, podstawy przetwarzania danych, upoważnienia, oświadczenia poufności, klauzule informacyjne, rejestr czynności, umowy powierzenia danych, klauzule poufności, polityka czystego biurka, czystego ekranu, udzielanie odpowiedzi na wnioski pisemne, przekazywanie informacji między instytucjami, informacja publiczna, BIP, audyty, analiza ryzyka, instrukcja naruszeń, kary.

stara się podnosić świadomość pracowników w zakresie ochrony danych osobowych poprzez stałą wymianę informacji i doświadczeń.

(akta kontroli str. 353-361, 455-456)

3.4 W okresie od 24 października 2022 r. do 17 stycznia 2023 r. przeprowadzony został audyt bezpieczeństwa informacji oraz zapewniania ciągłości działania systemów informatycznych. W jego wyniku sformułowanych zostało łącznie 20 rekomendacji, które do czasu zakończenia kontroli NIK zostały zrealizowane.

(akta kontroli str. 362-385, 386, 389)

Stwierdzone nieprawidłowości

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

OCENA CZĄSTKOWA

W Urzędzie podejmowano prawidłowe działania mające na celu zapobieganie incydentom bezpieczeństwa informacji, w tym prowadzono analizy ryzyka, szkolenia i audyty.

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

1. Bezzwłoczne podejmowanie działań istotnych z punktu widzenia bezpieczeństwa informacji.

Wnioski

1. Wskazanie w planie ciągłości działania osób odpowiedzialnych za prawidłową i terminową realizację działań w nim przewidzianych.
2. Dokonanie przeglądu nadanych uprawnień pracowników do systemów informatycznych i usunięcie uprawnień niezgodnych z zakresem obowiązków.
3. Zapewnienie bezzwłocznego blokowania dostępu do kont pracownikom, po zakończeniu stosunku pracy.
4. Ustawienie w systemach wymuszenia zmiany hasła nie rzadziej niż co 30 dni, zgodnie z wewnętrznie przyjętymi zasadami.
5. Dokonanie przeglądu Instrukcji zarządzania systemem informatycznym, pod kątem aktualizacji jej zapisów.

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 w Katowicach. 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 od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag i 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.

Katowice, dnia 19 września 2024 r.

Kontroler
Lucyna Mol
Gł. specjalista kontroli państwowej

Najwyższa Izba Kontroli
Delegatura w Katowicach