NAJWYŻSZA IZBA KONTROLI

DELEGATURA WE WROCŁAWIU

LWR.410.13.1.2024

Pani
Małgorzata Jędrzejewska-Skrzypczyk
Starosta Kłodzki
Starostwo Powiatowe w Kłodzku
ul. Okrzei 1
57-300 Nowa Kłodzko

WYSTĄPIENIE POKONTROLNE

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

I. Dane identyfikacyjne

Jednostka kontrolowana	Starostwo Powiatowe w Kłodzku, ul. Okrzei 1, 57-300 Kłodzko[1].
Kierownik jednostki kontrolowanej	Małgorzata Jędrzejewska-Skrzypczyk, Starosta Kłodzki od 31 stycznia 2024 r.[2]
Zakres przedmiotowy kontroli	Rozwiązania organizacyjne i techniczne w zakresie zapewnienia bezpieczeństwa przetwarzania informacji oraz zapewnienia ciągłości działania w urzędzie i ich stosowanie.
Okres objęty kontrolą	Od 1 stycznia 2023 r. do dnia zakończenia kontroli w 2024 r.[3], (także okresy wcześniejsze w zakresie uczestnictwa w programie Cyfrowa Gmina/Cyfrowy Powiat).
Podstawa prawna podjęcia kontroli	Artykuł 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[4].
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura we Wrocławiu
Kontroler	Waldemar Zimoch, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LWR/83/2024 z dnia 31 maja 2024 r.

(akta kontroli: str. 1-5)

[1] Dalej: Urząd lub Starostwo.
[2] Dalej: Starosta. Wcześniej od 22 listopada 2018 r. Maciej Awiżeń.
[3] Czynności kontrolne zakończono 6 września 2024 r.
[4] Dz. U. z 2022 r. poz. 623; dalej: ustawa o NIK.

II. Ocena ogólna[5] kontrolowanej działalności

OCENA OGÓLNA

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

Podstawą oceny ogólnej były oceny cząstkowe, dotyczące obszarów, które zostały poddane kontroli. W szczególności w badanym okresie w Urzędzie nie było w pełni wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji[6] w rozumieniu § 19 ust. 1 rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[7] Urząd nie posiadał również jednolitej dokumentacji odnośnie polityki bezpieczeństwa informacji. Jednocześnie w tym okresie stosowano dokumentację składającą się na Politykę Ochrony Danych Osobowych, uwzględniającą wymogi rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[8].

Wszystkie zweryfikowane umowy serwisowe posiadały zapisy gwarantujące odpowiedni poziom bezpieczeństwa. Ustalono także zasady tworzenia i przechowywania kopii zapasowych, które to tworzono regularnie, a ich testowanie odbywało się automatycznie. Nadawanie i odbieranie uprawnień pracownikom do pracy w systemach informatycznych odbywało się na podstawie wdrożonej w Urzędzie procedury. We wszystkich badanych przypadkach zablokowano konta w systemach informatycznych osobom, które zakończyły zatrudnienie. Ponadto prawidłowo realizowano obowiązek przeprowadzania audytu wewnętrznego w zakresie bezpieczeństwa informacji. Przeprowadzono także częściową analizę ryzyka utraty integralności, poufności oraz dostępności informacji. Należy jednak podkreślić, że niewystarczające było uwzględnienie ryzyk związanych ze zjawiskami atmosferycznymi czy też czynnikami zewnętrznymi, w związku z czym należy przeprowadzić ponowną analizę ryzyka dla całego obszaru IT.

W trakcie kontroli stwierdzono szereg nieprawidłowości polegających na: **[1]** braku nadania zbiorom danych odpowiedniej wagi istotności w procesie identyfikowania danych podlegających zabezpieczeniu, **[2]** nieprzeprowadzaniu analiz ryzyka związanych z potrzebą zachowania ciągłości działania systemów informatycznych; **[3]** nieopracowaniu polityki ciągłości działania, planu zapewnienia ciągłości działania oraz planu odtworzeniowego, **[4]** niedokonywaniu przeglądu i aktualizacji dokumentacji zawierającej elementy polityki bezpieczeństwa informacji, **[5]** niezapobieżeniu możliwości zainstalowania nieautoryzowanego oprogramowania, **[6]** użytkowaniu pomieszczenia serwerowni w sposób niezapewniający odpowiedniej ochrony, **[7]** wyłączeniu Referatu Informatyki z administrowania zasobami sprzętowymi jak i oprogramowaniem jednego z wydziałów Starostwa, **[8]** nieuwzględnieniu wszystkich etapów procedury identyfikacji kluczowych elementów infrastruktury i usług IT w procesie zapewnienia ciągłości działania oraz **[9]** nierealizowaniu wymaganych szkoleń z zakresu bezpieczeństwa informacji.

[5] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[6] Dalej: SZBI
[7] Dz. U. poz. 773, dalej: rozporządzenie KRI.
[8] Dz. Urz. UE L 119/1 z 4 maja 2016 r., str. 1, ze zm.; dalej: RODO.

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

OBSZAR

1. Organizacja bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych

Opis stanu faktycznego

1.1. Starostwo posiadało łącznie siedem systemów (rejestrów, programów) za pomocą których przetwarzano zbiory różnych danych. Urząd zidentyfikował, prowadził i aktualizował zbiory tych danych w formie elektronicznej w postaci tabelarycznej. Należy jednak nadmienić, że Starostwo nie przypisało poszczególnym zbiorom odpowiedniego poziomu ochrony, zgodnie z ich wagą, co zostało opisane w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli: str. 6-9)

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

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

Zarządzeniem nr 61/2018 Starosta Kłodzki wprowadził z dniem 3 października 2018 r. Politykę bezpieczeństwa danych osobowych i informacji[10] oraz Instrukcję zarządzania systemami informatycznymi w Starostwie[11]. W Polityce bezpieczeństwa danych zawarto m.in. zapisy na temat: [1] obowiązków Inspektora Ochrony Danych Osobowych[12], [2] obowiązków Administratora Systemów Informatycznych[13], [3] budowy rejestru zbioru danych, [4] sposobu przepływu danych, [5] obowiązku informacyjnego wynikającego z art. 13 RODO, [6] naruszenia ochrony danych osobowych. W wyżej wymienionym dokumencie zamieszczono również polityki bezpieczeństwa dla poszczególnych ogólnokrajowych systemów informatycznych.

Natomiast w Instrukcji zarządzania systemami zawarto zapisy dotyczące m.in.: [1] opisu ogólnej struktury teleinformatycznej, [2] procedury nadawania, odbierania, cofania i modyfikacji uprawnień do pracy w systemach informatycznych, [3] procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemach informatycznych, [4] zasad używania sprzętu IT, [5] procedury tworzenia kopii zapasowych, [6] zabezpieczenia przed złośliwym oprogramowaniem, [7] polityki zarządzania oprogramowaniem, [8] zasad użytkowania prywatnego sprzętu do celów służbowych. Załącznikiem do Instrukcji zarządzania systemami była Polityka zarządzania oprogramowaniem w Starostwie, która zawierała m.in. zasady instalacji, deinstalacji, przechowywania licencji, monitorowania oprogramowania oraz instrukcję przekazywania sprzętu komputerowego z oprogramowaniem poza Starostwo.

Koordynację, nadzór i kontrolę realizacji zadań w ramach wprowadzonych dokumentów powierzono Sekretarzowi Powiatu.

W wyżej wymienionych dokumentach nie wskazano wprost właściciela odpowiadającego za ich opracowanie, przegląd i modyfikację. Jedynie wskazano, że ich wykonanie powierza się wszystkim pracownikom Starostwa, których zapoznano z tymi dokumentami.

(akta kontroli: str. 12-115)

---

[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] Dalej: Polityka bezpieczeństwa danych.

[11] Dalej: Instrukcja zarządzania systemami.

[12] Dalej: IOD.

[13] Dalej: ASI.

1.3. W dniu 3 października 2018 r. Starostwo wprowadziło Politykę bezpieczeństwa danych w której uwzględniono wymagane zapisy wynikające z przepisów RODO oraz zakres odpowiedzialności IOD. Nadzór nad wykonaniem zarządzenia powierzono Sekretarzowi Powiatu, a realizację odpowiednio wszystkim pracownikom Starostwa, którzy zostali zapoznani z tym dokumentem.

(akta kontroli: str. 12-41)

1.4. W okresie objętym kontrolą w Starostwie nie przeprowadzono analizy ryzyka związanego z potrzebą zachowania ciągłości działania systemów informatycznych, co opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli: str. 42-46, 116, 623-633)

1.5. W kontrolowanym okresie Urząd nie wprowadził polityki ciągłości działania, co opisano w sekcji *Stwierdzone nieprawidłowości.*

W dokumentacji Starostwa dotyczącej Polityki bezpieczeństwa danych, a także Instrukcji zarządzania systemami opisano co prawda aspekty dotyczące elementów związanych z polityką ciągłości działania, takich jak m.in.: przechowywanie w innym pomieszczeniu niż serwerownia kopii zapasowych czy też reakcje na wystąpienie infekcji lub zawirusowania komputera. Nie były to jednak opisy poszczególnych reakcji na zaistniałe problemy, które powinny być jednym z elementów polityki ciągłości działania.

(akta kontroli: str. 12-101)

1.6/1.7. W Starostwie nie opracowano, a tym samym nie wdrożono planu zapewnienia ciągłości działania oraz planu odtworzeniowego, co opisano w sekcji *Stwierdzone nieprawidłowości*. Nie realizowano tym samym testów i treningów związanych z zapewnieniem ciągłości działania.

(akta kontroli: str. 12-101,116-117)

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

(akta kontroli: str. 118)

1.9. Urząd wyznaczył Zarządzeniem nr 105/2021 z dnia 30 listopada 2021 r. osobę odpowiedzialną za bezpieczeństwo informacji – IOD, której przypisano m.in. takie obowiązki jak:

- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie wykonania tych zaleceń;
- pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych;
- doradzanie w sprawach danych osobowych.

Jak stwierdzono w trakcie wykonywania czynności kontrolnych z powodu braku w Starostwie polityki i planów związanych z ciągłością działania nie wyznaczono osoby odpowiedzialnej za ten obszar działania.

(akta kontroli: str. 131-143)

1.10. Zgodnie z art. 37 ust. 1 i 5 RODO oraz art. 8 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[14] w Urzędzie wyznaczono osobę na stanowisko IOD. Osoba obejmująca ww. stanowisko posiadała odpowiednie wykształcenie

[14] Dz. U. z 2019 r. poz. 1781.

i kwalifikacje. Posiadała również w zakresie obowiązków przypisane zadania m.in. takie jak:

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

(akta kontroli: str. 131-143)

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

IOD zatrudniony był w Referacie ds. kadrowych i kancelaryjnych na stanowisku ds. zarządzania zasobami ludzkimi oraz obsługi kancelaryjnej wydziału. Zgodnie z art. 38 ust 6 RODO inspektor ochrony danych może wykonywać inne obowiązki, jednak najwyższe kierownictwo zapewnić mu powinno takie zadania i obowiązki, które nie powodowałyby konfliktu interesów. IOD oświadczył, że czynności, które wykonuje na podstawowym stanowisku nie kolidują z wykonywaniem czynności IOD i nie występuje konflikt interesów.

(akta kontroli: str. 131-143)

1.12. Urząd w dniu 23 maja 2023 r., Zarządzeniem nr 34/2023 Starosty Kłodzkiego wyznaczył, zgodnie z ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[15], jedną osobę odpowiedzialną za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. W ramach przesłanego w tym samym dniu zgłoszenia przekazano do CSIRT NASK[16] niezbędne informacje, a zgłoszenie to było zgodne z art. 21 ust. 1 ustawy o ksc.

Nie skorzystano natomiast z uprawnienia określonego w art. 21 ust. 2 i 3 ustawy o ksc, tj. nie wyznaczono jednej osoby odpowiedzialnej za utrzymywanie ww. kontaktów w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jednostki organizacyjne Starostwa oraz jednostki podległe i nadzorowane przez Starostę.

(akta kontroli: str. 144-147)

1.13. Starostwo nie posiadało formalnej i jednolitej polityki bezpieczeństwa informacji. Wprowadzono jednakże Politykę bezpieczeństwa danych oraz Instrukcję zarządzania systemami. W dokumentach tych znajdowały się zapisy, które zdaniem NIK odzwierciedlały elementy polityki bezpieczeństwa było to m.in.:

- opis budowy rejestru zbioru danych;
- sposób przepływu tych danych,
- opis ogólny struktury teleinformatycznej,
- procedury nadawania, odbierania, cofania i modyfikacji uprawnień do pracy w systemach informatycznych,
- procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemach informatycznych,
- zasady używania sprzętu IT,
- procedury tworzenia kopii zapasowych,

[15] Dz. U. z 2024 r. poz. 1077, ze zm.

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

- zabezpieczenie przed złośliwym oprogramowaniem,
- polityka zarządzania oprogramowaniem,
- zasady użytkowania prywatnego sprzętu do celów służbowych.

Załącznikiem do Instrukcji zarządzania systemami była Polityka zarządzania oprogramowaniem w Starostwie, która zawierała dodatkowo m.in. zasady instalacji, deinstalacji, przechowywania licencji, monitorowania oprogramowania oraz instrukcję przekazywania sprzętu komputerowego z oprogramowaniem poza Starostwo. Dokument ten nie zawierał wymogu sporządzenia innych odrębnych dokumentów wykonawczych, stanowiących uszczegółowione procedury, polityki czy instrukcje.

(akta kontroli: str. 12-115)

1.14. Do utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację, wymaganej przepisami § 19 ust. 2 pkt 2 rozporządzenia KRI, w Starostwie wykorzystywano dedykowane oprogramowanie. Oprogramowanie to w czasie przeprowadzania oględzin było w pełni wdrożone i pozwalało na automatyczne wykrywanie sieci oraz monitorowanie m.in. komputerów stacjonarnych i przenośnych oraz zainstalowanych na nich aplikacji. Dane zgromadzone w tym programie dotyczyły użytkowników sprzętu, wszystkich elementów serwisowych sprzętu komputerowego, oprogramowania, drukarek, urządzeń peryferyjnych w tym serwerów. Każdy zinwentaryzowany element posiadał odrębny rekord w tej bazie i był opisany za pomocą atrybutów. W ramach zakupu oprogramowania uzyskano 175 licencji. W dniu przeprowadzenia oględzin, zainstalowane końcówki systemu umożliwiały przeprowadzenie inwentaryzacji 98,8% zasobów (173, w tym komputery stacjonarne, przenośne oraz serwery).
Kierownik Referatu Informatyki nie posiadał dokładnej wiedzy na temat sprzętu informatycznego w Wydziale Geodezji, Kartografii i Katastru[17], co opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli: str. 148-177)

1.15. Starostwo wzięło udział w konkursie grantowym w ramach Projektu „*Cyberbezpieczny Samorząd"*[18] o numerze FERC.02.02-CS.01-001/23, Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe. Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa. Wniosek o dofinansowanie Projektu został złożony w dniu 12 grudnia 2023 r. na kwotę 850 000,00 zł[19]. W dniu 15 lutego 2024 r. wnioskodawca otrzymał informację, że wniosek uzyskał pozytywną ocenę formalno-merytoryczną, a w dniu 8 lipca 2024 r. podpisał umowę.

W ramach uzyskanego dofinansowania, Projektu Urząd zaplanował między innymi:
- sporządzenie Polityki Bezpieczeństwa Informacji oraz SZBI;
- budowę nowej serwerowni;
- zasilanie awaryjne;
- aktualizację urządzeń sieciowych;
- wdrożenie systemu kontroli dostępu za pomocą urządzeń klasy NAC[20];

Ponadto jako element pomiaru poprawy cyberbezpieczeństwa w wyniku realizacji tego Projektu, przewidziano ewaluację według kryteriów „Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego". Przed rozpoczęciem realizacji Projektu wypełniono ankietę, w której określono stan obecny w zakresie

[17] Dalej: GKiK.
[18] Dalej: Projekt.
[19] Dofinansowanie 100%, brak zaangażowania własnych środków Starostwa.
[20] NAC (Network Access Control) - system kontroli dostępu do sieci korporacyjnej.

ośmiu obszarów cyberbezpieczeństwa[21] oraz planowane zmiany w związku z realizacją tego Projektu.

(akta kontroli: str. 178-216)

Stwierdzone nieprawidłowości

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

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

Z wyjaśnień Kierownika Referatu Informatyki wynika, iż Starostwo nie dokonało „oflagowania posiadanych baz", ponieważ wszystkie bazy danych w posiadaniu Urzędu mają ten sam poziom ważności.

NIK wskazuje, że Starostwo powinno przypisać w procesie identyfikacji zbiorów danych podlegających zabezpieczeniu, odpowiedni poziom ochrony, zgodny z ich wagą. Informacje takie klasyfikuje się bowiem z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację.

(akta kontroli: str. 9-10)

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

Sekretarz Powiatu wyjaśnił, że SZBI zostanie opracowany i wdrożony w ramach Projektu, który będzie realizowało Starostwo.

NIK potwierdza, że Zarządzeniem Starosty Kłodzkiego nr 75/2024 z 5 września 2024 r., wprowadzono SZBI. W jego ramach opracowano Politykę Bezpieczeństwa Informacji, która uwzględniała m.in. plan postępowania z ryzykiem, monitorowanie dostępu do systemów informatycznych, czy też plan ciągłości działania[22].

(akta kontroli: str. 11)

3. W Urzędzie nie przeprowadzono analizy ryzyka związanego z potrzebą zachowania ciągłości działania systemów informatycznych, co było działaniem nierzetelnym.

Sekretarz Powiatu wyjaśnił, że obowiązujące zasady zarządzania ryzykiem[23], swoim zakresem obejmowały aspekty ryzyka. Wskazał również, że w Instrukcji zarządzania systemami zawarto opisy procedur: nadawania, cofania i modyfikacji uprawnień, tworzenia kopii zapasowych, zabezpieczenia przed złośliwym oprogramowaniem, wykonywania przeglądów i konserwacji urządzeń IT, monitoringu ruchu sieciowego, czy też zarządzania oprogramowaniem.

NIK wskazuje, że analiza ryzyka w związku z potrzebą zachowania ciągłości działania powinna składać się z kilku elementów. Powinna zidentyfikować i określić ryzyka wraz z dokonaniem ich podziału na zewnętrze oraz wewnętrze. Następnie powinna nadawać tym ryzykom odpowiedni poziom prawdopodobieństwa oraz opisywać działania obejmujące mechanizmy reagowania na zakłócenia, a także, co ważne, powinna być na bieżąco aktualizowana, szczególnie w zakresie ryzyk i działań zapewniających ciągłość funkcjonowania organizacji. Wskazany przez Starostę dokument nie spełniał powyższych warunków, więc nie może być

[21] Były to: [1] Zarządzanie, [2] System Zarządzania Bezpieczeństwem Informacji, [3] Ochrona, [4] Zdarzenia i Monitoring, [5] Reagowanie, [6] Odtwarzanie, [7] Infrastruktura i [8] Telekomunikacja.

[22] Dokument ten ze względu na czas wprowadzenia nie podlegał weryfikacji w ramach niniejszej kontroli.

[23] Zarządzenie nr 22/2016 Starosty Kłodzkiego z dnia 18 marca 2016 r. w sprawie wprowadzenia zasad zarządzania ryzykiem w Starostwie Powiatowym w Kłodzku.

traktowany jako analiza ryzyka związanego z potrzebą zachowania ciągłości działania systemów informatycznych.

(akta kontroli: str. 116-117, 509-510)

4. W Starostwie nie opracowano, a tym samym nie wdrożono polityki ciągłości działania systemów informatycznych, planu zapewnienia ciągłości działania oraz planu odtworzeniowego, co było działaniem nierzetelnym.

Sekretarz Powiatu wyjaśnił, że Urząd wprowadził w latach 2016-2023 procedury związane z ciągłością działania i zostały zawarte w takich dokumentach jak *Plan Działalności Starostwa*, *Zasady Zarządzenia Ryzykiem*, czy też *Ochrona danych osobowych i bezpieczeństwa informacji*.

NIK wskazuje, że brak było jednak procedur związanych m.in. z zachowaniem się w przypadku awarii energetycznej, awarii serwera, awarii macierzy dyskowej, umyślnego zniszczenia danych lub przypadkowej jej kasacji, czy też naruszenia cyberbezpieczeństwa, co nie minimalizowało w tym przypadku ryzyka dotyczącego zachowania ciągłości działania. Ponadto już audytor wewnętrzny w dokumencie z audytu z dnia 30 listopada 2023 r. wskazał, iż należy opracować procedurę planowania ciągłości działania, a także, że plan ciągłości działania powinien stanowić udokumentowaną procedurę, zawierającą wytyczne w zakresie odpowiedzi na zdarzenia oraz odtworzenia operacji po zdarzeniach krytycznych (pożar, powódź, włamanie, brak dostępu do sieci itd.).

Brak polityki ciągłości działania, planu zapewnienia ciągłości działania oraz planu odtworzeniowego nie minimalizuje zakłóceń w realizacji działalności w związku z dysfunkcją systemu informatycznego.

(akta kontroli: str.116-117, 509-510)

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

Kierownik Referatu Informatyki potwierdził, że w Starostwie nie wykonywano corocznego przeglądu tej dokumentacji. Dodał również, że został zaplanowany kompleksowy przegląd dokumentacji podczas tworzenia dokumentacji SZBI w ramach Projektu

(akta kontroli: str. 118)

6. W trakcie wykonywania czynności kontrolnych w Starostwie stwierdzono, że Referat Informatyki nie posiadał wiedzy na temat sprzętu, który zainstalowany został w jednym z wydziałów Urzędu - GKiK. Informatycy z tego Referatu nie posiadali również dostępu do zarządzania serwerami w wyżej wymienionym Wydziale, a administrowaniem jego zasobów sprzętowych jak i oprogramowaniem zajmowały się osoby niezwiązane z Referatem Informatyki.

Sekretarz Powiatu wyjaśnił, że obecna sytuacja w najbliższym czasie zostanie poprawiona, i że Wydział GKiK objęty zostanie nadzorem przez służby informatyczne z Referatu Informatyki.

(akta kontroli: str. 616-622, 645)

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli ocenia negatywnie działania Starostwa w zakresie organizacji bezpieczeństwa informacji oraz zapewnienia ciągłości działania. W Urzędzie nie było w pełni wdrożonego SZBI w rozumieniu § 19 ust. 1 rozporządzenia KRI. Starostwo nie posiadało również jednolitej dokumentacji odnośnie polityki bezpieczeństwa informacji. Wprowadzono jednak niepełne regulacje dotyczące bezpieczeństwa informacji w Polityce bezpieczeństwa danych. Prawidłowo zidentyfikowano zbiory danych podlegających zabezpieczeniu, jednakże nie nadano im odpowiedniego poziomu ochrony, zgodnie z ich wagą. Natomiast w okresie

kontrolowanym nie prowadzono analizy ryzyka w związku z potrzebą zachowania ciągłości działania systemów informatycznych, nie ustanowiono polityki ciągłości działania i nie tworzono planu zapewnienia ciągłości działania. Ponadto Referat Informatyki wyłączony był z administrowania zasobami sprzętowymi jak i oprogramowaniem jednego z wydziałów Starostwa.

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

Opis stanu faktycznego

2.1. Starostwo posiadało wdrożoną procedurę dotyczącą zabezpieczenia przed złośliwym oprogramowaniem będącą częścią Instrukcji zarządzania systemami. Próba dokonania zainstalowania nieautoryzowanego oprogramowania została przeprowadzona na pięciu komputerach (stacjonarnych) i we wszystkich pięciu przypadkach powiodła się. Każdy z użytkowników posiadał przyznane lokalnie uprawnienia administratora w tym zakresie, co było niezgodne z § 19 ust. 2 pkt 4 rozporządzenia KRI i co opisano w sekcji *Stwierdzone nieprawidłowości*.

Starostwo posiadało na stanie dziewięć służbowych telefonów komórkowych które, były zabezpieczone standardowymi aplikacjami i służyły tylko jako urządzenia do komunikacji oraz wykonywania zdjęć. Urząd nie posiadał tabletów.

(akta kontroli: str. 42-67)

2.2. Na dzień 28 czerwca 2024 r. w Starostwie zatrudnionych było 174 osoby, które uczestniczyły w ramach wykonywania swoich obowiązków służbowych w procesie przetwarzania informacji. Nadanie uprawnień do dostępu do systemów IT oraz ich odebranie w Urzędzie następowało na podstawie sformalizowanego wniosku o nadanie/zmianę/cofnięcie uprawnień do pracy w systemach informatycznych Starostwa zgodnie z załącznikiem nr 1 do Instrukcji zarządzania systemami. Przedmiotowy wniosek był podstawą do upoważnienia do przetwarzania danych osobowych we wskazanych zbiorach, ale nie w każdym przypadku był natomiast wskazaniem nadania lub odbierania praw dostępu do konkretnych funkcjonalności wewnątrz programu.

Kierownik Referatu Informatyki oświadczył, że uszczegółowienie nadania uprawnień następowało po ustnym wskazaniu przełożonego, natomiast cofnięcie uprawień, w przypadku zakończenia stosunku pracy, następowało na podstawie karty obiegowej wydawanej przez Referat Kadr.

W ramach przeprowadzonej weryfikacji[24] dotyczącej adekwatności uprawnień do systemów komputerowych i zasobów dyskowych pracowników Starostwa, nie stwierdzono by posiadane przez nich uprawnienia wykraczały poza ich zakresy czynności. Było to zgodne z § 19 ust. 2 pkt 4 rozporządzenia KRI.

(akta kontroli: str. 219-396)

2.3. W okresie od 1 stycznia 2023 do 18 lipca 2024 r. w Urzędzie zakończyło zatrudnienie szesnaście osób. W ramach przeprowadzonej kontroli dokonano weryfikacji odebrania uprawnień wszystkim tym osobom. Ustalono, że we wszystkich tych przypadkach ich konta miały status nieaktywny. Było to zgodne z wymogami wynikającymi z § 19 ust. 2 pkt 5 rozporządzenia KRI.

(akta kontroli: str. 219-396)

2.4. Nadawanie uprawnień użytkownikom, tworzenie identyfikatorów, przydział haseł, czy też częstotliwość ich zmiany określono w Instrukcji zarządzania systemami. Wdrożono także usługę katalogową Active Directory[25] jako podstawową usługę,

[24] 15 pracowników ze 174 pracowników, co stanowiło 8,6%.
[25] Dalej: AD.

w oparciu o którą funkcjonował system logowania użytkowników do stacji roboczych. System obiegu dokumentów jak i cały użytkowany pakiet oprogramowania firmy RADIX został zintegrowany z usługą AD, co nie wymagało od użytkownika ponownego logowania do aplikacji.
W Starostwie określono także zasady budowy hasła do poszczególnych systemów informatycznych określając minimalną liczbę znaków oraz ich złożoność.

Sprawdzenia zabezpieczeń technicznych w systemach IT dokonano na przykładzie trzech systemów informatycznych. Jeden z nich nie wymuszał zmiany hasła i jego złożoności, a budowa loginu była podobna jak w przypadku AD. Oprogramowanie to nie było jednak zintegrowane z AD, a hasło do programu było ustalane jednorazowo przez administratora systemu.

Kierownik Wydziału IT oświadczył, że oprogramowanie to jest archiwalne i wykorzystywane tylko do wglądu do już wytworzonych dokumentów (stare decyzje, rejestr wydawanych decyzji budowlanych).

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

(akta kontroli: str. 151-177)

2.5. Oględziny pięciu stanowisk pracy realizujących zadania w Referacie Komunikacji Starostwa, posiadające dostęp do ogólnopolskiej aplikacji „Źródło" i „CEPiK" wykazały, że monitory usytuowane były w sposób uniemożliwiający wgląd do danych przez osoby nieuprawnione, co było zgodne z § 19 ust. 2 pkt 7 rozporządzenia KRI.

(akta kontroli: str. 217)

2.6. W Instrukcji zarządzania systemami zawarto informacje m.in. na temat, zasad używania służbowego sprzętu przenośnego poza Starostwem, zdalnego dostępu do zasobów sieci wewnętrznej oraz zasad używania prywatnego sprzętu. Każdy użytkownik sprzętu przenośnego przed użytkowaniem własnoręcznym podpisem oświadczał, że znane mu są regulacje wewnętrzne odnośnie sprzętu IT. Było to zgodne z § 19 ust. 2 pkt 8 rozporządzenia KRI.

(akta kontroli: str. 12-41)

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

(akta kontroli: str. 151-177)

2.8. Serwerownia Starostwa była wydzielonym pomieszczeniem w budynku głównym zlokalizowanym w przyziemiu, co zdaniem NIK stwarzało dodatkowe ryzyko związane z możliwością zalania. Kierownik Referatu Informatyki oświadczył, że serwerownia została uruchomiona w 2003 r. i na tamtą chwilę było to najlepiej zorganizowane i najchłodniejsze miejsce.

Dostęp do serwerowni miały osoby z Zespołu do Spraw Informatyki oraz pracownicy zaplecza socjalnego w asyście informatyków. Pomieszczenie to było klimatyzowane, a w czasie oględzin klimatyzacja była sprawna. Sprzęt informatyczny w serwerowni był podłączony do sieci elektrycznej dedykowanej, posiadającej własne zabezpieczenia. Rozdzielnica elektryczna zasilania obwodów dedykowanych była zabezpieczona przed bezpośrednim dostępem osób nieuprawnionych, a w ramach zasilania zapasowego (podtrzymanie pracy urządzeń) wykorzystywane były UPS-y[26]. W pomieszczeniu serwerowni brak było jednak rejestru wejść/wyjść, a w trakcie oględzin stwierdzono ryzyko związane z potencjalnymi zagrożeniami fizycznymi lub

[26] Zasilacz awaryjny, zasilacz bezprzerwowy, zasilacz UPS (ang. uninterruptible power supply – zasilacz bezprzerwowy).

środowiskowymi dla tego pomieszczenia, co opisano w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli: str. 397-400)

2.9. W okresie objętym kontrolą obowiązywało 37 umów zawartych przez Starostwo na zakup lub serwis sprzętu informatycznego i oprogramowania. Szczegółowe badanie czterech z nich wykazało, że w umowach tych zawarto zapisy gwarantujące zachowanie odpowiedniego poziomu bezpieczeństwa informacji. Zapisy te dokonane były w tych umowach lub w, zawieranych osobno, dodatkowych umowach powierzenia danych osobowych. Było to zgodne z § 19 ust. 2 pkt 10 rozporządzenia KRI.

(akta kontroli: str. 401-499)

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

Kierownik Referatu Informatyki oświadczył, że dyski twarde z komputerów przekazanych, czy też uszkodzonych, przechowywane były w odpowiednio zabezpieczonej metalowej szafie.

(akta kontroli: str. 500)

2.11. W Instrukcji zarządzania systemami opisano procedurę tworzenia kopii zapasowych oraz sposób i okres ich przechowywania. Kopie te były tworzone automatycznie przez specjalistyczne oprogramowanie. Backup oprogramowania był wykonywany poza godzinami pracy Starostwa zgodnie z ustalonym, w wyżej wymienionym dokumencie, harmonogramie.

(akta kontroli: str.42-67, 501-508)

2.12. Zapisy w procedurze dotyczącej tworzenia kopii zapasowych określały na jakich nośnikach należy sporządzać odpowiednie kopie. W trakcie przeprowadzonych oględzin stwierdzono, że wykonywane były one na dostępnych zasobach dyskowych, znajdujących się w serwerowni Starostwa, jednakże dodatkowo replika tychże kopii zapasowych znajdowała się w innej, drugiej lokalizacji Urzędu. Kopie te były tworzone w zależności od aplikacji/zasobu, zgodnie z grafikiem tworzenia kopii zapasowych, znajdującym się w Instrukcji zarządzania systemami. W dokumencie tym wskazano również serwer i folder tworzenia kopii.

Zarządzanie automatyczne kopiami w Urzędzie zostało rozpoczęte od 2018 r., to jest od wdrożenia dedykowanego oprogramowania. Walidacja kopii zapasowych odbywała się podczas wykonywania samej kopii, co potwierdzał raport prawidłowości jej wykonania po zakończeniu działania oprogramowania. Urząd nie posiadał jednak sformalizowanej procedury testowania kopii zapasowych oraz harmonogramu testowania tychże kopii.

(akta kontroli: str. 42-67, 501-508)

2.13. Procedury obowiązujące w Starostwie nie przewidywały monitorowania pojemności nośników pamięci serwerów, natomiast w praktyce cały proces monitoringu był realizowany przez oprogramowanie, które było w posiadaniu Urzędu. Równocześnie w trakcie kontroli NIK w oprogramowaniu służącym do inwentaryzacji sprzętu IT uruchomiono funkcjonalność dotyczącą monitorowania i informowania pracowników o przepełnieniu dyskowym. Starostwo posiadało na stanie pięć serwerów fizycznych i 10 wirtualnych. Przeprowadzony w toku oględzin test zajętości

trzech serwerów wykazał poszczególne zajętości, które wynosiły: Serwer 1 – zajętość 29%; Serwer 2 – zajętość 40%; Serwer 3 – zajętość 78%.

(akta kontroli: str. 501-508)

2.14. Urząd nie posiadał w swoich zasobach procedury ciągłości działania, zidentyfikował jednak kluczowe elementy infrastruktury i usług IT. Nie uwzględnił jednak przy tym wszystkich etapów procedury takich jak nadanie odpowiednich procentowych ważności a także opisanie planów naprawczych w przypadku wystąpienia awarii, co opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli: str.12-147)

Stwierdzone nieprawidłowości

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

1. Próba dokonania zainstalowania nieautoryzowanego oprogramowania przeprowadzona w Starostwie na pięciu komputerach (stacjonarnych), we wszystkich przypadkach powiodła się. Każdy z użytkowników na obsługiwanym komputerze posiadał przyznane lokalnie uprawnienia administratora w tym zakresie, co było niezgodne z § 19 ust. 2 pkt 4 rozporządzenia KRI.

Jak wyjaśnił Kierownik Referatu IT prawa lokalnego administratora występują na niektórych stanowiskach (nie był wstanie określić całkowitej liczby) w Starostwie, fakt ten jest spowodowany tym, że niektóre oprogramowanie wymaga podniesienia uprawnień celem konfiguracji źródła danych.

Nieprawidłowość ta została usunięta w trakcie trwania kontroli.

(akta kontroli: str. 217-218)

2. Pomieszczenie serwerowni znajdujące się w Starostwie, w części dotyczącej zastosowanych zabezpieczeń fizycznych, było w niewystarczającym stopniu chronione, co zwiększało ryzyko ujawnienia, modyfikacji, usunięcia lub zniszczenia informacji, będących w posiadaniu Urzędu. Było to niezgodne z § 19 ust. 2 pkt 9 rozporządzenia KRI.

Kierownik Referatu Informatyki potwierdził, że zabezpieczenia fizyczne nie działały w chwili kontroli z powodów technicznych, a także, że w Starostwie nie prowadzi się rejestru zawierającą listę wejść i wyjść z serwerowni, ponieważ za każdym razem do pomieszczenia pobiera się klucze z referatu administracyjno-gospodarczego potwierdzając w rejestrze.

NIK wskazuje, że ewidencja wejść do serwerowni powinna obejmować obecność wszystkich osób (aby zachować rozliczalność), a nie tylko użytkownika pobierającego klucz z referatu administracyjno-gospodarczego. Osobie takiej mogą towarzyszyć inne, których nie obejmie stosowany w Urzędzie system.

(akta kontroli: str. 397-400)

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

Kierownik Referatu wyjaśnił, że w Zarządzeniu nr 6/2023 Starosty z dnia 23 stycznia 2023 r. w sprawie zatwierdzenia Planu Działalności zaplanowane zostały zadania dla komórek organizacyjnych w tym Referatu Informatyki takie jak ochrona danych osobowych, tworzenie zapasowych kopii bezpieczeństwa, czy też utrzymanie systemów informatycznych i sieci teleinformatycznej.

NIK wskazuje, że wyznaczenie zadań, wskazanie komórki organizacyjnej, czy też ustalenie wartości miernika nie były tożsame z określeniem elementów

procedury, związanej z ciągłością działania, dotyczącą zabezpieczenia pod kontem wpływu czynników zewnętrznych czy też wewnętrznych.

(akta kontroli: str.116)

OCENA CZĄSTKOWA

Wdrożone i wykorzystywane w Starostwie rozwiązania organizacyjne i techniczne nie zapewniały w pełni bezpieczeństwa informacji. Prawidłowo zidentyfikowane zostały kluczowe elementy infrastruktury i usługi IT oraz prawidłowo zabezpieczono urządzenia służbowe uniemożliwiające dostęp do danych na urządzeniach mobilnych. Jednakże Urząd nie zapewnił właściwego rozwiązania zapobiegającego możliwości instalacji nieautoryzowanego oprogramowania na komputerach w jednostce. Wszystkie zweryfikowane umowy serwisowe posiadały zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji.

Starostwo ustaliło także zasady tworzenia i przechowywania kopii zapasowych i były one tworzone regularnie oraz poddawane automatycznemu testowaniu. Natomiast pomieszczenie serwerowni było wykorzystywane w sposób niezapewniający odpowiedniej ochrony. Nadawanie i odbieranie uprawnień pracownikom do pracy w systemach informatycznych odbywało się za pomocą wdrożonej w Urzędzie procedury. We wszystkich badanych przypadkach zablokowano konta w systemach informatycznych osobom, które zakończyły zatrudnienie.

OBSZAR

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

3.1. W Starostwie w okresie kontroli przeprowadzano zewnętrzny, coroczny audyt, związany z utrzymaniem normy Systemu Zarządzania Jakością wg normy ISO 9001, który w swoim zakresie przewidział analizę integralności, poufności i dostępności. Zbieżność większości wymagań, określonych w standardach kontroli zarządczej, z wymaganiami normy ISO 9001 pozwoliła wdrożyć i utrzymać w Starostwie Zintegrowany System Zarządzania[27]. Urząd w raportach z przeglądu ZSZ wykonał analizę objętą planem postępowania w zidentyfikowanych ryzykach i potwierdzał działania, jednak nie uwzględniono w tej analizie w pełni wszystkich aspektów związanych integralnością, poufnością lub dostępnością informacji.

Należy podkreślić, że w szczególności uwzględnienie ryzyk związanych ze zjawiskami atmosferycznymi czy też czynnikami zewnętrznymi nie było wystarczające i należy przeprowadzić ponowną analizę ryzyka dla całego obszaru IT w ramach utraty integralności, poufności lub dostępności informacji.

(akta kontroli: str. 12-115, 119-130,509-510)

3.2. W Polityce bezpieczeństwa danych, zgodnie z § 19 ust. 2 pkt 13 rozporządzenia KRI, ustalono dla Starostwa sposób postępowania w przypadku naruszenia ochrony danych osobowych. W załączniku nr 9 do tego dokumentu wskazano m.in.: zasady zabezpieczenia dowodów zdarzenia, zasady przywrócenia stanu normalnego i oceny skutków dla ochrony danych, czy też zasadę zgłoszenia naruszenia i zawiadomienia osoby, której dane dotyczą.

IOD oświadczyła, że w okresie objętym kontrolą w Urzędzie wystąpił jeden incydent w zakresie bezpieczeństwa informacji i został on zgłoszony do Urzędu Ochrony Danych Osobowych, natomiast Starostwo w latach 2018-2022 odnotowało i zgłosiło łącznie pięć incydentów. We wszystkich przypadkach podjęto stosowne działania i zrealizowano postępowania naprawcze.

(akta kontroli: str. 12-41, 511-576)

3.3. W latach 2023-2024 w Starostwie nie realizowano szkoleń z zakresu bezpieczeństwa informacji, pomimo, że obowiązek ich przeprowadzania wynikał

[27] Dalej: ZSZ.

z § 19 ust. 2 pkt 6 rozporządzenia KRI, co opisano w sekcji *Stwierdzone nieprawidłowości*.

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

(akta kontroli: str. 577)

3.4. W 2023 r. w Urzędzie przeprowadzono okresowy audyt wewnętrzny, o którym mowa w § 19 ust. 2 pkt 14 rozporządzenia KRI. W wyniku tego audytu audytor sformułował rekomendacje. Nie wszystkie z tych rekomendacji zostały wdrożone, dotyczyło to w szczególności: 1. Opracowania procedury dotyczącej zachowania ciągłości, 2. Opracowania procedury wykonywania przeglądów, 3. Przeprowadzenia przez IOD szkoleń przypominających.

(akta kontroli: str. 578-615)

Stwierdzone nieprawidłowości

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

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

Sekretarz Powiatu wyjaśnił, że wszyscy nowo przyjęci pracownicy przechodzą odpowiednie szkolenia, natomiast w uzyskanej w ramach grantu dotacji przewidziano szkolenia w ramach bezpieczeństwa informacji dla wszystkich pracowników zatrudnionych w Urzędzie. Ponadto w 2024 r. w czwartym kwartale ujęto do planu w priorytetach szkoleniowych tematykę związaną z przetwarzaniem danych osobowych.

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

(akta kontroli: str. 577)

OCENA CZĄSTKOWA

W Starostwie przeprowadzono częściową analizę ryzyka utraty integralności, poufności oraz dostępności informacji. Należy jednak podkreślić, że w szczególności niewystarczające było uwzględnienie ryzyk związanych ze zjawiskami atmosferycznymi czy też czynnikami zewnętrznymi, w związku z czym należy przeprowadzić ponowną analizę ryzyka dla całego obszaru IT. Równocześnie wdrożono postępowanie w sytuacjach wystąpienia lub podejrzenia incydentu w zakresie bezpieczeństwa informacji. Zapewniono szkolenia tylko dla nowoprzyjętych pracowników, zaangażowanych w proces przetwarzania informacji. Przeprowadzono również w 2023 r. okresowy, coroczny audyt wewnętrzny z zakresu bezpieczeństwa informacji, niemniej jednak nie wykonano rekomendacji z tego audytu.

IV. Uwagi i wnioski

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

Uwagi

NIK zwraca uwagę, że charakter, waga i skala stwierdzonych nieprawidłowości wskazują na potrzebę wzmocnienia przez Starostę działań podejmowanych w obszarze kontroli zarządczej, o której mowa w art. 68 ust. 1 i 2 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych[28], w celu zapewnienia zgodnego z prawem, terminowego i efektywnego realizowania celów i zadań Urzędu w zakresie związanym z zapewnieniem bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych.

Wnioski

1. Wdrożenie jednolitego Systemu Zarządzania Bezpieczeństwa Informacji, wraz z Polityką Bezpieczeństwa Informacji, polityką ciągłości działania, planem ciągłości działania oraz planem odtworzeniowym.
2. Zapewnienie w procesie identyfikacji zbiorów danych podlegających zabezpieczeniu odpowiedniej wagi istotności, a tym samym poziomu ochrony.
3. Przeprowadzenie identyfikacji kluczowych elementów infrastruktury i usług IT oraz analizy ryzyka uwzględniającego konieczność zachowania ciągłości działania systemów informatycznych.
4. Bieżące aktualizowanie dokumentacji składającej się na SZBI w zakresie dotyczącym zmieniającego się otoczenia.
5. Ujednolicenie i objęcie administrowaniem zasobami sprzętowymi jak i oprogramowaniem przez służby informatyczne wszystkich komórek organizacyjnych Starostwa.
6. Właściwe zabezpieczenie pomieszczeń infrastruktury informatycznej (serwerowni).
7. Przeprowadzenie szkoleń dla pracowników Urzędu w zakresie bezpieczeństwa informacji.

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

V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

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

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

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

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

Wrocław, 18 września 2024 r.

Kontroler
Waldemar Zimoch
Główny specjalista kontroli państwowej

.....
podpis

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

.....
podpis