NAJWYŻSZA IZBA KONTROLI

DELEGATURA WE WROCŁAWIU

LWR.410.13.3.2024

Pan
Paweł Kleszcz
Starosta Lubiński
Starostwo Powiatowe w Lubinie
ul. Jana Kilińskiego 12 B
59-300 Lubin

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 Lubinie, ul. Jana Kilińskiego 12 B, 59-300 Lubin[1].
Kierownik jednostki kontrolowanej	Paweł Kleszcz, Starosta Lubiński[2], od 8 kwietnia 2022 r.
Zakres przedmiotowy kontroli	Rozwiązania organizacyjne i techniczne w zakresie zapewnienia bezpieczeństwa przetwarzania informacji oraz zapewnienia ciągłości działania w urzędzie i ich stosowanie.
Okres objęty kontrolą	Od 1 stycznia 2023 r. do dnia zakończenia kontroli w 2024 r.[3], (także okresy wcześniejsze w zakresie uczestnictwa w programie Cyfrowa Gmina/Cyfrowy Powiat).
Podstawa prawna podjęcia kontroli	Artykuł 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[4].
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura we Wrocławiu
Kontroler	Cezary Mazik, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LWR/86/2024 z dnia 3 czerwca 2024 r.

(akta kontroli: str. 1, 4)

[1] Dalej: Starostwo lub Urząd.
[2] Dalej: Starosta.
[3] Czynności kontrolne zakończono w dniu 28 sierpnia 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.

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

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

Właściwie wdrożono również rozwiązania organizacyjne i techniczne zapobiegające możliwości instalowania nieautoryzowanego oprogramowania oraz regularnie tworzono i testowano kopie zapasowe danych.

W toku kontroli stwierdzono jednak nieprawidłowości w każdym z trzech kontrolowanych obszarów, polegające na: **[1]** braku bieżącej aktualizacji SZBI wraz ze stwierdzanymi zmianami zachodzącymi w otoczeniu; **[2]** niezablokowaniu kont w systemach IT byłym pracownikom Urzędu; **[3]** ustaleniu wymogów dla haseł w jednym z systemów informatycznych niezgodnie z wymogami SZBI; **[4]** niedostatecznym zabezpieczeniu pomieszczenia serwerowni; **[5]** braku w umowie na zakup sprzętu IT wraz z oprogramowaniem postanowień gwarantujących odpowiedni poziom bezpieczeństwa informacji; **[6]** braku realizacji szkoleń z zakresu bezpieczeństwa informacji; **[7]** przeprowadzeniu w 2023 r. okresowego, corocznego audytu wewnętrznego z zakresu bezpieczeństwa informacji z naruszeniem zasad niezależności i obiektywności.

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

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

OBSZAR

1. Organizacja bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych

Opis stanu faktycznego

1.1. Identyfikacja zbiorów danych wymagających ochrony w Starostwie dokonywana była corocznie jako element szacowania ryzyka aktywów informacyjnych[11]. W jej ramach aktywa informacyjne były opisywane przez ich właścicieli (komórki organizacyjne), kwalifikowane do kategorii (I-IV) według istotności dla działalności Urzędu[12] oraz zidentyfikowano dla nich potencjalne zagrożenia.

Według stanu na 8 lipca 2024 r. w ramach przeprowadzonej inwentaryzacji zidentyfikowano 148 rodzajów aktywów informacyjnych w wersji papierowej oraz 196 w wersji elektronicznej przetwarzanej w Urzędzie, podlegającej ochronie.

Ponadto w Starostwie zidentyfikowano 96 zbiorów danych, w których przetwarzane są dane osobowe[13]. W procesie tym każdemu zbiorowi danych przypisano: komórkę organizacyjną, która wykorzystuje dane; podstawę prawną tworzenia zbioru; nazwę systemu lub oprogramowania, z którym dane są powiązane; cel przetwarzania danych; kategorię danych osobowych w tych zbiorach; kategorię osób, których dane dotyczą; kategorię odbiorców, którym dane osobowe zostały lub zostaną ujawnione; ogólny opis technicznych i organizacyjnych środków bezpieczeństwa; planowany termin usunięcia kategorii danych oraz informację czy dane osobowe podlegają przekazaniu do państw trzecich lub organizacji międzynarodowych.

(akta kontroli: str. 23-24)

1.2. W Starostwie opracowano i wdrożono SZBI, o którym mowa w § 19 ust. 1 rozporządzenia KRI.

SZBI stanowił część Księgi Zintegrowanego Systemu Zarządzania[14], wprowadzony do niej 10 sierpnia 2015 r.[15], gdzie definiowano bezpieczeństwo informacji w Urzędzie, wskazywano zakres uprawnień i odpowiedzialności związany z zarządzaniem bezpieczeństwem informacji, wskazywano osoby upoważnione do przetwarzania danych oraz wymagania prawne związane z bezpieczeństwem i ochroną informacji. Załącznikiem do tego dokumentu była Deklaracja stosowania wymagań normy ISO/IEC 27001[16], wskazująca na sposób realizacji w Starostwie działań według załącznika A – „Wzorcowy wykaz celów stosowania zabezpieczeń i zabezpieczenia", przedmiotowej normy.

Ponadto SZBI stanowiły także, m.in.:

- Polityka Bezpieczeństwa Informacji[17], będąca załącznikiem do zarządzenia Nr 75/2015 Starosty Lubińskiego z dnia 21 lipca 2015 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji Starostwa Powiatowego w Lubinie oraz PBI będąca załącznikiem do zarządzenia Nr 29/2024 Starosty Lubińskiego

[10] Oceny cząstkowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena cząstkowa może być sformułowana jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej.
[11] Zgodnie z zarządzeniem Nr 144/2018 Starosty Lubińskiego z dnia 20 września 2018 r. w sprawie procedury szacowania ryzyka aktywów informacyjnych w Starostwie Powiatowym w Lubinie. Dalej: Procedura szacowania ryzyka aktywów informacyjnych.
[12] Pod względem wymagań prawnych, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację.
[13] Wyszczególnione w Rejestrze czynności przetwarzania danych osobowych dla których Administratorem danych jest Starosta Lubiński (aktualizacja 31 maja 2024 r.).
[14] Dalej: KZSZ.
[15] Ostatnia aktualizacja 10 lipca 2024 r.
[16] Norma ISO/IEC 27001 - Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania; dalej: norma ISO/IEC 27001.
[17] Dalej: PBI.

z dnia 26 czerwca 2024 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Starostwie Powiatowym w Lubinie;
- PODO, będąca załącznikiem do zarządzenia Nr 52/2022 Starosty Lubińskiego z dnia 28 czerwca 2022 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych przetwarzanych w Starostwie Powiatowym w Lubinie;
- Instrukcja zarządzania systemem informatycznym, będąca załącznikiem nr 10 do PODO;
- Procedura szacowania ryzyka aktywów informacyjnych;
- Zasady gospodarowania mieniem, wprowadzone Uchwałą Nr 1/2022 Zarządu Powiatu Lubińskiego z dnia 12 stycznia 2022 r. w sprawie zasad gospodarowania mieniem powiatu pozostającym do dyspozycji jednostek;
- Regulamin określający zasady i procedury korzystania z legalnego oprogramowania, sprzętu komputerowego i sieci komputerowej oraz poczty elektronicznej, wprowadzony zarządzeniem Nr 38/2022 Starosty Lubińskiego z dnia 29 kwietnia 2022 r. w sprawie wprowadzenia Regulaminu określającego zasady i procedury korzystania z legalnego oprogramowania, sprzętu komputerowego i sieci komputerowej oraz poczty elektronicznej w Starostwie Powiatowym w Lubinie[18].

Zgodnie z postanowieniami PBI, właścicielem odpowiadającym za jej opracowanie, wdrożenie, ocenę, przegląd i modyfikację był Zespół ds. Bezpieczeństwa Informacji, w skład którego wchodzili: Sekretarz Powiatu[19], Pełnomocnik ds. Zintegrowanego Systemu Zarządzania, Inspektor Danych Osobowych[20], Kierownik Referatu Informatyki, wyznaczony pracownik Referatu Informatyki, Kierownik Biura Administracji oraz Kierownik Biura Kadr. PBI w momencie wprowadzenia została właściwie przedstawiona i zakomunikowana pracownikom.

(akta kontroli: str. 44-47 plik 4, 9-10, 17, 19, 48-49, 52)

1.3. Dokumentacja związana z ochroną danych osobowych uwzględniająca wymogi RODO została wprowadzona PODO oraz właściwie przedstawiona i zakomunikowana pracownikom.

PODO zawierała m.in: opis obszaru przetwarzania danych, opis rejestru czynności przetwarzania danych osobowych, sposób przepływu danych pomiędzy systemami, określenie środków technicznych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych, zasady korzystania z urządzeń przenośnych przetwarzających dane osobowe, procedurę postępowania w sytuacji naruszenia ochrony danych osobowych oraz zakres odpowiedzialności.

Załącznikiem do PODO były: Instrukcja postępowania w przypadku braku zasilania w serwerowni Starostwa Powiatowego oraz Instrukcja Zarządzania Systemem Informatycznym. Ta ostatnia instrukcja, zawierała dodatkowo procedury:
- nadawania, zmiany i rejestracji uprawnień;
- zarządzania i użytkowania metodami i środkami uwierzytelnienia;
- rozpoczęcia, zawieszenia i zakończenia pracy w systemie;
- tworzenia kopii zapasowych zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania;

[18] Zmieniony Zarządzeniem Nr 47/2022 Starosty Lubińskiego z dnia 1 czerwca 2022 r. zmieniającym Zarządzenie Nr 38/2022 Starosty Lubińskiego z dnia 29 kwietnia 2022 r. w sprawie wprowadzenia Regulaminu określającego zasady i procedury korzystania z legalnego oprogramowania, sprzętu komputerowego i sieci komputerowej oraz poczty elektronicznej w Starostwie Powiatowym w Lubinie. Dalej: Regulamin określający zasady i procedury korzystania z legalnego oprogramowania, sprzętu komputerowego i sieci komputerowej oraz poczty elektronicznej.
[19] Dalej: Sekretarz.
[20] Dalej: IOD.

- przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii programów i narzędzi programowych służących do ich przetwarzania;
- zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu;
- wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych.

(akta kontroli: str. 44-47 plik 9)

1.4. W okresie objętym kontrolą w Starostwie prowadzone były coroczne analizy ryzyka w związku z potrzebą zachowania ciągłości działania systemów informatycznych. Analizy te wykonywane były w ramach Procedury szacowania ryzyka aktywów informacyjnych. W jej ramach aktywa informacyjne były opisywane przez ich właścicieli (komórki organizacyjne), kwalifikowane do kategorii (I-IV) według istotności dla działalności Urzędu[21] oraz zidentyfikowano dla nich potencjalne zagrożenia. Następnie dokonywano oceny podatności aktywa/zasobu pod kątem poufności, integralności, dostępności, przypisywano im wagę zagrożeń, prawdopodobieństwo ich wystąpienia oraz wpływ (skutek) zmaterializowania się zagrożenia. Opisywano także ryzyko aktywa/zasobu, poziom zabezpieczeń, wpływ (skutek) materializowania się zagrożenia po zastosowaniu zabezpieczeń oraz określano ryzyko szczątkowe. Ocenie w ten sposób podlegały aktywa informacyjne w formie elektronicznej lub papierowej[22]. Ponadto w tym procesie dokonywano identyfikacji pracowników Starostwa na zarządzających zasobami oraz użytkowników zasobów, a także zasobów biorących udział w przetwarzaniu aktywów informacyjnych w postaci: komputerów stacjonarnych, komputerów przenośnych, telefonów stacjonarnych, telefonów komórkowych, pomieszczeń w których przetwarzano aktywa i urządzeń, w których je zabezpieczano oraz urządzeń peryferyjnych których używano (drukarki, skanery, niszczarki).

(akta kontroli: str. 23-24)

1.5. W Urzędzie nie opracowano osobnej polityki ciągłości działania, ale jej elementy były częścią obowiązującej PBI. W tym dokumencie zawarto cel zapewnienia ciągłości funkcjonowania usług związanych z przetwarzaniem danych, poprzez przeciwdziałanie przerwom w działalności oraz ochronę krytycznych procesów przed rozległymi awariami lub katastrofami. Jako procesy wspomagające politykę ciągłości działania opisano procedury tworzenia kopii zapasowych zbiorów danych osobowych oraz programów i narzędzi programowych do ich przetwarzania, a także wskazano sposób reagowania na zdarzenia mogące prowadzić do zaburzeń procesów przetwarzania danych[23]. Dokument ten (PBI, zawierająca elementy polityki ciągłości działania) został w momencie wprowadzenia właściwie przedstawiony i zakomunikowany pracownikom.

(akta kontroli: str. 44-47 plik 17, 19)

1.6. W Starostwie opracowano plany zapewnienia ciągłości działania oraz plany odtworzeniowe, które zawarto w Procedurze odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania, przyjętej zarządzeniem Nr 72/2018 Starosty Lubińskiego z dnia 16 maja 2018 r.[24] W przedmiotowym dokumencie opisano pięć procedur dotyczących: dysfunkcji systemu informatycznego, awarii krytycznych zależności (awarii sieci komputerowej), utraty

[21] Pod względem wymagań prawnych, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację.
[22] O których mowa w pkt. 1.1. niniejszego Wystąpienia pokontrolnego.
[23] To ostatnie tylko w PBI wprowadzonym zarządzeniem Nr 75/2015 Starosty Lubińskiego.
[24] W sprawie wprowadzenia procedur odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania. Dalej: Procedura odtwarzania techniki IT.

danych (usunięcia danych lub ich uszkodzenia), utraty pojedynczego centrum danych (serwerowni) oraz utraty całej lokalizacji. Dla każdego z tych scenariuszy opisano cel, przedmiot procedury, zakres zastosowania, odpowiedzialność i uprawnienia pracowników, szczegółowy sposób postępowania i aktualizacji planu. Dla dwóch scenariuszy przewidziano przeprowadzanie testów, bez wskazywania ich częstotliwości.

(akta kontroli: str. 44-47 plik 20)

1.7. W okresie objętym kontrolą, w Starostwie wykonano testy ciągłości działania, według scenariusza dysfunkcji systemu informatycznego, opisanego w Procedurze odtwarzania techniki IT. Przedmiotowy test przeprowadzono 2 marca 2023 r.[25] Następne testy zaplanowano w okresie wrzesień-październik 2024 r.

(akta kontroli: str. 31, 44-47 plik 16)

1.8. W okresie objętym kontrolą dokonywano przeglądu aktualności dokumentacji SZBI. Czynność tą wykonał 6 października 2023 r. oraz 11 marca 2024 r. zespół, w skład którego wchodzili: Sekretarz, Pełnomocnik ds. Zintegrowanego Systemu Zarządzania, IOD, Kierownik Referatu Informatyki oraz Kierownik Biura Administracji, a jego wyniki zostały udokumentowane.

W obu dokonanych przeglądach stwierdzono konieczność aktualizacji dokumentacji dotyczącej PBI, lecz działania te podjęto dopiero w czasie niniejszej kontroli NIK, co opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli: str. 44-47 plik 50-51)

1.9. Osobami odpowiedzialnymi za bezpieczeństwo informacji oraz zapewnienie ciągłości działania w Starostwie byli IOD, Kierownik Referatu Informatyki oraz Administrator Systemów Informatycznych[26]. Zadania te wynikały zarówno z zakresu obowiązków na tych stanowiskach pracy, jak i zarządzeń wewnętrznych, które włączono do akt pracowniczych.

Z zakresu czynności Kierownika Referatu Informatyki wynikały zadania związane m. in. z: nadzorem i administrowaniem systemami informatycznymi oraz infrastrukturą informatyczną; nadzorem nad bezpieczeństwem i ochroną danych systemów informatycznych; nadzorem i szkoleniem użytkowników z zasad i procedur bezpieczeństwa; opracowanie planów awaryjnych i planów napraw systemów; nadzór nad prowadzeniem prac zleconych firmom zewnętrznym oraz wykonywanie zadań Inspektora Bezpieczeństwa Teleinformatycznego[27]. Przy czym do zadań IBT należały: weryfikacja i bieżąca kontrola zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzeganie procedur bezpiecznej eksploatacji; udział w procesie zarządzania ryzykiem w systemie informatycznym, weryfikując poprawność realizacji zadań administratora, w tym właściwe zarządzanie konfiguracją oraz uprawnieniami przydzielonymi użytkownikom, stan zabezpieczeń systemu teleinformatycznego, w tym analizując rejestry zdarzeń systemu teleinformatycznego.

Natomiast ASI był odpowiedzialny za funkcjonowanie systemu informatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa, przewidzianych dla systemu teleinformatycznego. Jego zadaniem był także udział w tworzeniu dokumentacji bezpieczeństwa systemu teleinformatycznego oraz w procesie zarządzania ryzykiem w systemie teleinformatycznym, realizując szkolenia użytkowników systemu teleinformatycznego, utrzymując zgodność systemu teleinformatycznego z jego

[25] Test powiódł się, system przywrócono, nie stwierdzono potrzeby modyfikacji procedury/testu.
[26] Dalej: ASI.
[27] Dalej: IBT.

dokumentacją bezpieczeństwa oraz wdrażając zabezpieczenia w systemie teleinformatycznym. Z kolei z zakresu czynności IOD wynikało m. in. monitorowanie zagrożeń związanych z bezpieczeństwem informacji, a dodatkowo w procesie zarządzania ryzykiem w systemie teleinformatycznym podlegali mu IBT i ASI.

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

(akta kontroli: str. 20-21, 44-47 plik 3, 5, 7-8)

1.10. Zgodnie z art. 37 ust. 1 i 5 RODO i art. 8 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[28], Starosta wyznaczył[29] Pełnomocnika ds. Informacji Niejawnych, będącą pracownikiem Urzędu, do pełnienia funkcji IOD. Osoba ta posiadała odpowiednie kwalifikacje do pełnienia tej funkcji, potwierdzone świadectwem ukończenia studiów podyplomowych w zakresie „Inspektor ochrony danych osobowych". Zakres obowiązków w zakresie IOD obejmował zadania związane z ochroną i zabezpieczeniem danych osobowych, w tym m.in. zadania określone w art. 39 ust. 1 RODO.

(akta kontroli: str. 20-21, 44-47 plik 7-8)

1.11. Zgodnie z regulaminem organizacyjnym Urzędu[30], Pełnomocnik ds. Informacji Niejawnych, będący równocześnie IOD, podlegał bezpośrednio Staroście, co było zgodne z art. 38 ust. 3 RODO[31].

W zakresie obowiązków pracownika pełniącego funkcję IOD wskazano czynności związane także z realizacją zadań dotyczących informacji niejawnych oraz monitorowaniem zagrożeń związanych z bezpieczeństwem informacji. Zadania te nie powodowały konfliktu interesów, o którym mowa w art. 38 ust. 6 RODO.

(akta kontroli: str. 20-21)

1.12. Zgodnie z art. 21 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[32], zarządzeniem Nr 97/2021 Starosty Lubińskiego z 6 października 2021 r. wyznaczono Kierownika Referatu Informatyki jako osobę odpowiedzialną za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Dane wyżej wymienionej osoby zostały przekazane 7 października 2021 r. do CSIRT-NASK[33], tj. w terminie zgodnym z art. 22 ust. 1 pkt 5 ustawy o ksc[34].

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. 44-47 plik 6, 11, 21)

---

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

[29] Zarządzeniem Nr 73/2018 Starosty Lubińskiego z 22 maja 2018 r. w sprawie powołania Inspektora Ochrony Danych w Starostwie Powiatowym w Lubinie oraz Zarządzeniem nr 48/2023 Starosty Lubińskiego z 7 sierpnia 2023 r. w sprawie powołania Inspektora Ochrony Danych w Starostwie Powiatowym w Lubinie.

[30] Uchwała nr 153/2022 Zarządu Powiatu Lubińskiego z dnia 29 czerwca 2022 r. w sprawie uchwalenia Regulaminu Organizacyjnego Starostwa Powiatowego w Lubinie, ze zmianami.

[31] W którym wskazano, że IOD podlega bezpośrednio najwyższemu kierownictwu administratora danych lub podmiotu przetwarzającego.

[32] Dz. U. z 2024 r. poz. 1077, ze zm., dalej: ustawa o ksc.

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

[34] Tj. w terminie 14 dni od dnia wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.

1.13. Wymienione w PBI[35], w pkt. 5.1 *Dokumentacja SZBI,* regulacje wewnętrzne stanowiące szczegółowe dokumenty wykonawcze i procedury zostały sporządzone. Były to w szczególności:

- instrukcja zarządzania systemem informatycznym;
- procedura szacowania ryzyka aktywów informacyjnych;
- procedura odtwarzania techniki IT;
- zarządzenie Nr 23/2022 Starosty Lubińskiego z 16 marca 2022 r. w sprawie powołania Inspektora Bezpieczeństwa Teleinformatycznego oraz Administratora Systemu Informatycznego w Starostwie Powiatowym w Lubinie;
- regulamin określający zasady i procedury korzystania z legalnego oprogramowania, sprzętu komputerowego i sieci komputerowej oraz poczty elektronicznej.

(akta kontroli: str. 44-47 plik 19)

1.14. Starostwo posiadało pełną informację o zasobach informatycznych obejmujących ich rodzaj oraz konfigurację, co spełniało wymogi § 19 ust. 2 pkt 2 rozporządzenia KRI.

Prowadzono rejestr zasobów informatycznych w arkuszu kalkulacyjnym, który obejmował podstawowe informacje, takie jak: zasoby sprzętowe, dyskowe, adresację IP, adresy MAC, nazwy, numery inwentarzowe sprzętu, klucze licencji, lokalizację sprzętu, nazwy użytkowników, rodzaje dysków, procesory, pamięć RAM, daty audytów oraz inne uwagi.
Ponadto wdrażano oprogramowanie do automatycznej inwentaryzacji zasobów informatycznych. Według stanu na 24 czerwca 2024 r. pozwalało to na przeprowadzanie inwentaryzacji 47,5% użytkowanych zasobów, a jego wdrożenie ma zostać zakończone do 31 sierpnia 2024 r.

W toku przeprowadzonych oględzin na próbie 10 komputerów, w tym jednego laptopa oraz jednego serwera, jednego routera i jednej drukarki stwierdzono, że wdrażany system nie inwentaryzował serwerów, a dla pozostałych urządzeń pozwalał uzyskać aktualne dane m.in. w zakresie zainstalowanego oprogramowania, sprzętu, konfiguracji systemu oraz osoby odpowiedzialnej/użytkownika.

(akta kontroli: str. 18, 27, 31, 44-47 plik 12)

1.15. W okresie objętym kontrolą Urząd przystąpił do rządowego programu „Cyberbezpieczny Samorząd", realizując projekt „Cyberbezpieczny Samorząd dla Powiatu Lubińskiego". Według stanu na dzień 28 sierpnia 2024 r. umowa o wartości 1 048 826,00 zł[36] na realizację grantu była w trakcie podpisywania przez strony, a czas jej realizacji miał zostać określony na 24 miesiące.

Celem i efektami tego projektu mają być poprawa cyberbezpieczeństwa, obejmująca obszar organizacyjny, kompetencyjny i techniczny oraz zminimalizowanie zagrożeń i skutków ataków, tworząc bezpieczne środowisko informatyczne dla samorządu i jego mieszkańców. W tym celu zaplanowano w poszczególnych obszarach:

- organizacyjnym – przeprowadzenie audytów bezpieczeństwa informacji i SZBI Starostwa;
- kompetencyjnym – przeprowadzenie łącznie sześciu szkoleń dedykowanych informatykom, kadrze kierowniczej i pracownikom Starostwa z zakresu cyberbezpieczeństwa i dostarczonych rozwiązań IT;

[35] Wprowadzona zarządzeniem Nr 29/2024 Starosty Lubińskiego z dnia 26 czerwca 2024 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Starostwie Powiatowym w Lubinie.
[36] W tym 849 548,86 zł dofinansowania oraz 199 277,14 zł wkład własny.

- technicznym – zakup urządzeń i oprogramowania wraz z ich wdrożeniem w celu budowy zapasowej serwerowni oraz wymiany urządzeń sieciowych, w postaci serwerów, urządzeń do tworzenia kopii zapasowych danych, macierzy dyskowych, urządzeń typu: firewall, switch, acces point, UPS[37] oraz oprogramowania do zarządzania urządzeniami końcowymi i oprogramowania NAC[38],

W ramach oceny realizacji tego Projektu przewidziano ewaluację według kryteriów „Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego".

(akta kontroli: str. 43, 44-47 plik 13)

Stwierdzone nieprawidłowości

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

Do 26 czerwca 2024 r. (w zakresie dotyczącym PBI[39]) oraz do 10 lipca 2024 r. (w zakresie dotyczącym KZSZ[40]) nie dokonywano aktualizacji dokumentacji SZBI, pomimo stwierdzenia takiej konieczności podczas wykonywanych kolejnych przeglądów[41], o których mowa w § 19 ust. 1 rozporządzenia KRI.

Dotyczyło to przede wszystkim:

- deklaracji zgodności PBI i KZSZ z normą ISO/IEC 27001:2007, która od 2014 r. została zastąpiona normą ISO/IEC 27001:2013;
- powoływania się w PBI i KZSZ na postanowienia Polityki Bezpieczeństwa Danych Osobowych, która została zastąpiona PODO w dniu 28 czerwca 2022 r.;
- powoływania się w KZSZ na uregulowania *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych*, która to po wejściu w życie PODO została zastąpiona *Instrukcją zarządzania systemem informatycznym*.

Starosta przyznał, że podczas dokonywanych przeglądów zidentyfikowano potrzebę aktualizacji dokumentów SZBI, ale jej wykonanie odłożono w czasie ze względu na odbywające się wybory do Sejmu i Senatu oraz późniejsze wybory do samorządów. Okres przedwyborczy i wybory wymagały bowiem, jego zdaniem, zaangażowania wielu kluczowych pracowników, co znacznie wpłynęło na ich dostępność.

NIK wskazuje, że wymienione wyżej dokumenty SZBI zdezaktualizowały się jeszcze przed okresem kontroli NIK, tj. w 2014 r. i w 2022 r., a więc było wystarczająco dużo czasu, aby dokonać przedmiotowej aktualizacji jeszcze przed wskazanymi wyborami odbywającymi się w 2023 r.

(akta kontroli: str. 27, 30-31, 44-47 plik 4, 9-10, 17, 19, 48-52)

OCENA CZĄSTKOWA

W badanym okresie stosowano dokumentację składającą się na SZBI i PODO, uwzględniającą wymogi odpowiednio rozporządzenia KRI oraz RODO. Mimo tego nie dokonywano bieżącej aktualizacji SZBI w ślad za stwierdzanymi zmianami zachodzącymi w otoczeniu.

Ponadto w Starostwie prawidłowo zidentyfikowano zbiory danych podlegających zabezpieczeniu oraz kluczowe elementy infrastruktury i usług IT. Prowadzono także niezbędne analizy ryzyka oraz sporządzono odpowiednią dokumentację w celu m.in. zapewnienia ciągłości działania.

[37] Zasilacz awaryjny, zasilacz bezprzerwowy, zasilacz UPS (ang. uninterruptible power supply – zasilacz bezprzerwowy).
[38] NAC (Network Access Control) - system kontroli dostępu do sieci korporacyjnej.
[39] Ukazanie się zarządzenia Nr 29/2024 Starosty Lubińskiego z dnia 26 czerwca 2024 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Starostwie Powiatowym w Lubinie.
[40] Data dokonania ostatniej aktualizacji KZSZ.
[41] Zrealizowanych 6 października 2023 r. oraz 11 marca 2024 r.

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

Opis stanu faktycznego

2.1. Przyjęte w Urzędzie rozwiązanie, polegające na nieprzyznawaniu użytkownikom uprawnień administracyjnych do systemu operacyjnego, zapobiegało możliwości instalowania nieautoryzowanego oprogramowania przez pracowników na komputerach służbowych. Próba dokonania zainstalowania nieautoryzowanego oprogramowania przeprowadzona[42] na dziesięciu komputerach (siedmiu stacjonarnych oraz trzech laptopach[43]) nie powiodła się, co było zgodne z0 wymaganiami wynikającymi z § 19 ust. 2 pkt 4 rozporządzenia KRI.

Według wyjaśnień Starosty, tablety i smartfony służbowe używane przez pracowników Starostwa służą tylko i wyłącznie do wykonywania lub odbierania połączeń telefonicznych oraz wykonywania i odbierania wiadomości tekstowych. Dodatkowo każdy pracownik odbierający tablet lub smartfon podpisuje umowę o indywidualnej odpowiedzialności za powierzone mienie, w której to umowie zobowiązuje się do sprawowania pieczy nad powierzonym mieniem. Dodał także, że rozważane jest aktualnie wdrożenie zabezpieczania tabletów i smartfonów, przed instalacją na nich dowolnego oprogramowania.

(akta kontroli: str. 22-33)

2.2. Obowiązek dotyczący podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w sposób adekwatny do realizowanych przez nie zadań był realizowany prawidłowo.

Nadanie uprawnień do dostępu do systemów IT oraz ich odebranie w Starostwie następowało na podstawie sformalizowanego wniosku o wydanie upoważnienia do przetwarzania danych osobowych, wynikającego z PODO (oraz z obowiązującej SZBI). Wniosek ten był sporządzany w momencie rozpoczęcia pracy lub jej zakończenia (wraz z kartą obiegową) przez pracownika.

W wyniku przeprowadzonego badania adekwatności uprawnień w systemach informatycznych 15 pracowników Starostwa[44], nie stwierdzono by posiadane przez nich uprawnienia wykraczały poza zakres ich obowiązków wynikający z zakresów czynności, co było zgodne z § 19 ust. 2 pkt 4 rozporządzenia KRI.

(akta kontroli: str. 10-17)

2.3. Badanie przeprowadzone na próbie 15 pracowników, którzy zakończyli zatrudnienie po 1 stycznia 2023 r.[45], wykazało, że pięciu z nich nadal posiadało aktywne konta w systemie informatycznym, co opisano w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli: str. 10-17)

2.4. Obowiązujące w Starostwie zasady nadawania haseł, zawarte w Instrukcji zarządzania systemem informatycznym, określały minimalną liczbę znaków oraz złożoność hasła.

[42] 5 lipca 2024 r.

[43] Według oświadczenia Kierownika Referatu Informatyki sprawdzeniu podlegały wszystkie pracujące w momencie prowadzenia oględzin laptopy.

[44] Według stanu na 24 czerwca 2024 r. próba ta stanowiła 10,7% wszystkich osób zatrudnionych w Urzędzie i użytkujących systemy IT.

[45] Według stanu na 24 czerwca 2024 r. próba ta stanowiła 71,4% wszystkich osób kończących zatrudnienie.

Oględziny trzech systemów informatycznych zarządzanych przez Starostwo wykazały jednak, że w jednym przypadku system nie wymuszał na użytkownikach wymagań dla haseł dostępu, co opisano w sekcji *Stwierdzone nieprawidłowości*.

Stosowane w badanych systemach loginy nie były uniwersalne[46] i nie wskazywały na wykorzystanie ich przez kilku użytkowników.

(akta kontroli: str. 18-19, 44-47 plik 9, 48-49)

2.5. Sprawdzenie usytuowania monitorów sześciu stanowisk przeprowadzone w salach obsługi klientów w Biurze Komunikacji Starostwa, gdzie na komputerach zainstalowane było oprogramowanie CEPiK[47], wykazało, że we wszystkich przypadkach usytuowanie monitorów uniemożliwiało wgląd do danych przez osoby nieupoważnione. Stan ten był zgodny z wymaganiami wynikającymi z § 19 ust. 2 pkt 7 rozporządzenia KRI.

(akta kontroli: str. 22)

2.6. W Urzędzie opracowano zasady korzystania ze służbowych komputerów przenośnych poza miejscem pracy, które stanowiły załącznik do PODO, co było zgodne z § 19 ust. 2 pkt 8 rozporządzenia KRI.

Zgodnie z powyższymi zasadami pracownicy mieli obowiązek m.in.: wystąpić o zgodę na używanie komputera poza miejscem pracy, zachowania w tajemnicy identyfikatora i haseł do systemów, zakazu korzystania z komputerów w miejscach publicznych oraz ich transportowania w sposób minimalizujących ryzyko kradzieży bądź zniszczenia.

(akta kontroli: str. 44-47 plik 9, 48-49)

2.7. Według wyjaśnień przekazanych przez Starostę komputery przenośne były zabezpieczone przed dostępem osób nieuprawnionych poprzez oprogramowanie szyfrujące dyski twarde. Spełniało to wymogi § 19 ust. 2 pkt 9 i 11 rozporządzenia KRI.

(akta kontroli: str. 29, 33)

2.8. Serwerownia Starostwa zlokalizowana była w odrębnym, nieoznaczonym i klimatyzowanym pomieszczeniu, do którego dostęp mieli informatycy, a wejścia były rejestrowane. Posiadała ona wydzieloną instalację elektryczną i nie przechowywano w niej materiałów zagrażających infrastrukturze IT. Niemniej, pomieszczenie to nie posiadało należytych zabezpieczeń, o czym szerzej w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli: str. 6-7)

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

(akta kontroli: str. 5, 25-26, 44-47 plik 1)

2.10. W Starostwie opracowano procedurę dotyczącą przekazywania sprzętu informatycznego poza jednostkę, określającą postępowanie służb informatycznych w sytuacji wydania urządzeń komputerowych zewnętrznemu serwisowi lub jego zbycia, będącą częścią Instrukcji zarządzania systemem informatycznym.

Zgodnie z nią przekazanie sprzętu do naprawy poza jednostkę lub jego zbycie wymagało usunięcia danych, a w przypadku serwisu dokonywanego na terenie jednostki wymagany był nadzór ze strony służb informatycznych.

(akta kontroli: str. 44-47 plik 9, 48-49)

[46] Konstrukcja loginów pozwalała na prostą identyfikację użytkowników.
[47] Centralna Ewidencja Pojazdów i Kierowców.

2.11. Zasady stanowiące politykę kopii zapasowych zostały opisane w Instrukcji zarządzania systemem informatycznym. Określały one organizację oraz sposób archiwizacji danych (tworzenia kopii zapasowych), miejsce i okres ich przechowywania, odpowiedzialność oraz osoby mające do nich dostęp. Ponadto określono sposób postępowania z nośnikami wyłączonymi z użytkowania i zasady testowania kopii bezpieczeństwa.

(akta kontroli: str. 44-47 plik 9, 48-49)

2.12. W toku oględzin[48] ustalono, że kopie zapasowe danych tworzone były zgodnie z zasadami, określonymi w Instrukcji zarządzania systemem informatycznym. tj. wykonywane były na dostępnych zasobach dyskowych znajdujących się w serwerowni Starostwa oraz na dyskach zewnętrznych USB, z częstotliwością zgodną z aktualnym grafikiem tworzenia kopii zapasowych[49]. Wykonane kopie na bieżąco odnotowywane były w dzienniku wykonywania kopii zapasowych, w którym odnotowywano również przeprowadzenie testu kopii (raz w miesiącu).

Kopie zapasowe wykonane na zasobach dyskowych znajdowały się na serwerach w pomieszczeniu serwerowni, a dyski zewnętrzne USB przechowywane były prawidłowo w zamkniętej metalowej kasetce w szafie stalowej. Przeprowadzony w trakcie oględzin test na odzyskiwanie danych z wybranej kopii zapasowej[50] zakończył się poprawnym przywróceniem danych.

Zabezpieczenie serwerów archiwizacyjnych i dysków zewnętrznych USB spełniało wymogi wynikające z § 19 ust. 2 pkt 7 oraz § 19 ust. 2 pkt 12 lit. b i e rozporządzenia KRI.

(akta kontroli: str. 8-9)

2.13. W Starostwie nie przyjęto formalnej procedury monitorowania pojemności nośników pamięci masowych, wykorzystywanych w serwerach Monitoring taki był prowadzony ręcznie przez informatyków. Przeprowadzony w trakcie oględzin[51] test zajętości dysków twardych na trzech serwerach wykazał, że ich zajętość wynosiła odpowiednio 35%, 57% i 81%.

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

(akta kontroli: str. 18-19)

2.14. W ramach zapewnienia ciągłości działania Urzędu zidentyfikowano kluczowe elementy infrastruktury IT oraz kluczowe usługi IT, wykorzystywane w jednostce. Identyfikacja ta dokonywana była corocznie jako element szacowania ryzyka aktywów informacyjnych. W dokumentacji ciągłości działania nie wskazano czasu przywrócenia poszczególnych systemów oraz procesów do działania. W złożonych wyjaśnieniach Sekretarz Powiatu stwierdził, że dokładne określenie czasu przywrócenia poszczególnych systemów oraz procesów do działania jest niezwykle trudne, m.in. z powodu warunków w jakich proces ten będzie przeprowadzany; wielkości zasobów przyrastających z dnia na dzień oraz aktualizacji dostarczanych przez zewnętrznych dostawców.

(akta kontroli: str. 23-24, 38, 41, 44-47 plik 9, 20, 48-49)

[48] Przeprowadzonych 17 czerwca 2024 r.
[49] W dokumencie tym wskazano sposób (wskazanie serwera i foldera tworzenia kopii) oraz częstotliwość tworzenia kopii zapasowych (codziennie, tygodniowo, miesięcznie).
[50] Baza danych systemu z 23 kwietnia 2024 r.
[51] 24 czerwca 2024 r.

Stwierdzone nieprawidłowości

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

1. Pięciu z 15 objętych badaną próbą byłych pracowników, pomimo zakończenia zatrudnienia w Starostwie, nie miało zablokowanego dostępu do systemów informatycznych, co było niezgodne z § 19 ust. 2 pkt 5 rozporządzenia KRI oraz Rozdziałem II ust. 2 pkt 3 Instrukcji zarządzania systemem informatycznym.

Badanie przeprowadzone 24 czerwca 2024 r. wykazało, że w jednym z testowanych systemów aktywne konto miało dwóch zwolnionych pracowników, a w drugim pięciu zwolnionych pracowników[52]. Wszystkie te konta zostały zablokowane w czasie prowadzenia przedmiotowego badania.

Starosta wyjaśnił, że wszyscy pracownicy, o których mowa, mieli zablokowany dostęp w domenie Active Directory[53], co uniemożliwiało zalogowanie się im do stacji roboczej, a tym samym do systemów informatycznych Starostwa.

Należy podnieść, że zgodnie ze wskazanymi przepisami wewnętrznymi zablokowanie dostępu do systemu informatycznego polega na unieważnieniu hasła, zablokowaniu konta użytkownika oraz odebraniu wszelkich uprawnień do zasobów systemu, przypisanych do tego konta lub likwidację konta. Zatem samo zablokowanie dostępu w domenie AD nie spełnia tych wymogów i nie może być traktowane jako prawidłowe zrealizowanie procedury zablokowania dostępu.

(akta kontroli: str. 10-17, 28, 31, 44-47 plik 9, 48-49)

2. Oględziny trzech systemów informatycznych zarządzanych przez Starostwo wykazało, że w jednym przypadku system nie wymuszał na użytkownikach wymagań dla haseł dostępu, co było niezgodne z § 19 ust. 2 pkt 7 lit. c rozporządzenia KRI oraz Rozdziałem III ust. 1 i 3 Instrukcji zarządzania systemem informatycznym.

Przedmiotowy system mimo takich możliwości w chwili prowadzenia oględzin[54] nie miał aktywnego wymuszania stosowania wymagań dotyczących jakości i złożoności hasła oraz czasu jego ważności. W czasie prowadzenia oględzin opcja ta została włączona.

Starosta przyznał, że po aktualizacji przedmiotowego programu do nowszej wersji system wyłączył automatyczną opcję wymuszania zmiany haseł, która została przywrócona.

(akta kontroli: str. 18-19, 28, 31, 44-47 plik 9, 48-49)

3. W pomieszczeniu serwerowni Starostwa brak było adekwatnych zabezpieczeń[55], co stwarzało potencjalne zagrożenie włamania i narażenia na zniszczenie lub nieuprawniony dostęp do aktywów informacyjnych i było niezgodne z § 19 ust. 2 pkt 9 rozporządzenia KRI.

Starosta wyjaśnił, że usytuowanie serwerowni i sposoby jej dozoru zmniejszają ryzyko włamania.

Należy jednak podkreślić, że wskazane przez Starostę zabezpieczenia nie eliminują jednak ryzyka włamania do tego pomieszczenia.

(akta kontroli: str. 6-7, 28, 31-32)

4. W treści umowy na zakup i dostawę Firewall z Acces Point wraz z systemem do zarządzania urządzeniami końcowymi z 11 grudnia 2023 r., nie zawarto postanowień gwarantujących odpowiedni poziom bezpieczeństwa informacji, co było niezgodne z § 19 ust. 2 pkt 10 rozporządzenia KRI.

[52] W tym dwóch którzy mieli aktywne konto w pierwszym systemie.
[53] Dalej: AD.
[54] 24 czerwca 2024 r.
[55] O szczegółach Starosta został powiadomiony pismem LWR.410.13.3.2024 z 18 lipca 2024 r. (pkt 6).

Wykonawca przedmiotowej umowy objął jej wykonanie 24 miesięczną gwarancją oraz rękojmią, mogąc mieć dostęp do urządzenia, oprogramowania, a przez to aktywów informacyjnych Starostwa.

Starosta wyjaśnił, że w dniu 30 lipca 2024 r. do Biura Prawnego Starostwa wystosowane zostało pismo dotyczące sporządzenia aneksu do przedmiotowej umowy, obejmujące zawarcie w niej postanowień gwarantujących odpowiedni poziom bezpieczeństwa informacji.

(akta kontroli: str. 5, 25-26, 28, 32, 44-47 plik 1)

OCENA CZĄSTKOWA

W badanym okresie w Starostwie sporządzono odpowiednią dokumentację w celu m.in. określenia bezpiecznych zasad pracy zdalnej, określenia zasad tworzenia i przechowywania kopii zapasowych, nadawania i odbierania pracownikom uprawnień do pracy w systemach informatycznych. Właściwie wdrożono również rozwiązania organizacyjne i techniczne zapobiegające możliwości instalowania nieautoryzowanego oprogramowania oraz regularnie tworzono i testowano kopie zapasowe danych. Niemniej w toku kontroli stwierdzono nieprawidłowości polegające na: niezablokowaniu kont w systemach IT byłym pracownikom Urzędu; ustaleniu wymogów dla haseł w jednym z systemów informatycznych niezgodnie z wymogami SZBI; niedostatecznym zabezpieczeniu pomieszczeń serwerowni; oraz braku w umowie na zakup sprzętu IT wraz z oprogramowaniem postanowień gwarantujących odpowiedni poziom bezpieczeństwa informacji.

OBSZAR

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

3.1. Zgodnie z przyjętą Procedura szacowania ryzyka aktywów informacyjnych, w 2023 r. i 2024 r. przeprowadzono w Starostwie analizę ryzyka utraty integralności, poufności lub dostępności informacji. W jej ramach aktywa informacyjne były opisywane przez ich właścicieli (komórki organizacyjne), kwalifikowane do kategorii (I-IV) według istotności dla działalności Urzędu[56] oraz zidentyfikowano dla nich potencjalne zagrożenia. Następnie dokonywano oceny podatności aktywa/zasobu pod kątem poufności, integralności, dostępności, przypisywano im wagę zagrożeń, prawdopodobieństwo ich wystąpienia oraz wpływ (skutek) zmaterializowania się zagrożenia. Opisywano także ryzyko aktywa/zasobu, poziom zabezpieczeń, wpływ (skutek) materializowania się zagrożenia po zastosowaniu zabezpieczeń oraz określano ryzyko szczątkowe. Na ich podstawie wyliczano wartość punktową dla każdego aktywa i porównywano ją z wartością jaką przyjęto dla poziomu akceptowalnego. Przekroczenie określonego wyznaczoną wartością progu rodziło obowiązek podjęcia działań korygujących mających na celu minimalizację ryzyka do poziomu akceptowalnego. W wyniku przeprowadzanych analiz w okresie objętym kontrolą, stwierdzono, że wszystkie zagrożenia jakie występowały były na poziomie akceptowalnym.

(akta kontroli: str. 23-24, 38, 41-42)

3.2. W Starostwie w przypadku wystąpienia incydentów w zakresie bezpieczeństwa informacji zastosowanie miała Procedura postępowania w sytuacji naruszenia danych osobowych (załącznik do PODO). W dokumencie tym wskazano sytuacje stanowiące naruszenie bezpieczeństwa informacji, zasady postępowania w przypadku ich stwierdzenia lub podejrzenia ich zaistnienia oraz odpowiedzialność poszczególnych osób uczestniczących w tym procesie.

W okresie objętym kontrolą w Starostwie wystąpiły dwa incydenty w zakresie bezpieczeństwa informacji, jeden dotyczył awarii zasilania w budynku Starostwa,

[56] Pod względem wymagań prawnych, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację.

a drugi zagubienia korespondencji z danymi osobowymi przez operatora pocztowego. W obu tych przypadkach podjęto stosowne działania i zrealizowano postępowania naprawcze.

(akta kontroli: str. 44-47 plik 2, 9, 48-49)

3.3. W latach 2023 – 2024 w Starostwie nie realizowano szkoleń z zakresu dotyczącym bezpieczeństwa informacji, pomimo że obowiązek przeprowadzania takich szkoleń wynikał z przepisów rozporządzenia KRI, co zostało opisane w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli: str. 28, 32-33)

3.4. Audyty wewnętrzne, o których mowa w § 19 ust. 2 pkt 14 rozporządzenia KRI, były wykonywane w okresie objętym kontrolą przez IOD, co naruszało zasady niezależności oraz obiektywności audytu i zostało opisane w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli: str. 44-47 plik 22-47)

Stwierdzone nieprawidłowości

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

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

Starosta wyjaśnił, że PBI z 2015 roku była rozpowszechniona za pośrednictwem poczty elektronicznej w trybie zwyczajowo przyjętym w Starostwie, a w latach 2023-2024 nowozatrudnieni pracownicy Starostwa przechodzili obowiązkowe szkolenia z ochrony danych osobowych z uwzględnieniem bezpieczeństwa informacji. Przyznał jednak, że samo oświadczenie o zapoznaniu z przepisami dotyczącymi ochrony danych osobowych nie obejmowało zapisów dotyczących zapoznania z przepisami dotyczącymi bezpieczeństwa informacji. Dodał również, że aktualna PBI rozpowszechniona została w dniu 26 czerwca 2024 r. za pośrednictwem poczty elektronicznej, a w przygotowaniu jest wersja zarządzenia wprowadzającego PBI z obowiązkiem wypełnienia oświadczenia o zapoznaniu się z treścią ww. dokumentu. Zadeklarował także, że wszyscy nowo zatrudniani pracownicy Starostwa, po ukończeniu szkolenia z ochrony danych osobowych będą również szkoleni w zakresie znajomości PBI, co będzie potwierdzone podpisaniem stosownego oświadczenia.

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

(akta kontroli: str. 28, 32-33)

2. Audyty wewnętrzne, o których mowa w § 19 ust. 2 pkt 14 rozporządzenia KRI, były wykonywane przez IOD, co naruszało zasady niezależności i obiektywności audytu.

W związku z faktem, że w zakresie bezpieczeństwa informacji, na mocy obowiązujących w Starostwie regulacji, zastosowanie mają reguły dotyczące ochrony danych osobowych, w tym przede wszystkim PODO wraz z Instrukcją zarządzania systemem informatycznym, IOD dokonuje audytu obszaru, za który odpowiada. Ponadto przedmiotowe audyty w swoim zakresie mają wskazane także „bezpieczeństwo informacji" i oceniają spełnianie przepisów rozporządzenia KRI. Narusza to zasady niezależności i obiektywności audytu określone w *Standardach*

audytu wewnętrznego dla jednostek finansów publicznych[57] oraz w pkt 9.2 lit. e ISO/IEC 27001.

Starosta wyjaśnił, że IOD przeprowadza audyty w swoim zakresie, zgodnie z art. 39 RODO, gdzie między innymi zapisano, że do jego obowiązków należy przeprowadzanie regularnych ocen i audytów w celu zapewnienia zgodności z RODO. W ramach powyższego powstają załączniki raportów z audytów wewnętrznych autoryzowane wyłącznie przez IOD. Dodał także, że stanowią one uzupełnienie raportów z „auditów wewnętrznych", realizowanych w ramach obowiązującego w Starostwie Zintegrowanego Zarządzania.

NIK na podstawie przedstawionej dokumentacji stwierdza jednak, że audyt prowadzony przez IOD wykracza poza ramy określone w art. 39 RODO i sprawdza wymogi rozporządzenia KRI, przez co narusza, tylko w odniesieniu do tego aktu prawnego (rozporządzenie KRI) zasady niezależności i obiektywności audytu.

(akta kontroli: str. 28, 32, 38, 40, 44-47 plik 22-49)

OCENA CZĄSTKOWA

W badanym przez NIK okresie prowadzono niezbędne analizy ryzyka oraz sporządzono odpowiednią dokumentację w celu m.in postępowania w sytuacjach wystąpienia lub podejrzenia wystąpienia incydentu w zakresie bezpieczeństwa informacji. W toku kontroli stwierdzono jednak nieprawidłowości polegające na braku realizacji szkoleń z zakresu bezpieczeństwa informacji oraz przeprowadzeniu w 2023 r. okresowego, corocznego audytu wewnętrznego z zakresu bezpieczeństwa informacji z naruszeniem zasad niezależności i obiektywności.

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 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych[58], 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. Bieżące aktualizowanie dokumentacji składającej się na SZBI w zakresie dotyczącym zmieniającego się otoczenia.
2. Zapewnienie wymaganych zabezpieczeń w pomieszczeniu serwerowni.
3. Zawieranie w umowach o zakup sprzętu IT, oprogramowania i ich serwisowania postanowień gwarantujących zachowanie odpowiedniego poziomu bezpieczeństwa informacji.
4. Prowadzenie systematycznych szkoleń pracowników z zakresu bezpieczeństwa informacji.
5. Zapewnienie przeprowadzania audytu wewnętrznego z zakresu bezpieczeństwa informacji w sposób obiektywny i niezależny.

[57] Komunikat Ministra Rozwoju i Finansów z dnia 12 grudnia 2016 r. w sprawie standardów audytu wewnętrznego dla jednostek sektora finansów publicznych. (Dz. Urz. MRiF poz. 28).
[58] 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 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
Cezary Mazik
Główny specjalista kontroli państwowej

.....
podpis

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

.....
podpis