NAJWYŻSZA IZBA KONTROLI

DEPARTAMENT ADMINISTRACJI PUBLICZNEJ

KAP.410.3.4.2024

Pan Piotr Liżewski
Starosta Ostrołęcki
Starostwo Powiatowe w Ostrołęce
Pl. Gen. J. Bema 5
07-410 Ostrołęka

WYSTĄPIENIE POKONTROLNE

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

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

I. Dane identyfikacyjne

Jednostka kontrolowana	Starostwo Powiatowe w Ostrołęce[1], pl. Gen. Józefa Bema 5, 07-410 Ostrołęka
Kierownik jednostki kontrolowanej	Pan Piotr Liżewski, Starosta Ostrołęcki, od 7 maja 2024 r. W okresie objętym kontrolą funkcję kierownika jednostki poprzednio pełnił: Pan Stanisław Kubeł, Starosta Ostrołęcki, od 21 listopada 2018 r. do 6 maja 2024 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 zakończenia czynności kontrolnych, tj. 30 lipca 2024 r.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[2]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Departament Administracji Publicznej
Kontroler	Marcin Grochal, Główny specjalista kontroli państwowej, upoważnienie do kontroli nr KAP/43/2024 z 21 maja 2024 r.

(akta kontroli str. 1-3)

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

II. Ocena ogólna[3] kontrolowanej działalności

OCENA OGÓLNA

Najwyższa Izba Kontroli ocenia negatywnie stan zapewnienia bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w Starostwie Powiatowym w Ostrołęce.

Uzasadnienie oceny ogólnej

Negatywną ocenę uzasadnia liczba i zakres stwierdzonych nieprawidłowości, które ze względu na swój charakter i zakres skutkowały negatywnymi ocenami cząstkowymi we wszystkich trzech badanych obszarach. Nieprawidłowości te związane były w szczególności z niewypełnieniem obowiązków wynikających z ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa[4], rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[5] oraz wymogów Polskiej Normy PN-EN ISO/IEC 27001/2017 *Technika bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania*.

W obszarze dotyczącym organizacji bezpieczeństwa informacji i zapewnienia ciągłości działania stwierdzone nieprawidłowości dotyczyły m.in. niezidentyfikowania wszystkich zbiorów danych urzędu podlegających zabezpieczeniu oraz niewdrożenia Systemu Zarządzania Bezpieczeństwem Informacji. Ponadto nie zostały w urzędzie ustanowione polityki ciągłości działania oraz plany zapewnienia ciągłości działania i plany odtworzeniowe, a także nie prowadzono analiz ryzyka w związku z potrzebą zachowania ciągłości działania. W Starostwie nie utrzymywano także w aktualności inwentaryzacji zasobów informatycznych urzędu, rozumianej jako stałe posiadanie aktualnych informacji w zakresie posiadanego sprzętu informatycznego oraz jego konfiguracji.

W obszarze rozwiązań organizacyjnych i technicznych zapewniających bezpieczeństwo informacji oraz ciągłość działania, wdrożonych i wykorzystywanych w urzędzie, nie zapewniono adekwatności przyznawanych uprawnień przetwarzania informacji do zadań realizowanych przez pracowników, nie ustanowiono zasad gwarantujących bezpieczną pracę przy pracy zdalnej, a także nie zapewniono właściwego poziomu zabezpieczeń serwerowni urzędu. Ponadto, nie zagwarantowano odpowiedniego poziomu bezpieczeństwa informacji w umowach w sprawie usług IT, a także nie zidentyfikowano kluczowych elementów infrastruktury i usług IT pod kątem wpływu czynników zewnętrznych.

W zakresie działań w celu zapobiegania incydentom bezpieczeństwa, nieprawidłowości dotyczyły m.in. nieprzeprowadzania okresowych audytów bezpieczeństwa, nieopracowania procedur umożliwiających bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji oraz incydentów cyberbezpieczeństwa, a także niezapewnienie pracownikom szkoleń z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa.

W ocenie NIK, stwierdzone nieprawidłowości wskazywały, że w zakresie objętym kontrolą, w Starostwie nie funkcjonowała adekwatna, skuteczna i efektywna kontrola zarządcza, o której mowa w art. 68 ustawy z 27 sierpnia 2009 r. o finansach publicznych[6]. Stwierdzone nieprawidłowości dotyczyły w szczególności celów i zarządzania ryzykiem, mechanizmów kontroli, informacji i komunikacji,

---

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

[4] Dz.U. z 2024 r. poz. 1077, dalej: ustawa o KSC.

[5] Dz. U. z 2017 r., poz. 2247, dalej: stare rozporządzenie KRI. Obowiązywało do 22 maja 2024 r. Od 23 maja 2024 r. obowiązuje rozporządzenie 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, Dz.U. poz. 773, dalej: nowe rozporządzenie KRI.

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

stanowiących elementy kontroli zarządczej określone w Standardach kontroli zarządczej dla jednostek sektora finansów publicznych[7].

W urzędzie prawidłowo realizowano zadania w zakresie m.in. wyznaczenia i zapewnienia niezależności Inspektora Ochrony Danych Osobowych (IOD), opracowania i wdrożenia dokumentacji w zakresie bezpieczeństwa danych osobowych i jej dostosowania do wymogów 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[8]. Także wyznaczenie i zgłoszenie osób odpowiedzialnych za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa (CSIRT NASK) nastąpiło zgodnie z ustawą o KSC. Ponadto w Starostwie zapobiegano możliwości zainstalowania nieautoryzowanego oprogramowania na komputerach urzędu oraz zapewniono właściwe usytuowanie komputerów w salach obsługi obywateli, aby uniemożliwić wgląd do danych przez osoby nieuprawnione. Prawidłowo wykonywano i przechowywano kopie zapasowe systemów informatycznych.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[9] kontrolowanej działalności

OBSZAR

1. Organizacja bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych

Opis stanu faktycznego

1. W Starostwie nie zostały zidentyfikowane i sklasyfikowane z uwzględnieniem wymagań prawnych, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikacje, zbiory danych urzędu, co opisano w pkt 1 sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 5-13, 714-716)

2. W Starostwie nie został opracowany, ustanowiony i wdrożony System Zarządzania Bezpieczeństwem Informacji, o którym mowa w § 20 ust. 1 w zw. z ust. 3 starego rozporządzenia KRI oraz § 19 ust. 1 w związku z ust. 3 nowego rozporządzenia KRI, co opisano w pkt 2 sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 5-13)

3. W zakresie ochrony danych osobowych, w okresie objętym kontrolą, w Starostwie obowiązywały dokumenty uwzględniające wymogi RODO. Do 19 czerwca 2024 r. była to Polityka Bezpieczeństwa Danych Osobowych Starostwa Powiatowego, Starosty Ostrołęckiego i Powiatu Ostrołęckiego, wprowadzona zarządzeniem nr 52/2022 Starosty Ostrołęckiego[10].

Od 19 czerwca 2024 r. obowiązywała, wprowadzona zarządzeniem nr 30/2024 Starosty Ostrołęckiego[11] Polityka Bezpieczeństwa Danych Osobowych Starostwa Powiatowego, Starosty Ostrołęckiego i Powiatu Ostrołęckiego. Wprowadzone uregulowania zostały zakomunikowane pracownikom urzędu.

---

7 stanowiących 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).

8 Dz. Urz. UE L 119 z 04.05.2016 r., str. 1, dalej: RODO.

9 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.

10 Zarządzenie nr 52/2022 Starosty Ostrołęckiego z dnia 12 grudnia 2022 r. w sprawie wdrożenia w Starostwie Powiatowym w Ostrołęce dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych, dalej: Zarządzenie PBDO.

11 Zarządzenie nr 30/2024 Starosty Ostrołęckiego z dnia 19 czerwca 2024 r. zmieniające zarządzenie w sprawie wdrożenia w Starostwie Powiatowym w Ostrołęce dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych, dalej: Zarządzenie zmieniające PBDO.

(akta kontroli str. 5-13, 60-139)

4. W okresie objętym kontrolą, w Starostwie nie prowadzono analiz ryzyka w związku z potrzebą zachowania ciągłości działania, co opisano w pkt 3 sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 5-13, 539-542)

5. W urzędzie nie została wprowadzona polityka ciągłości działania oraz nie zostały opracowane plany ciągłości działania i plany odtworzeniowe, co opisano w pkt 4 sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 5-13)

6. Zadania związane z bezpieczeństwem informacji i zapewnieniem ciągłości działania systemów informatycznych zostały powierzone dwóm informatykom zatrudnionym w urzędzie, w tym Administratorowi Systemów Informatycznych (ASI). Do ich zadań należało m.in.:

- administrowanie systemami, w tym nadawanie lub zmiana uprawnień do przetwarzania danych osobowych w systemach informatycznych;
- wdrażanie oprogramowania użytkowego w Starostwie;
- prowadzenie szkoleń w zakresie obsługi sprzętu komputerowego, używania systemów i programów wykorzystywanych w Starostwie;

Do zadań ASI należało ponadto m.in.:

- podejmowanie działań w przypadku wykrycia naruszeń w systemie zabezpieczeń;
- zapewnienie ciągłości działania systemów informatycznych, w tym zabezpieczenie zbiorów danych;
- zabezpieczenie systemów służących do przetwarzania danych osobowych przed działaniem złośliwego oprogramowania;
- monitorowanie działania zabezpieczeń.

Wyznaczone osoby posiadały wiedzę i kompetencje do realizacji powierzonych zadań.

Starosta poinformował, że w zakresie ochrony danych osobowych osobą odpowiedzialną za bezpieczeństwo informacji wyznaczony został Inspektor Ochrony Danych.

(akta kontroli str. 539-567, 770-778)

7. Wyznaczenie IOD nastąpiło na podstawie zarządzenia PBDO oraz zarządzenia zmieniającego PBDO. Wyznaczona osoba, zgodnie z art. 37 ust. 5 RODO, posiadała niezbędne kwalifikacje zawodowe do pełnienia tej funkcji.

W okresie objętym kontrolą zadania Inspektora Ochrony Danych zostały powierzone osobie nie będącej pracownikiem Starostwa na podstawie dwóch, następujących po sobie umów zawartych z firmą zewnętrzną, posiadającą doświadczenie w zakresie ochrony danych osobowych. W umowach określono zadania IOD, które były zgodne z art. 39 RODO i obejmowały m.in.:

- informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
- monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;

- współpraca z organem nadzorczym;
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem.

(akta kontroli str. 5-13, 35-150, 197, 559)

8. Osoba wyznaczona na IOD nie była pracownikiem Starostwa, co zapewniało wypełnienie, wynikającego z art. 38 ust. 3 i ust. 6 RODO, obowiązku zapewnienia niezależności i eliminacji konfliktu interesów w realizacji zadań przez IOD.

(akta kontroli str. 35-59)

9. Starosta, zgodnie z obowiązkiem wynikającym z art. 21 ust. 1 ustawy o KSC, 8 grudnia 2022 r. wyznaczył, a 9 grudnia 2022 r. zgłosił do CSIRT NASK osoby odpowiedzialne za kontakty z podmiotem krajowego systemu cyberbezpieczeństwa.

W Starostwie nie została wyznaczona osoba odpowiedzialna za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jednostki podległe i nadzorowane oraz jednostki organizacyjne Starostwa, której wyznaczenie fakultatywnie przewidywał art. 21 ust. 2 i 3 ustawy KSC.

(akta kontroli str. 5-12, 151-154)

10. Starostwo nie posiadało informacji o zasobach informatycznych obejmujących ich rodzaj i konfigurację w rozumieniu § 20 ust. 2 pkt 2 starego rozporządzenia KRI oraz § 19 ust. 2 pkt 2 nowego rozporządzenia KRI, co opisano w pkt 5 sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 5-13, 207-264)

11. W dniu 13 grudnia 2023 r. Starosta złożył wniosek o przystąpienie do projektu pn. *Zwiększenie cyberbezpieczeństwa infrastruktury i usług teleinformatycznych w Urzędzie Starostwa Powiatowego w Ostrołęce w ramach projektu grantowego „Cyberbezpieczny Samorząd”,* realizowanego z wykorzystaniem Funduszy Europejskich na Rozwój Cyfrowy, Priorytet II Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa, Fundusz – Europejski Fundusz Rozwoju Regionalnego (EFRR)[12]. Łączna wnioskowana kwota wydatków wynosiła 977,7 tys. zł, w tym 850,0 tys. zł dofinansowania ze środków Unii Europejskiej i 127,7 tys. zł wkładu własnego. Zawarta 12 lipca 2024 r. umowa zakłada realizację projektu w trzech obszarach: organizacyjnym, kompetencyjnym i technicznym.

W obszarze organizacyjnym przewidziano przede wszystkim opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji oraz przeprowadzenie audytu SZBI.

W obszarze kompetencyjnym projekt będzie koncentrował się na zapewnieniu pracownikom urzędu szkoleń z zakresu cyberbezpieczeństwa i bezpieczeństwa informacji.

W ramach obszaru technicznego przewidziano w szczególności zakup systemów bezpieczeństwa teleinformatycznego, kompleksowego systemu do backupu i zasilania awaryjnego.

Zgodnie z umową Starostwo zobowiązane jest do realizacji Projektu maksymalnie do 30 czerwca 2026 r.

(akta kontroli str. 155-179, 654-713)

Stwierdzone nieprawidłowości

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

[12] Numer naboru: FERC.02.02-CS.01-001/23

1. W Starostwie nie zidentyfikowano i nie sklasyfikowano z uwzględnieniem wymagań określonych w normie PN-EN ISO/EIC 27001:2017 wszystkich zbiorów danych, co zdaniem NIK było nierzetelne.

   Zgodnie z pkt A.8.1.1 i A.8.2.1 załącznik A normy PN-EN ISO/EIC 27001:2017, w jednostce należy zidentyfikować informacje, aktywa związane z informacjami i środkami przetwarzania informacji oraz sporządzić i utrzymywać ewidencję tych aktywów. Informacje powinny być klasyfikowane z uwzględnieniem wymagań prawnych, wartości krytyczności i wrażliwości na modyfikację lub nieuprawnione ujawnienie.

   Wicestarosta wyjaśnił, że urzędzie nie posiadano zatwierdzonej przez Starostę klasyfikacji wszystkich posiadanych i przetwarzanych zbiorów danych. Jako przyczynę wskazał braki kadrowe w zakresie informatyki i brak środków finansowych na zadania związane z zapewnieniem bezpieczeństwa informacji. Dodał także, że (…) *zadania są zaplanowane do realizacji dzięki pozyskanym przez Powiat Ostrołęcki środkom z programu „Cyberbezpieczny Samorząd".*

   (akta kontroli str. 5-13, 207-264, 714-716, 779-780)

2. W urzędzie nie opracowano, nie ustanowiono i nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji, co było niezgodne z § 20 ust. 1 w zw. z ust. 3 starego rozporządzenia KRI oraz § 19 ust. 1 w związku z ust. 3 nowego rozporządzenia KRI. Zgodnie z ww. przepisami Starostwo zobowiązane było m.in. do opracowania, ustanowienia, wdrożenia, monitorowania, utrzymania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji, zapewniającym poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

   Starosta wyjaśnił, że *(…) we wniosku, w ramach projektu „Cyberbezpieczny Samorząd" w obszarze organizacyjnym część grantu przeznaczono na opracowanie i wdrożenie SZBI, aby był to dokument sformalizowany, który spina ramami wszystkie strategie, regulaminy i instrukcje, spełniający wymagania dla systemów teleinformatycznych określone w Rozporządzeniu KRI.*

   (akta kontroli str. 5-13, 539-542)

3. W Starostwie nie przeprowadzano analizy ryzyka w związku z potrzebą zachowania ciągłości działania systemów informatycznych, co było działaniem nierzetelnym.

   Norma ISO 22301 wskazuje na kluczowe znaczenie analizy ryzyka w związku z potrzebą zachowania ciągłości działania, gdyż określa prawdopodobieństwo i wpływ zagrożeń, mogących być przyczyną przerwania działalności. Po ocenieniu możliwości zaistnienia zagrożenia analizuje się mechanizmy zabezpieczające w organizacji, zmniejszające ryzyko operacyjne w firmie, w tym ryzyko przerwania działania.

   Starosta wyjaśnił, że w 2024 r. została przeprowadzona przez IOD analiza ryzyka obejmująca potrzebę zachowania ciągłości działania systemów informatycznych poprzez uwzględnienie w analizie każdego ze zbiorów danych, ryzyka awarii systemów informatycznych oraz ataków złośliwego oprogramowania. Dodał także, że w przypadku każdego zidentyfikowania ryzyka, podejmowane były działania naprawcze i mitygacyjne.

   Zdaniem NIK, wskazana analiza ryzyka, obejmująca jedynie ryzyka dotyczące zbiorów danych osobowych, nie zapewniła skutecznej identyfikacji zagrożeń mających wpływ na zapewnienie ciągłości działania systemów informatycznych urzędu.

   (akta kontroli str. 5-13, 539-552, 629-632)

4. W Starostwie nie wprowadzono polityki ciągłości działania i nie opracowano planów ciągłości działania oraz planów odtworzeniowych dotyczących m.in.

zasilania i topologii sieci, klastrów i macierzy dyskowych, systemów kopii zapasowych i urządzeń brzegowych. Nie został także określony akceptowalny czas przywrócenia ciągłości działania systemów informatycznych urzędu, co było działaniem nierzetelnym.

Starosta wyjaśnił, że *urząd nie wprowadził odrębnej polityki działania, jednak stosowne zapisy dotyczące tworzenia kopii zapasowych, ich testowania i odzyskiwania danych zawiera Instrukcja Zarządzania Systemami Informatycznymi (…).* Dodał także, że *główna przyczyna to brak środków w budżecie urzędu i braki osobowe w kadrze IT (brak komórki IT). Złożenie wniosku (…) w ramach projektu „Cyberbezpieczny Samorząd" ma tę przyczynę zniwelować. Otrzymane środki pozwolą na skorzystanie z doświadczenia i wiedzy specjalistów z zakresu cyberbezpieczeństwa, opracowania polityki i procedur.*

NIK zauważa, że wskazana instrukcja[13] przeznaczona była dla użytkowników systemów informatycznych Starostwa, którzy wykorzystują te systemy w ramach wykonywania swoich obowiązków służbowych. Rolą Polityki Ciągłości Działania jest z kolei umożliwienie kierownictwu jednostki określenia założeń, zakresu oraz podstawowych zasad zarządzania ciągłością działania, a także zdefiniowanie, w jaki sposób urząd zapewni spełnienie warunków umożliwiających odtworzenie działalności po katastrofie lub innym incydencie zakłócającym działanie.

(akta kontroli str. 5-13, 115-150, 539-542)

5. Urząd nie posiadał aktualnej informacji o zasobach informatycznych obejmującej ich rodzaj i konfigurację.

   Zgodnie z § 20 ust. 2 pkt 2 starego rozporządzenia KRI oraz § 19 ust. 2 pkt 2 nowego rozporządzenia KRI, zarządzanie infrastrukturą informatyczną wymaga utrzymywania w urzędzie aktualnej inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. Ustalono, że w Starostwie nie był prowadzony elektroniczny rejestr zasobów teleinformatycznych urzędu.

   Starosta wyjaśnił, że użytkowany w urzędzie program do inwentaryzacji nie spełnia wymogów rozporządzenia KRI, w szczególności w zakresie opisu konfiguracji sprzętu i przypisanych do niego aplikacji. Wskazał także, że w celu spełnienia warunków rozporządzenia KRI zakupiono system pozwalający zarządzać wszystkimi zasobami IT, który pozwala m.in. na uzyskanie szczegółowych informacji dot. sprzętu z opisem rodzaju, konfiguracji i zainstalowanego oprogramowania. Dodał, że zakupiony system jest obecnie na etapie wdrożenia.

   (akta kontroli str. 5-13, 207-264)

OCENA CZĄSTKOWA

NIK negatywnie ocenia stan organizacji bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych. Ocena wynika z liczby oraz zakresu stwierdzonych nieprawidłowości, które dotyczyły w szczególności:

- nieopracowania i niewdrożenia Systemu Zarządzania Bezpieczeństwem Informacji,
- nieposiadania przez Urząd aktualnej informacji o zasobach informatycznych obejmującej ich rodzaj i konfigurację,
- niewprowadzenia polityki ciągłości działania oraz planów ciągłości działania i planów odtworzeniowych,

[13] Instrukcja została wprowadzona 19 czerwca 2024 r. Nie obowiązywała w objętym kontrolą okresie od 1 stycznia 2023 r. do 18 czerwca 2024 r.

- niezidentyfikowania i niesklasyfikowania z uwzględnieniem wymagań określonych w normie PN-EN ISO/EIC 27001:2017 wszystkich zbiorów danych urzędu.

W badanym obszarze w Starostwie prawidłowo zrealizowano natomiast zadania związane ze sporządzeniem dokumentacji w zakresie ochrony danych osobowych uwzględniającą wymogi RODO i wyznaczeniem Inspektora Ochrony Danych, a także wyznaczeniem osoby odpowiedzialnej za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.

OBSZAR

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

Opis stanu faktycznego

1. W urzędzie została zablokowana możliwość instalacji przez użytkowników systemów informatycznych nieautoryzowanego oprogramowania na komputerach służbowych.

Na podstawie oględzin przeprowadzonych na próbie 10 komputerów ustalono, że we wszystkich przypadkach użytkownicy nie mieli możliwości zainstalowania nieautoryzowanego oprogramowania, ze względu na brak uprawnień. Było to zgodne z § 20 ust. 2 pkt 4 starego rozporządzenia KRI i § 19 ust. 2 pkt 4 nowego rozporządzenia KRI. Ponadto, na wszystkich objętych badaniem komputerach był zainstalowany program antywirusowy, który miał zaktualizowaną bazę wirusów.

(akta kontroli str. 193-195)

2. Badanie zgodności posiadanych przez pracowników uprawnień do systemów informatycznych urzędu z ich rzeczywiście wykonywanymi zadaniami wskazanymi w zakresach obowiązków przeprowadzono na próbie obejmującej 15 pracowników urzędu. W 11 przypadkach zakres uprawnień był adekwatny do realizowanych przez nich zadań. W przypadku 4 pracowników stwierdzono, że posiadali oni dostęp do systemów informatycznych niezwiązanych z wykonywanymi przez nich obowiązkami, co opisano w pkt 1 sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 811-833)

3. W okresie objętym kontrolą, w urzędzie pracę zakończyło 11 osób, w tym cztery nieposiadające dostępu do systemów informatycznych[14]. W toku oględzin ustalono, że w przypadku trzech osób dostęp do systemów został odebrany niezwłocznie, tj. zostały cofnięte przez Starostę upoważnienia do przetwarzania danych i Administrator Systemów Informatycznych (ASI) odłączył użytkowników od domeny. W przypadku czterech pracowników nie został natomiast zablokowany dostęp użytkowników do systemów informatycznych urzędu, pomimo zakończenia przez nich pracy w urzędzie, co opisano w pkt 2 sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 180-189)

4. Na podstawie oględzin trzech systemów informatycznych zarządzanych przez Starostwo ustalono, że we wszystkich systemach stosowano unikalne identyfikatory użytkowników, które można powiązać z pracownikami urzędu. W Starostwie nie określono zasad dotyczących długości i złożoności haseł oraz częstotliwości ich zmiany w systemach informatycznych.

Wicestarosta wyjaśnił, że konta i hasła użytkownika konfigurowane są z poziomu domeny, a zasady haseł kontroluje Group Policy Objects (GPO), będące zbiorem zasad i ustawień dla systemu, które określają, jak użytkownik lub komputer może postępować w danej sytuacji. Dodał także, że *używanie bezpiecznych haseł oraz okresową ich zmianę wymusza zasada GPO na serwerze Active Directory (…).*

[14] Starosta, wicestarosta, kierowca oraz pracownik interwencyjny.

Logowanie (…) odbywa się dwuetapowo, dopiero po zalogowaniu do stacji roboczej jest możliwe uruchomienie aplikacji.

Na podstawie badania próby 10 komputerów urzędu ustalono, że długość hasła logowania do domeny wynosiła od ośmiu do 16 znaków.

(akta kontroli str. 194-195, 789-810)

5. Oględziny sześciu stanowisk pracy realizujących zadania z zakresu rejestracji pojazdów i wydawania praw jazdy wykazały, że monitory usytuowane były w sposób uniemożliwiający wgląd do danych przez osoby nieuprawnione. Było to zgodne z § 20 ust. 2 pkt 7 starego rozporządzenia KRI i § 19 ust. 2 pkt 7 nowego rozporządzenia KRI.

(akta kontroli str. 191-192)

6. W Regulaminie pracy zdalnej urzędu nie ustanowiono podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, co opisano w pkt 3 sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 645-653)

7. W zakresie zapewnienia bezpieczeństwa danych zgromadzonych na laptopach urzędu w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym, Starosta poinformował, że dyski na komputerach służbowych są zaszyfrowane. Było to zgodne z § 20 ust. 2 pkt 9 starego rozporządzenia KRI i § 19 ust. 2 pkt 9 nowego rozporządzenia KRI. Ponadto, na podstawie oględzin przeprowadzonych na pięciu laptopach służbowych stwierdzono, że długość hasła wynosiła od ośmiu do 11 znaków.

(akta kontroli str. 629-633)

8. W urzędzie nie zastosowano właściwego zabezpieczenia serwerowni w celu ochrony informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie, co opisano w pkt 4 sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 785-788)

9. Na podstawie badania czterech umów[15] zawartych w okresie objętym kontrolą, obejmujących swym zakresem zakup sprzętu i usługi serwisowe IT ustalono, że w jednej umowie zawarto zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji. W przypadku trzech umów nie uwzględniono zapisów zapewniających bezpieczeństwo informacji, co opisano w pkt 5 sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 568-597)

10. W urzędzie nie została opracowana formalna procedura dotycząca zabezpieczenia danych przed nieuprawnionym dostępem w przypadku przekazywania sprzętu IT poza jednostkę. Starosta poinformował, że stosowaną praktyką w przypadku przekazania sprzętu do serwisu lub zbycia sprzętu jest wymontowywanie z nich nośników danych. Dodał także, że w przypadku użyczania sprzętu m.in. do szkół lub Radnym Powiatu, na podstawie umowy, przekazywany sprzęt jest fabrycznie nowy i nie zawiera żadnych danych jednostki.

(akta kontroli str. 598-602, 654-713)

11. Instrukcja Zarządzania Systemami Informatycznymi Starostwa Powiatowego w Ostrołęce[16] określała m.in. procedury tworzenia kopii zapasowych oraz sposób ich przechowywania. W Starostwie kopie zapasowe danych przechowywane były w innej lokalizacji niż miejsce wytwarzania tych danych. Jednocześnie zapewnione zostało

[15] Umowy nr: 138/2023 z 9 maja 2023 r., 170/2023 z 30 maja 2023 r., 231/2023 z 12 lipca 2023 r. i 1/2024 z 3 stycznia 2024 r.

[16] Instrukcja stanowiła załącznik nr 2 do zarządzenia nr 30/2024 Starosty Ostrołęckiego z dnia 19 czerwca 2024 r. zmieniającego zarządzenie w sprawie wdrożenia w Starostwie Powiatowym w Ostrołęce dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych.

ograniczenie dostępu do pomieszczeń, w których przechowywane były kopie zapasowe, co było zgodne z § 19 ust. 2 pkt 7 nowego rozporządzenia KRI.

Wicestarosta poinformował także, że obszar wykonywania kopii zapasowych również przewidziany jest do realizacji w projekcie „Cyberbezpieczny Samorząd".

W okresie objętym kontrolą (od 1 stycznia 2023 r. do 19 czerwca 2024 r.) w urzędzie nie były ustalone zasady przechowywania kopii zapasowych, co opisano w pkt 6 sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 60-150, 207-264, 766-778)

12. Kopie zapasowe baz danych systemów informatycznych wykonywane były codziennie.

Oględziny odzyskiwania danych z kopii zapasowej jednego z systemów wykorzystywanych w urzędzie potwierdziły, że kopie zapasowe tego systemu wykonywane były codziennie, a ostatnia została zrobiona w dzień poprzedzający oględziny. Na podstawie kopii zapasowej z 1 kwietnia 2024 r. nie stwierdzono błędów w utworzonej kopii. Ponadto system został poprawnie uruchomiony z wybranej do kontroli kopii. ASI oświadczył, że przynajmniej raz na kwartał sprawdzana jest poprawność wykonywanych kopii bezpieczeństwa, poprzez uruchamianie z nich systemów. W szczególności czynność ta jest wykonywana w przypadku aktualizacji systemu. Dodał także, że nie ma na to potwierdzenia w dokumentach.

Powyższe stanowiło realizację obowiązku zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii i zapewnienia bezpieczeństwa plików systemowych, o których mowa w § 19 ust. 2 pkt 12 lit. b i e nowego rozporządzenia KRI.

(akta kontroli str. 140-150, 198-206)

13. Zgodnie z pkt 12.1.3 załącznika A do normy PN-ISO/IEC 27001:2017 należy monitorować i dostosowywać wykorzystanie zasobów oraz przewidywać wymaganą pojemność w przyszłości, dla zapewnienia właściwej wydajności systemu.

W urzędzie nie została wprowadzona procedura, która obejmowałaby swym zakresem monitorowanie przestrzeni dyskowej na serwerach.

Wicestarosta poinformował, że *fakt wolno przyrastających danych na dyskach pozwala na podjęcie decyzji o jej zwiększeniu odpowiednio wcześniej.*

W wyniku oględzin zajętości przestrzeni dyskowej trzech serwerów urzędu ustalono, że monitorowanie jest prowadzone za pomocą specjalistycznego oprogramowania. Zajęta przestrzeń serwerów wynosiła od 33,1% do 63,2% całkowitej przestrzeni dyskowej serwerów.

(akta kontroli str. 781-784, 806-810)

14. W Starostwie nie zostały zidentyfikowane kluczowe elementy infrastruktury i usługi IT oraz ich zabezpieczenie pod kątem wpływu czynników zewnętrznych, co opisano w pkt 7 sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 766-769)

Stwierdzone nieprawidłowości

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

1. W przypadku czterech pracowników stwierdzono, że posiadali oni dostęp do systemów informatycznych niezwiązanych z wykonywanymi przez nich obowiązkami, co było niezgodne z § 19 ust. 2 pkt 4 nowego rozporządzenia KRI.

   Na podstawie oględzin przeprowadzonych na próbie 15 pracowników urzędu stwierdzono, że trzech pracowników Wydziału Gospodarki Nieruchomościami miało nadany dostęp do systemu EWOPIS, wykorzystywanego przez Wydział

Geodezji. Ponadto, jeden pracownik Wydziału Komunikacji i Drogownictwa posiadał dostęp do systemu finansowo-księgowego.

Wicestarosta wyjaśnił, że niezgłoszenie pisemnych wniosków o cofnięcie upoważnienia do systemu EWOPIS i systemu FK oraz brak odebrania uprawnień był wynikiem przeoczenia.

(akta kontroli str. 722-765, 811-903)

2. W przypadku czterech z siedmiu pracowników, którzy zakończyli pracę w urzędzie w okresie od 1 stycznia 2023 r. do 31 maja 2024 r., nie został zablokowany dostęp do domeny urzędu[17] i tym samym do systemów informatycznych. Oznaczało to zwłokę od 69 do 520 dni[18] i było niezgodne z § 20 ust. 2 pkt 5 starego rozporządzenia KRI i § 19 ust. 2 pkt 5 nowego rozporządzenia KRI.

   ASI wyjaśnił, że przyczyną nieodłączenia pracowników było nieotrzymanie przez niego informacji na temat ustania świadczenia pracy.

   Zgodnie z obowiązującą w Starostwie PBDO, *(...) upoważnienie wygasa automatycznie z chwilą rozwiązania umowy o pracę (...).* W urzędzie nie ustalono jednak zasad określających obowiązek poinformowania ASI o zakończeniu pracy przez pracownika.

   Wicestarosta wyjaśnił, że przyczyną niewprowadzenia zasad dotyczących przekazywania do ASI[19] informacji umożliwiającej niezwłoczne odłączenie byłego pracownika od zasobów informatycznych urzędu było przeoczenie.

   Zdaniem NIK brak skutecznego przepływu informacji pomiędzy komórkami organizacyjnym stanowi słabość systemu kontroli zarządczej w urzędzie w ramach elementu określonego w pkt D 17 Standardów kontroli zarządczej – Komunikacja wewnętrzna.

   (akta kontroli str. 180-189, 722-765, 894-903)

3. W Regulaminie pracy zdalnej urzędu, wprowadzonym zarządzeniem Starosty Ostrołęckiego[20], nie ustanowiono podstawowych zasad gwarantujących bezpieczeństwo informacji podczas pracy zdalnej.

   Dokument został wprowadzony 7 kwietnia 2023 r. Określono w nim ogólne zasady wykonywania pracy zdalnej wynikające z kodeksu pracy. Nie ustanowiono w nim jednak podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, co było niezgodne z § 20 ust. 2 pkt 8 starego rozporządzenia KRI oraz § 19 ust. 2 pkt 8 nowego rozporządzenia KRI.

   Wicestarosta wyjaśnił, że nie ma wiedzy dlaczego zasady te nie zostały ujęte w dokumencie.

   (akta kontroli str. 645-653, 714-716)

4. W Starostwie nie zapewniono odpowiedniego zabezpieczenia fizycznego serwerowni[21]. W konsekwencji w urzędzie nie zapewniono zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie, co było niezgodne z § 20 ust. 2 pkt 9 starego rozporządzenia KRI i § 19 ust. 2 pkt 9 nowego rozporządzenia KRI.

---

17 Według stanu na dzień przeprowadzenia oględzin, tj. 2 lipca 2024 r.

18 Zakończenie pracy: GM - 12 maja 2023 r. (417 dni zwłoki), KK – 3 kwietnia 2023 r. (457 dni zwłoki), MM – 31 stycznia 2023 r. (520 dni zwłoki), PM – 27 kwietnia 2024 r. (69 dni zwłoki).

19 Standardy stanowią załącznik do Komunikatu nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla jednostek sektora finansów publicznych.

20 Zarządzenie nr 10/2023 Starosty Ostrołęckiego z dnia 7 kwietnia 2023 r. w sprawie ustalenia Regulaminu pracy zdalnej pracowników w Starostwie Powiatowym w Ostrołęce.

21 Szczegółowe ustalenia w tym zakresie zostały przekazane w trakcie czynności kontrolnych Administratorowi Systemów Informatycznych oraz Staroście Powiatu Ostrołęckiego pismem KAP.410.3.4.2024/8 z dnia 4 lipca 2024 oraz pismem KAP.410.3.4.2024/23 z dnia 18 lipca 2024 r.

Wicestarosta wyjaśnił, że przyczyną niezapewnienia właściwego poziomu zabezpieczenia serwerowni był w szczególności brak środków finansowych na prace remontowo-konserwatorskie, które w obiekcie zabytkowym wymagają bardzo dużych nakładów.

Zdaniem NIK zapewnienie zabezpieczenia serwerowni jest kluczowym elementem bezpieczeństwa informacji przechowywanych i przetwarzanych na serwerach.

(akta kontroli str. 785-788, 806-810)

5. W przypadku trzech z czterech objętych badaniem umów obejmujących swym zakresem zakup sprzętu i usługi serwisowe IT[22] nie zawarto zapisów zapewniających bezpieczeństwo informacji, co było niezgodne z § 20 ust. 2 pkt 10 starego rozporządzenia KRI. Umowy dotyczyły m.in. zakupu i wdrożenia systemu informatycznego, zakupu komputerów przenośnych oraz usług utrzymania poczty elektronicznej urzędu.

   Starosta wyjaśnił, że w przypadku umowy zakupu i wdrożenia systemu informatycznego (138/2023 z 9 maja 2023 r.), wykonawcę obowiązywała klauzula zawarta w umowie serwisowej 401/2022 zawartej 20 grudnia 2022 r.

   Wskazana przez Starostę umowa zawierające klauzulę bezpieczeństwa informacji została zawarta w związku z podpisaniem wcześniejszych umów na realizację konkretnych zadań. Objęte badaniem umowy nie były kontynuacją poprzednio zawartych umów (nie były to aneksy do tych umów). Zdaniem NIK nie można więc przyjąć, że zawarte we wcześniejszych umowach klauzule są prawnie wiążące w przypadku kolejnych umów z tymi samymi podmiotami, w których takich klauzul nie zawarto.

   W przypadku umowy 170/2023 z 30 maja 2023 r. Starosta wskazał, że *(…) w przypadku naprawy gwarancyjnej lub wymiany sprzętu, sprzęt byłby przekazywany bez dysków (…)*.

   Zdaniem NIK zapisy umowy nie przewidywały demontażu nośników danych w przypadku przekazywania sprzętu do serwisu. W urzędzie nie obowiązuje także żadna procedura regulująca przedmiotową kwestię.

   W zakresie umowy 231/2023 z 12 lipca 2023 r. na utrzymanie poczty elektronicznej urzędu Starosta wyjaśnił, że *w dniu 9.08.2022 r. została podpisana „umowa powierzenia przetwarzania danych osobowych usługa utrzymania poczty elektronicznej i systemu skyCMS", która jest uzupełnieniem do umowy głównej nr 231/2023.*

   Zdaniem NIK, wskazana przez Starostę umowa powierzenia zawarta 11 miesięcy przed umową objętą kontrolą, związana była z umową główną nr 139/2020 z 29 czerwca 2020 r., która była zawarta na okres do 30 czerwca 2023 r. Nie dotyczy zatem umowy objętej badaniem. Ponadto, umowa powierzenia dotyczy jedynie danych osobowych i nie spełnia wymogów zapewnienia bezpieczeństwa informacji w rozumieniu rozporządzenia KRI.

   (akta kontroli str. 568-628)

6. W okresie objętym kontrolą (od 1 stycznia 2023 r. do 19 czerwca 2024 r.) w urzędzie nie były ustalone zasady przechowywania kopii zapasowych, co było działaniem nierzetelnym.

   Starosta wyjaśnił, że Instrukcja Zarządzania Systemami Informatycznymi, określająca m.in. zasady dotyczące kopii zapasowych została w sposób błędny potraktowana jako integralna część Polityki Bezpieczeństwa Danych Osobowych i nie została przyjęta Zarządzeniem PBDO.

[22] Umowy nr: 138/2023 z 9 maja 2023 r., 170/2023 z 30 maja 2023 r., 231/2023 z 12 lipca 2023 r.

W związku z usunięciem nieprawidłowości w toku kontroli poprzez wprowadzenie Instrukcji zarządzeniem zmieniającym PBDO, NIK odstępuje od formułowania wniosku pokontrolnego w tym zakresie.

(akta kontroli str. 60-150, 207-264, 766-778)

7. W Starostwie nie zostały zidentyfikowane kluczowe elementy infrastruktury i usługi IT oraz ich zabezpieczenie pod kątem wpływu czynników zewnętrznych, co było działaniem nierzetelnym.

   Identyfikacja kluczowych dla pracy urzędu elementów infrastruktury informatycznej i usług informatycznych ma na celu zapewnienie szybkiego i skutecznego przywrócenia infrastruktury i usług IT w sytuacji zakłócenia ciągłości działania. Nie został także określony czas przywrócenia poszczególnych systemów oraz procesów do działania po katastrofie lub incydencie zakłócającym ciągłość działania.

   Wicestarosta wyjaśnił, że nie zna przyczyn takiego stanu rzeczy. Dodał także, że zapewnienie środowiska odtworzeniowego oraz określenie czasu przywrócenia systemów przewidziane jest w ramach zakupu systemu backup, który jest przewidziany do sfinansowania z projektu „Cyberbezpieczny Samorząd".

(akta kontroli str. 766-769)

OCENA CZĄSTKOWA

NIK ocenia negatywnie działalność Starostwa w zakresie wdrożonych i wykorzystywanych rozwiązań organizacyjnych i technicznych zapewniających bezpieczeństwo informacji oraz ciągłość działania, ze względu na liczbę i zakres stwierdzonych nieprawidłowości, które dotyczyły: braku w zawieranych umowach zapisów zapewniających bezpieczeństwo informacji, niedostatecznego zabezpieczenia fizycznego serwerowni urzędu, przypadków nieblokowania dostępu do zasobów informatycznych urzędu osobom, które zakończyły pracę, oraz nadmiarowego przydzielenia pracownikom uprawnień do zasobów informatycznych Starostwa. Ponadto w Starostwie nie zidentyfikowano kluczowych elementów infrastruktury oraz nie określono zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.

W Starostwie prawidłowo realizowano zadania w zakresie zabezpieczenia komputerów przed nieuprawnioną instalacją oprogramowania przez użytkowników. Zapewniono także bezpieczeństwo informacji poprzez ustawienie monitorów w sali obsługi obywateli w sposób uniemożliwiający wgląd do danych przez osoby nieuprawnione.

OBSZAR

3. Działania w celu zapobiegania incydentom bezpieczeństwa danych

Opis stanu faktycznego

1. W okresie objętym kontrolą nie przeprowadzono okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji, co opisano w pkt 1 sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 5-13)

2. Zasady zgłaszania incydentów dotyczących danych osobowych w Starostwie zostały określone w PBDO. Wskazano w niej także przykłady incydentów, mogących powodować naruszenie bezpieczeństwa przetwarzania danych osobowych.

W urzędzie nie zapewniono bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji oraz cyberbezpieczeństwa, co opisano w pkt 2 sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 5-13, 60-140, 766-769)

3. W urzędzie nie zapewniono szkoleń pracowników zaangażowanych w proces przetwarzania informacji, co opisano w pkt 3 sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 5-13)

4. W okresie objętym kontrolą w urzędzie nie przeprowadzono okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, co opisano w pkt 4 sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 5-13)

Stwierdzone nieprawidłowości

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

1. W okresie objętym kontrolą nie przeprowadzono okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji, co było niezgodne z § 20 ust. 2 pkt 3 starego rozporządzenia KRI oraz § 19 ust. 2 pkt 3 nowego rozporządzenia KRI.

   Wicestarosta wyjaśnił, że *powodem nieprzeprowadzenia w latach 2023-2024 analizy ryzyka (…) jest brak środków finansowych w budżecie Powiatu. Działania te zostały wpisane do zrealizowania w ramach pozyskanych środków z programu „Cyberbezpieczny samorząd".*

   (akta kontroli str. 5-13, 806-809)

2. W Starostwie nie zapewniono bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji, o którym mowa w § 20 ust. 2 pkt 13 starego rozporządzenia KRI oraz § 19 ust. 2 pkt 13 nowego rozporządzenia KRI oraz obowiązku zgłaszania incydentów cyberbezpieczeństwa wynikającego z art. 22 ustawy o KSC, gdyż nie opracowano i nie wprowadzono w życie stosownych procedur w tym zakresie.

   Wicestarosta wyjaśnił, że *opracowanie procedur i rejestrów zgodnych z KRI i KSC przewidziano do realizacji w projekcie „Cyberbezpieczny Samorząd".*

   (akta kontroli str. 5-13, 766-769)

3. Pracownikom urzędu zaangażowanym w proces przetwarzania informacji nie zapewniono szkoleń z zakresu bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 6 rozporządzenia KRI i § 19 ust. 2 pkt 6 nowego rozporządzenia KRI

   Przeciętne zatrudnienie w Starostwie w okresie objętym kontrolą wynosiło 136 osób, z czego niemal wszyscy są zaangażowani w proces przetwarzania informacji[23]. W 2023 r. zorganizowano w urzędzie szkolenia z zakresu ochrony danych osobowych, w którym uczestniczyło 127 pracowników. Ponadto, szkoleniem takim objęci byli nowozatrudnieni pracownicy.

   W latach 2023 – 2024 w szkoleniach z zakresu cyberbezpieczeństwa uczestniczyły cztery osoby pracujące w urzędzie, w tym dwóch informatyków. Stanowiło to zaledwie 3,1% przeciętnego zatrudnienia w okresie objętym kontrolą, co zdaniem NIK nie może stanowić wypełnienia obowiązku wynikającego z rozporządzenia KRI. Szkolenia z zakresu bezpieczeństwa informacji powinny obejmować wszystkich pracowników, ponieważ świadomość zagrożeń i konsekwencji zaistnienia incydentów na każdym poziomie procesu przetwarzania informacji stanowi istotny element bezpieczeństwa.

   Wicestarosta wyjaśnił, że szkolenia wszystkich pracowników Starostwa przewidziane są do realizacji w roku 2024 w ramach programu grantowego „Cyberbezpieczny samorząd".

   (akta kontroli str. 5-13, 207-281, 560-567, 714-721)

4. W okresie objętym kontrolą nie przeprowadzono w urzędzie okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 starego rozporządzenia KRI oraz § 19 ust. 2 pkt 14 nowego rozporządzenia KRI. Przepisy w ramach zarządzania bezpieczeństwem

[23] W urzędzie siedem osób nie było zaangażowanych w proces przetwarzania informacji – dwóch kierowców oraz pięć sprzątaczek.

informacją, nakładają na podmiot realizujący zadania publiczne obowiązek zapewnienia takiego audytu nie rzadziej niż raz na rok.

Starosta wyjaśnił, że audyt nie był przeprowadzony *ponieważ audytor wewnętrzny i inspektor ds. audytu i kontroli nie posiadają niezbędnej wiedzy z zakresu bezpieczeństwa informacji (…).* Dodał także, że wykonanie audytu zaplanowane zostało w ramach realizacji grantu z projektu „Cyberbezpieczny Samorząd.

(akta kontroli str. 5-13, 207-265)

OCENA CZĄSTKOWA

NIK ocenia negatywnie działania Starostwa w celu zapobiegania incydentom bezpieczeństwa danych, ze względu stwierdzone w toku kontroli nieprawidłowości. W urzędzie nie przeprowadzono okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji. Nie zapewniono także bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji i incydentów cyberbezpieczeństwa. Ponadto w okresie objętym kontrolą w urzędzie nie przeprowadzono okresowych audytów wewnętrznych z zakresu bezpieczeństwa informacji i nie zapewniono pracownikom szkoleń z zakresu bezpieczeństwa informacji.

IV. Wnioski

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

Wnioski

1. Zidentyfikowanie wszystkich posiadanych i przetwarzanych zbiorów danych oraz ich sklasyfikowanie z uwzględnieniem wymagań prawnych, wartości krytycznych i wrażliwości na modyfikację lub nieuprawnione ujawnienie.
2. Opracowanie, ustanowienie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji.
3. Prowadzenie analiz ryzyka w związku z potrzebą zachowania ciągłości działania systemów informatycznych i podejmowanie działań minimalizujących stwierdzone ryzyko.
4. Wprowadzenie polityki ciągłości działania w Starostwie oraz opracowanie planów ciągłości działania urzędu i planów odtworzeniowych, a także określenie akceptowalnego czasu przywrócenia ciągłości działania systemów informatycznych.
5. Utrzymywanie w Starostwie aktualnej inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.
6. Zapewnienie dostępu do przetwarzania informacji w zakresie adekwatnym do zadań realizowanych przez pracowników.
7. Zapewnienie niezwłocznego odłączania od systemów informatycznych osób, które zakończyły pracę w urzędzie.
8. Wprowadzenie w regulaminie pracy zdalnej podstawowych zasad zapewnienia bezpieczeństwa informacji podczas pracy zdalnej.
9. Zapewnienie odpowiedniego poziomu zabezpieczenia fizycznego serwerowni urzędu.
10. Zawieranie w umowach serwisowych zapisów zapewniających bezpieczeństwo informacji.
11. Identyfikacja kluczowych elementów infrastruktury i usługi IT oraz ich zabezpieczenie pod kątem wpływu czynników zewnętrznych.
12. Zapewnienie przeprowadzania okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji.
13. Opracowanie i wprowadzenie w życie procedur postępowania z incydentami bezpieczeństwa informacji i cyberbezpieczeństwa, umożliwiających bezzwłoczne zgłaszanie incydentów w tym zakresie.
14. Zapewnienie szkoleń z zakresu bezpieczeństwa informacji wszystkim pracownikom zaangażowanym w proces zaangażowanym w proces przetwarzania informacji.
15. Zapewnienie corocznego przeprowadzania okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Departamentu Administracji Publicznej. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykonania wniosków

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

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

Warszawa, 13 sierpnia 2024 r.

Najwyższa Izba Kontroli
Departament Administracji Publicznej
Dyrektor
Bogdan Skwarka
wz. Dariusz Łubian
p.o. Wicedyrektor

/podpisano elektronicznie/

Kontroler
Marcin Grochal
Główny specjalista

/podpisano elektronicznie/