NAJWYŻSZA IZBA KONTROLI

DEPARTAMENT ADMINISTRACJI PUBLICZNEJ

KAP.410.3.2.2024

Pani Jolanta Gonta
Starosta Sochaczewski
Starostwo Powiatowe w Sochaczewie
ul. Marszałka Józefa Piłsudskiego 65
96-500 Sochaczew

WYSTĄPIENIE POKONTROLNE

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

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

I. Dane identyfikacyjne

Jednostka kontrolowana	Starostwo Powiatowe w Sochaczewie[1], ul. Marszałka Józefa Piłsudskiego 65, 96- 500 Sochaczew.
Kierownik jednostki kontrolowanej	Jolanta Gonta, Starosta Sochaczewski, od 20 listopada 2018 r.
Zakres przedmiotowy kontroli	Rozwiązania organizacyjne i techniczne w zakresie zapewnienia bezpieczeństwa przetwarzania informacji oraz zapewnienia ciągłości działania w urzędzie i ich stosowanie.
Okres objęty kontrolą	Od 1 stycznia 2023 r. do dnia zakończenia czynności kontrolnych, tj. 26 lipca 2024 r. (także okresy wcześniejsze w zakresie uczestnictwa w programie Cyfrowy Powiat).
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[2]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Departament Administracji Publicznej
Kontroler	Łukasz Hertel, Główny specjalista kontroli państwowej, upoważnienie do kontroli nr KAP/41/2024 z 21 maja 2024 r.

(akta kontroli str. 1-8)

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

II. Ocena ogólna[3] kontrolowanej działalności

OCENA OGÓLNA

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

Uzasadnienie oceny ogólnej

W Urzędzie nie zapewniono należytej organizacji bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych.

Negatywną ocenę uzasadniają istotne nieprawidłowości w obszarze dotyczącym organizacji bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych. W szczególności:

- Urząd nie opracował i nie wdrożył Systemu Zarządzania Bezpieczeństwem Informacji w rozumieniu § 19 ust. 1-3 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[4] (dalej: rozporządzenie KRI);
- nie dokonywał przeglądów Polityki Bezpieczeństwa Informacji w zakresie dotyczącym zmieniającego się otoczenia;
- nie podjął wystarczających działań w związku z zapewnieniem ciągłości działania (m.in.: nie prowadził analizy ryzyka w tym zakresie, a także nie wdrożył odpowiednich polityk i procedur).

W Starostwie nie prowadzono pełnej inwentaryzacji zasobów informatycznych obejmujących ich rodzaj i konfigurację. Ponadto dodatkowe zadania i obowiązki wykonywane przez osobę będącą zastępcą Inspektora Ochrony Danych (dalej: IOD) powodują konflikt interesów z zadaniami IOD.

W Urzędzie nie testowano kopii zapasowych i w niewłaściwy sposób je przechowywano. Ustanowione w Polityce Bezpieczeństwa Informacji procedury w tym zakresie nie były przestrzegane. Kopie zapasowe były przechowywane w miejscu wytwarzania danych, co w przypadku zdarzenia losowego (np. pożar) doprowadziłoby do utraty zarówno danych, jak i ich kopii.

Starostwo nie zapewniło pracownikom szkoleń z zakresu bezpieczeństwa informacji. W Urzędzie nie prowadzono okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, a także nie wdrożono kompleksowej procedury bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji.

W Urzędzie prawidłowo realizowano zadania dotyczące m.in.: opracowania dokumentacji w zakresie bezpieczeństwa przetwarzania danych osobowych i jej dostosowania do wymogów 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)[5] (dalej: RODO), zidentyfikowania zbiorów danych w tym danych osobowych podlegających zabezpieczeniu, zabezpieczenia komputerów przed możliwością instalowania dowolnego oprogramowania przez użytkowników, a także w zakresie monitorowania zajętości dysków.

---

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

[4] Dz.U. z 2024 r. poz. 773. W okresie objętym kontrolą był to przepis § 20 ust. 1-3 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247).

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

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[6] kontrolowanej działalności

OBSZAR

1. Organizacja bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych

Opis stanu faktycznego

1. W Starostwie zidentyfikowano zbiory danych wymagające ochrony (w tym danych osobowych) podlegające zabezpieczeniu, przypisując im odpowiednie wagi zgodnie z ich istotnością, ujęto je w *Wykazie zbiorów*[7]. Zidentyfikowanym zbiorom danych przypisano odpowiedni poziom ochrony, zgodny z ich wagą.

   (akta kontroli str. 9-16, 74-87)

2. W Starostwie 5 kwietnia 2023 r.[8] została wdrożona Polityka Bezpieczeństwa Informacji (dalej: PBI). W zarządzeniu wprowadzającym uregulowania w zakresie bezpieczeństwa informacji zobowiązano wszystkich pracowników do zapoznania się z PBI oraz przestrzegania zasad w niej zawartych. Zgodnie z tym dokumentem IOD został zobowiązany do opracowania i aktualizowania PBI oraz dokumentacji związanej z przetwarzaniem danych osobowych. W Urzędzie przechowywano oświadczenia pracowników potwierdzające zapoznanie się z tą dokumentacją.

   Na potrzeby realizacji programu pn. *Cyfrowy Powiat* zlecono 13 maja 2023 r. przeprowadzenie *diagnozy cyberbezpieczeństwa*[9]*,* w wyniku której stwierdzono m.in.: że wdrożona w Urzędzie PBI nie stanowi Systemu Zarządzania Bezpieczeństwem Informacji w rozumieniu § 19 ust. 1 w związku z ust. 3 rozporządzenia KRI.

   Jak ustalono w toku kontroli, wdrożona PBI dotyczyła głównie zapewnienia ochrony danych osobowych.

   W okresie objętym kontrolą pomimo wprowadzenia PBI w Urzędzie nie wdrożono kompleksowego Systemu Zarządzania Bezpieczeństwem Informacji o którym mowa w § 19 ust. 1 w związku z ust. 3 rozporządzenia KRI (dalszy opis w sekcji *Stwierdzone nieprawidłowości).*

   (akta kontroli str. 9-25, 30-48, 88-120, 122-193)

3. W okresie objętym kontrolą w Starostwie obowiązywały dokumenty dotyczące przetwarzania danych osobowych. Były to m.in. *Polityka ochrony danych osobowych Starostwa Powiatowego w Sochaczewie*[10] (obowiązująca do 5 kwietnia 2023 r.) oraz PBI, uwzględniające wymogi RODO. Wszyscy pracownicy Urzędu zaangażowani w proces przetwarzania danych osobowych, zostali zapoznani z powyższą dokumentacją.

   (akta kontroli str. 88-120, 194-254)

4. W Urzędzie nie prowadzono analizy ryzyka w związku z potrzebą zachowania ciągłości działania systemów informatycznych (dalszy opis w sekcji *Stwierdzone nieprawidłowości).*

---

6 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.

7 Stanowiący załącznik nr 3 do Polityki Bezpieczeństwa Informacji (dalej: PBI) wprowadzonej Zarządzeniem nr 21.2023 Starosty Sochaczewskiego z dnia 5 kwietnia 2023 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Starostwie Powiatowym w Sochaczewie.

8 Do dnia 5 kwietnia 2023 r. w Urzędzie funkcjonowały wprowadzone Zarządzeniem nr 17/2019 Starosty Sochaczewskiego z dnia 29 kwietnia 2019 r. w sprawie ochrony danych osobowych (dalej: Zarządzenie ODO): *Polityka ochrony danych osobowych* oraz *Instrukcja Zarządzania Systemem Informatycznym Starostwa Powiatowego w Sochaczewie*.

9 Zgodnie z formularzem stanowiącym załącznik nr 8 do Programu Operacyjnego Polska Cyfrowa na lata 2014- 2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia.

10 Stanowiąca załącznik nr 7 do Zarządzenia ODO.

(akta kontroli str. 9-16, 43-48)

5. W Urzędzie nie zostały ustanowione polityki ciągłości działania określające założenia, zakres oraz podstawowe zasady zarządzania ciągłością działania Urzędu oraz systemów informatycznych (dalszy opis w sekcji *Stwierdzone nieprawidłowości).*

(akta kontroli str. 9-25, 30-48)

6. W Urzędzie nie opracowano, nie wdrożono oraz nie testowano *Planu zapewnienia ciągłości działania, planów odtworzeniowych* zawierających procedury opisujące, w jaki sposób Starostwo wznowi i będzie kontynuować krytyczne procesy podczas wystąpienia sytuacji kryzysowej. Nie określono również akceptowalnego czasu przywrócenia ciągłości działania systemów informatycznych Urzędu (dalszy opis w sekcji *Stwierdzone nieprawidłowości).*

(akta kontroli str. 9-25, 30-48)

7. Od 5 kwietnia 2023 r. PBI[11] nie była poddana formalnemu przeglądowi i aktualizacji (dalszy opis w sekcji *Stwierdzone nieprawidłowości*).

(akta kontroli str. 17-25, 30-42, 61-67)

8. Starosta wyznaczył osoby odpowiedzialne za bezpieczeństwo informacji oraz zapewnienie ciągłości działania[12]. W dokumentach powierzających funkcje zostały określone podstawowe zakresy obowiązków na tych stanowiskach. Zadania związane z utrzymaniem ciągłości działania oraz bezpieczeństwem w infrastrukturze informatycznej zostały powierzone Administratorowi Systemów Informatycznych (dalej: ASI)[13], natomiast IOD powierzono zadania związane z utrzymaniem bezpieczeństwa informacji, m.in. monitorowanie przestrzegania RODO, aktualizowanie PBI oraz dokumentacji związanej z przetwarzaniem danych osobowych. Wyznaczeni pracownicy posiadali niezbędne kompetencje do pełnienia powierzonych im zadań z zakresu bezpieczeństwa informacji, poparte m.in.: wykształceniem i praktyką zawodową.

   W okresie od 1 stycznia do 5 kwietnia 2023 r. w Starostwie nie było wyznaczonych osób odpowiedzialnych za bezpieczeństwo informacji. Jak wyjaśnił Sekretarz Powiatu[14] w tym okresie *sprawy związane z ochroną danych osobowych regulowało zarządzenie Starosty Sochaczewskiego nr 17/2019, zgodnie z którym „Administrator powołuje Administratora Systemów Informatycznych osobnym zarządzeniem (…) Przeprowadzona analiza ww. zarządzenia, ujawniła braki dotyczące wyznaczenia ASI w Starostwie (…). W związku ze wskazaną sytuacją, w odpowiedzi na powyższe uchybienie zarządzeniem Starosty Sochaczewskiego nr 21.2023 z dnia 5 kwietnia 2023 r. powołano Administratora Systemów Informatycznych.*

(akta kontroli str. 9-25, 30-42, 255-286)

9. W kontrolowanym okresie w Starostwie, zgodnie z art. 37 ust. 1 i 5 RODO oraz art. 8 ustawy z dnia 18 maja 2018 r. o ochronie danych osobowych[15], wyznaczono IOD oraz jego zastępcę. Osoby te posiadały odpowiednie kwalifikacje zawodowe do pełnienia tej funkcji. Do zadań jakie powierzono IOD należało m.in.: *monitorowanie przestrzegania RODO, innych przepisów krajowych dot. ochrony danych osobowych oraz polityk Administratora Danych*

---

11 Wg stanu na dzień 20 czerwca 2024 r.

12 1. Inspektora Ochrony Danych w Starostwie Powiatowym w Sochaczewie (Zgodnie z załącznikiem nr 9 do PBI); 2. Administratora Systemów Informatycznych w Starostwie Powiatowym w Sochaczewie (zgodnie z załącznikiem nr 10 do PBI).

13 Pracownik został również zobowiązany do inwentaryzowania oraz okresowego sprawdzenia stanu urządzeń oraz sprzętu pozwalającego na obsługę czynności przetwarzania danych osobowych w systemach informatycznych.

14 Na podstawie Upoważnienia Starosty Sochaczewskiego z dnia 27 grudnia 2022 r. (Znak: ORN.077.127.2022.KF).

15 Dz. U. z 2019 r. poz. 1781.

Osobowych, przedstawianie harmonogramu czynności audytowych zgodnie z przyjętą Polityką Bezpieczeństwa Informacji, współpraca z organem nadzorczym, udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych osobowych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO.

Ustalono, że Powiat zawarł umowę z firmą zewnętrzną na *usługi audytu zerowego związanego z ochroną danych osobowych, zaktualizowania dokumentacji związanej z ochroną danych osobowych oraz pełnienia obowiązków Inspektora Ochrony Danych.* Ponadto Powiat zawarł z tą samą firmą umowę na usługę prowadzenia audytu wewnętrznego w Starostwie Powiatowym w Sochaczewie i jednostkach organizacyjnych Powiatu Sochaczewskiego.

Osoba wyznaczona na IOD przeprowadzała w Urzędzie audyt wewnętrzny i odpowiadała jednocześnie za przygotowanie, opracowanie i aktualizacje PBI. Zastępca IOD przeprowadzał Audyt Bezpieczeństwa Informacji (dalszy opis w sekcji *Stwierdzone nieprawidłowości).*

(akta kontroli str. 9-25, 30-42, 88-118, 275-382)

10. W Urzędzie stosownie do art. 21 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa[16] (dalej: ustawa o ksc) 31 stycznia 2023 r. wyznaczono dwie osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa[17]. Zgłoszenie tych osób do właściwego CSIRT NASK[18] nastąpiło 27 lutego 2023 r. Jak wyjaśnił Sekretarz Powiatu *przekroczenie terminu 14 dni na zgłoszenie danych osób kontaktowych do właściwego CSIRT było niezamierzone i wynikało z obciążenia obowiązkami pracownika dokonującego zgłoszenia. Zgłoszenie zostało przesłane niezwłocznie. W momencie zmiany osób kontaktowych i wyznaczenia ponownie osób kontaktowych do właściwego CSIRT, terminy zostały zachowane (…).*

    Zgodnie z Zarządzeniem nr 44.2023 Starosty Sochaczewskiego z dnia 10 listopada 2023 r. *w sprawie wyznaczenia osób odpowiedzialnych* za utrzymanie *kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa* wyznaczono trzy osoby i przekazano ich zgłoszenie do właściwego CSIRT NASK w terminie 14 dni od ich wyznaczenia, co było zgodne z art. 22 ust. 1 pkt 5 ustawy o ksc.

    (akta kontroli str. 9-16, 61-67, 383-401)

11. W ramach funkcjonowania PBI, określono *Instrukcję Zarządzania Systemem Informatycznym Starostwa Powiatowego w Sochaczewie* (dalej: Instrukcja Zarządzania SI)*[19],* w której w sposób ogólny zdefiniowano zasady oraz tryb wykonywania czynności w systemach informatycznych Starostwa w związku z ochroną danych osobowych. Zawarto w niej m.in.: *procedurę nadawania i cofania uprawnień, procedurę określającą wymogi oraz sposób użytkowania haseł w Systemie Informatycznym, procedurę rozpoczęcia, zawieszenia i zakończenia pracy, procedurę tworzenia kopii zapasowych danych oraz programów i narzędzi programowych służących do przetwarzania danych osobowych w Systemie Informatycznym*.

    Jak poinformował Sekretarz Powiatu, *obecnie jesteśmy na etapie weryfikacji i analiz obszarów związanych ze wskazaną dokumentacją. Biorąc pod uwagę jej obszerny charakter i mając świadomość pewnych niedociągnięć w tym zakresie, jakie mimo wprowadzenia PBI ujawniła przeprowadzona w 2023 roku „Diagnoza*

---

16 Dz. U. z 2024 r. poz.1077.

17 Zarządzeniem Nr 4.2023 Starosty Sochaczewskiego z dnia 31 stycznia 2023 roku w sprawie wyznaczenia osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.

18 Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy.

19 Stanowiącą Załącznik nr 12 do PBI.

cyberbezpieczeństwa", bardzo liczymy na możliwość kompleksowego opracowania i wdrożenia całościowego Systemu Zarządzania Bezpieczeństwem Informacji w ramach grantu „Cyberbezpieczny Samorząd" (…).

(akta kontroli str. 9-42)

12. Inwentaryzacja zasobów informatycznych, o której mowa w § 19 ust. 2 pkt 2 rozporządzenia KRI, rozumiana jako stałe posiadanie aktualnych informacji w zakresie posiadanego sprzętu informatycznego oraz jego konfiguracji, była prowadzona przy pomocy oprogramowania Axence Nvision. W wyniku oględzin ustalono, że system ten nie zawierał pełnej informacji o wszystkich zasobach informatycznych obejmujących ich rodzaj i konfigurację[20] (dalszy opis w sekcji *Stwierdzone nieprawidłowości*).

    (akta kontroli str. 9-16, 49-60, 402-420)

13. Powiat Sochaczewski po złożeniu wniosku został w lutym 2024 r. zakwalifikowany do dofinansowania w ramach konkursu grantowego „Cyberbezpieczny Samorząd"[21] realizowanego w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

    Według stanu na dzień 12 czerwca 2024 r. umowa na realizację grantu nie została jeszcze zawarta. Jak poinformował Sekretarz Powiatu *w dniu 15 kwietnia 2024 r. Powiat Sochaczewski otrzymał plik z umową z informacją, aby podpisały ją osoby do tego upoważnione reprezentujące powiat. (…) Umowa została podpisana (…), przesłana w dniu 18 kwietnia 2024 r. Czekamy na podpisanie umowy przez drugą stronę, co będzie stanowiło o jej zawarciu – termin tego podpisu nie jest nam znany.*

    Zgodnie z wnioskiem o dofinansowanie (nr FERC.02.02-CS.01-001/23/0950) założono podniesienie bezpieczeństwa informacji poprzez wzmocnienie odporności Urzędu na cyberzagrożenia oraz jego zdolności wykrywania ich i reagowania na nie w trzech obszarach, tj. organizacyjnym, kompetencyjnym i technicznym. Zaplanowano m.in. audyty obejmujące PBI, role i odpowiedzialność za elementy bezpieczeństwa informacji, testy penetracyjne, realizacje szkoleń z zakresu cyberbezpieczeństwa dla pracowników Urzędu i szkoleń specjalistycznych działu IT obejmujących procedury awaryjne, odzyskiwanie danych, obsługę kopii zapasowych. W odniesieniu do potencjału technicznego zaplanowano m.in.: zakup nowego urządzenia zabezpieczającego sieć, doposażenie w przełączniki agregacyjne, zakup nośnika kopii zapasowych, zakup oprogramowania do ochrony poczty elektronicznej umożliwiający skanowanie i szyfrowanie, zakup oprogramowania umożliwiającego wykonywanie kopii awaryjnych serwera oraz stacji roboczych, zakup serwera, zakup oprogramowania do monitoringu sieci. Wydatki ogółem oszacowano na kwotę 960 180,69 zł, a dofinansowanie ze środków Unii Europejskiej przewidziano w kwocie 849 932,94 zł.

    (akta kontroli str. 9-25, 421-458)

[20] Podczas oględzin nie zlokalizowano w systemie laptopów m.in. Sekretarza Powiatu, zasilaczy UPS oraz fizycznych serwerów, które są w posiadaniu Urzędu.

[21] Centrum Projektów Polska Cyfrowa poinformowało Starostwo, że wniosek uzyskał pozytywną ocenę formalno-merytoryczną. Lista rankingowa została opublikowana 23 lutego 2024 r.

Stwierdzone nieprawidłowości

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

1. W Starostwie nie opracowano i nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji. Ustanowiona PBI dotyczyła głównie ochrony danych osobowych.

   Było to niezgodne z § 19 ust. 1 w związku z ust. 3 rozporządzenia KRI, stanowiącym, że *podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność*. Ponadto § 19 ust. 3 rozporządzenia KRI wskazuje, że wymagania określone w ww. ust 1 uznaje się za spełnione, jeżeli System Zarządzania Bezpieczeństwem Informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanowienie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą[22].

   Sekretarz Powiatu wyjaśnił, że *Opracowanie i wdrożenie całościowego Systemu Zarządzania Bezpieczeństwem Informacji, o którym mowa w § 19 ust. 1 rozporządzenia KRI, było rekomendacją działań naprawczych po przeprowadzeniu audytu wewnętrznego w 2023 r. Wykonanie tej rekomendacji zostało zaplanowane na rok 2024 w ramach programu „Cyberbezpieczny Samorząd", co potwierdza koncepcja przedstawiona w aplikacji o grant.*

   (akta kontroli str. 9-25, 30-48, 88-120, 122-193)

2. Nieprowadzanie analizy ryzyka w związku z potrzebą zachowania ciągłości działania systemów informatycznych, co było działaniem nierzetelnym.

   Sekretarz Powiatu wyjaśnił, że *urząd przeprowadza analizy ryzyka w zakresie bieżącego wskazywania zagrożeń związanych z bezpieczeństwem informacji i ochrony danych osobowych, każdorazowo przy naruszeniu. Do chwili obecnej nie została zakłócona ciągłość działania systemów informatycznych, nie wystąpiło naruszenie. Dział IT monitoruje na bieżąco czy występuje lub może wystąpić zakłócenie związane z ciągłością działania systemów informatycznych, bierze udział w szkoleniach (…), co w naszej ocenie jest pewną analizą ryzyka w związku z potrzebą zachowania ciągłości działania systemów informatycznych*.

   Zdaniem NIK - jak wskazano w Normie ISO 22301 - analiza ryzyka w związku z potrzebą zachowania ciągłości działania jest kluczowa. Ocena ryzyka, w kontekście zarządzania ciągłością działania, określa prawdopodobieństwo i wpływ zagrożeń, mogących być przyczyną przerwania działalności. Natomiast po ocenie możliwości wystąpienia zagrożenia analizuje się mechanizmy zabezpieczające w organizacji. Mechanizmy te mają zmniejszyć ryzyko przerwania działania.

   Nieprzeprowadzenie analizy ryzyka w tym zakresie nie pozwala w pełni zidentyfikować zagrożeń występujących w tym obszarze.

   (akta kontroli str. 9-16, 43-48)

3. Nieustanowienie polityki ciągłości działania określającej założenia, zakres oraz podstawowe zasady zarządzania ciągłością działania Urzędu oraz systemów informatycznych, co było działaniem nierzetelnym.

[22] W tym: PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem.

Sekretarz Powiatu wskazał, że *funkcjonowanie Urzędu jest określone w Planie zarządzania kryzysowego, gdzie jest uregulowane przeniesienie Urzędu na wypadek wystąpienia zagrożenia związanego np. z katastrofą czy innym incydentem zakłócającym działanie. We wskazanym zakresie urząd skorzysta z planu zarządzania kryzysowego, jaki jest przyjęty. Nie mniej jednak planujemy wdrożyć politykę ciągłości działania w trakcie realizacji grantu „Cyberbezpieczny samorząd”.*

Zdaniem NIK określenie polityki ciągłości działania służy zdefiniowaniu zaleceń oraz konkretnie sprecyzowanych działań, których celem jest zapewnienie funkcjonowania krytycznych procesów w Starostwie w sytuacji kryzysowej. Brak ustanowienia polityki ciągłości działania w Starostwie negatywnie wpływa na przygotowanie Urzędu na sytuacje awaryjne, istotnie utrudniając skuteczne reagowanie na ich wystąpienie i zapewnienie ciągłego działania Urzędu.

(akta kontroli str. 9-25, 30-48)

4. Nieopracowanie, niewdrożenie Planu zapewnienia ciągłości działania, planów odtworzeniowych dotyczących w szczególności: zasilania i topologii sieci, klastrów i macierzy dyskowych, systemów kopii zapasowych, systemów serwerów wirtualnych co było działaniem nierzetelnym.

   Sekretarz Powiatu wskazał, że ww. plany *nie zostały opracowane na piśmie. Jest natomiast prowadzona dobra praktyka oraz zminimalizowane ryzyko utraty ciągłości działania w następujący sposób (…) Testowanie, nie zostało przeprowadzone. Taki stan rzeczy jest wynikiem braku posiadania sprzętu jaki można do takiej symulacji wykorzystać, brak urządzeń zapasowych o parametrach takich samych jak posiadane lub lepszych. (…) Akceptowalny czas przywrócenia ciągłości działania systemów informatycznych nie został określony w sposób dokładny z powodu braku możliwości przetestowania takiej sytuacji, z uwagi na brak sprzętu zapasowego. W przybliżeniu takie działanie zajęłoby ok. 24 h w momencie posiadania identycznego lub lepszego sprzętu jaki jest obecnie na wyposażeniu Urzędu*.

   Zdaniem NIK, brak procedur operacyjnych zapewniających ciągłość działania w Starostwie w zakresie zasilania i topologii sieci, klastrów i macierzy dyskowych, systemów kopii zapasowych, systemów serwerów wirtualnych może istotnie utrudnić przywracanie do funkcjonowania infrastruktury informatycznej w szczególności najistotniejszych dla działalności Starostwa systemów informatycznych po zdarzeniu losowym (np. pożar, zalanie).

   Praktyka stosowana w Urzędzie nie daje wystarczającego zapewnienia, że w przypadku zaistniałej katastrofy Urząd zapewni sprawne wznowienie działalności.

   (akta kontroli str. 9-25, 30-48, 61-73, 595)

5. Niepoddanie formalnemu przeglądowi ustanowionej w Starostwie PBI od momentu jej wdrożenia, tj. 5 kwietnia 2023 r., co było działaniem nierzetelnym.

   Zgodnie z § 19 ust. 2 pkt 1 rozporządzenia KRI *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań: zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia*. Stosownie do załącznika A PN-ISO/IEC 27001:2017, punkt A.5.1.2, *polityki bezpieczeństwa informacji należy poddawać przeglądom w zaplanowanych odstępach czasu lub wtedy, gdy wystąpią istotne zmiany, aby zapewnić, że nadal są właściwe, adekwatne i skuteczne*.

Sekretarz Powiatu wyjaśnił, że *przytoczony przepis nie wskazuje wprost terminu na przeprowadzenie formalnego przeglądu PBI. Biorąc pod uwagę stosunkowo niedawny termin wprowadzenia PBI w Starostwie Powiatowym w Sochaczewie oraz małą dynamikę zmieniającego się otoczenia, przyjęto robić przegląd PBI co 2 lata. (…)*

NIK wskazuje, iż biorąc pod uwagę obecny rozwój nowych technologii informacyjnych w tym zagrożeń związanych z cyberbezpieczeństwem, a także często zmieniające się przepisy w tym zakresie, za zasadne należy uznać przeglądy PBI nie rzadziej niż raz na 12 miesięcy.

(akta kontroli str. 17-25, 30-42, 61-67, 88-118, 665-668)

6. Przeprowadzenie Audytu Bezpieczeństwa Informacji przez osobę, która pełniła w Urzędzie funkcję zastępcy IOD, co naruszało art. 38 ust. 6 RODO.

   Zgodnie z art. 38 ust. 6 RODO, osoba wyznaczona na IOD może wykonywać inne zadania i obowiązki, jednak administrator danych (tj. Starosta) musi zapewnić, by takie zadania i obowiązki nie powodowały konfliktu interesów. Zgodnie z wytycznymi Normy PN-ISO/IEC 27001:2017 punkt 9.2 *Audyt wewnętrzny Organizacja powinna: wybierać audytorów i prowadzić audyty w sposób zapewniający obiektywność i bezstronność procesu audytu.*

   Sekretarz Powiatu wyjaśnił, że *Inspektor Ochrony Danych wykonuje swoje zadania zgodnie ze swoją najlepszą wiedzą oraz doświadczeniem, wypełniając zapisy umowy zawartej z firmą (…). zgodnie z zadaniami jakie znajdują się w dokumencie. PBI została opracowana przez IOD Starostwa Powiatowego w Sochaczewie, a przed jej wprowadzeniem w dniu 5 kwietnia 2023 roku (…) została przedstawiona kierownictwu wyższego szczebla do akceptacji. Dokument został przyjęty bez poprawek. Inspektor Ochrony Danych nie określił samodzielnie środków i zasad, zostały one ustalone przez kierownictwo Urzędu a spisane i wprowadzone do PBI przez IOD. (…) Na zastępcę IOD został wyznaczony (…) Do chwili obecnej jednak nie było przypadku, aby musiał on w zastępstwie za IOD, wykonywać w Starostwie Powiatowym w Sochaczewie zadania przypisane IOD. (…) Zdaniem Urzędu nie występuje konflikt interesów.*

   Zdaniem NIK wykonywanie obowiązków zastępcy IOD w Starostwie oraz przeprowadzenie audytu wewnętrznego z zakresu bezpieczeństwa informacji, za które m.in. odpowiada IOD stanowi konflikt interesów i tym samym narusza przepis art. 38 ust. 6 RODO. Wątpliwości może budzić to czy osoba pełniąca funkcję zastępcy IOD przeprowadza audyt bezpieczeństwa informacji, obejmujący przedmiot będący w zakresie jego obowiązków jako zastępcy IOD, w sposób zapewniający obiektywność i bezstronność procesu audytu.

   (akta kontroli str. 9-25, 30-42, 88-118, 275-382)

7. Brak pełnej informacji o wykorzystywanych zasobach informatycznych, obejmującej ich rodzaj i konfigurację, co było niezgodne z § 19 ust. 2 pkt 2 rozporządzenia KRI.

   Zgodnie z § 19 ust. 2 pkt 2 rozporządzenia KRI *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań: utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację*.

   Sekretarz Powiatu wyjaśnił, że *Urząd inwentaryzuje posiadany przez siebie sprzęt w formie papierowej na podstawie książki inwentarzowej. Każde urządzenie posiada numer inwentarzowy. Urządzenia wpięte do sieci rejestruje ponadto program Axence, którego wersja zostanie podniesiona w ramach*

realizacji programu „Cyberbezpieczny Samorząd”. Ponadto dodał, że *zasoby przypisane są w książce inwentarzowej na podstawie numeru inwentarzowego nadawanego zaraz po zakupie sprzętu. Numer nadawany jest na podstawie FV i przypisany do sprzętu a następnie do osoby/wydziału, która korzysta z tego sprzętu w Urzędzie.*

Zdaniem NIK ograniczony zakres informacji dotyczący posiadanych zasobów informatycznych oraz ich konfiguracji istotnie utrudni przywrócenie tych zasobów do działania po katastrofie lub innym zdarzeniu losowym.

(akta kontroli str. 9-16, 49-60, 402-420, 570-585)

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli ocenia negatywnie działalność kontrolowanej jednostki w zakresie organizacji bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych ze względu na to, że w Starostwie: nie opracowano i nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji (wdrożona PBI dotyczyła głównie ochrony danych osobowych), nie dokonywano przeglądu PBI w zakresie dotyczącym zmieniającego się otoczenia, nie prowadzono pełnej inwentaryzacji zasobów informatycznych obejmującej ich rodzaj i konfigurację. Było to niezgodne z wymaganiami rozporządzenia KRI. W Urzędzie nie podjęto wystarczających działań w związku z zapewnieniem ciągłości działania (m.in.: brak analiz ryzyka, polityk, procedur). Ponadto stwierdzono, że inne zadania i obowiązki wykonywane przez zastępcę IOD powodują konflikt interesów.

W Urzędzie natomiast prawidłowo realizowano zadania dotyczące m.in. opracowania dokumentacji z zakresu bezpieczeństwa przetwarzania danych osobowych i jej dostosowania do wymogów RODO, a także zidentyfikowania zbiorów danych w tym danych osobowych podlegających zabezpieczeniu.

OBSZAR

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

Opis stanu faktycznego

1. W toku kontroli dokonano oględzin w zakresie ustalenia czy w Urzędzie zapobiega się możliwości zainstalowania nieautoryzowanego oprogramowania. Weryfikację przeprowadzono poprzez próbę zainstalowania na 12 komputerach pracowników Urzędu, programu Adobe Reader[23], z poziomu użytkownika komputera. Ustalono, że zalogowani pracownicy nie mieli przyznanych uprawnień administracyjnych, umożliwiających instalację dowolnego oprogramowania. Powyższe działania były zgodne z § 19 ust. 2 pkt 4 rozporządzenia KRI. Ponadto Sekretarz Powiatu wyjaśnił, że *Urząd nie posiada oprogramowania jak np. MDM[24] na telefonach komórkowych. Urząd nie posiada tabletów natomiast posiada 20 numerów służbowych wraz z aparatami telefonicznymi. Aparaty telefoniczne nie są wykorzystywane do przetwarzania danych osobowych i spełniają swoje podstawowe funkcje komunikacyjne.*

   (akta kontroli str. 49-60, 459-465)

2. W PBI określono ogólne zasady dotyczące nadawania/cofania uprawnień do pracy w systemach informatycznych. Na podstawie badania próby uprawnień do systemów informatycznych 13 pracowników Urzędu ustalono, że wszyscy posiadali uprawnienia do pracy adekwatne do zakresu realizowanych zadań. Badaniem objęto także uprawnienia dwóch pracowników, którzy w okresie objętym kontrolą zmienili stanowiska pracy. Stwierdzono, że uprawnienia tych

[23] Ze strony https://get.adobe.com/pl/reader, sprawdzenia dokonał ASI w obecności kontrolera.

[24] MDM (skrót od angielskiego Mobile Device Management) to oprogramowanie, które umożliwia zarządzanie, zabezpieczenie i monitoring wszystkich urządzeń mobilnych wykorzystywanych w miejscu pracy i znajdujących się w firmowej sieci.

osób były zgodne z nowym zakresem obowiązków. Powyższe działania były zgodne z § 19 ust. 2 pkt 4 i 5 rozporządzenia KRI.

(akta kontroli str. 88-118, 466-569)

3. W wyniku badania blokowania kont w systemach informatycznych, przeprowadzonego na próbie kont dziewięciu osób, które w okresie objętym kontrolą zakończyły pracę w Urzędzie ustalono, że: jeden były pracownik posiadał aktywne konto w programie Bestia, a jeden w usłudze Active Directory. ASI w obecności kontrolera dokonał wyłączenia kont (dalszy opis w sekcji *Stwierdzone nieprawidłowości*).

(akta kontroli str. 61-67, 570-585)

4. Komputery Starostwa były zarządzane centralnie w oparciu o mechanizm *Active Directory.* Wymogi dotyczące złożoności haseł do systemów informatycznych, zostały określone w *Instrukcji Zarządzania SI*. Ustalono, że pracownicy Urzędu posiadają unikalne identyfikatory oraz hasła dostępu o odpowiedniej złożoności[25] a system cyklicznie wymusza zmianę hasła. W wyniku badania trzech systemów informatycznych[26] w Urzędzie ustalono, że wymogi wynikające z powyższej instrukcji zostały wdrożone. Powyższe działania spełniały wymogi § 19 ust. 2 pkt 7 rozporządzenia KRI.

(akta kontroli str. 586-593)

5. Oględziny pięciu stanowisk pracy realizujących zadania z zakresu rejestracji pojazdów oraz jednego stanowiska realizującego zadania z zakresu wydawania praw jazdy wykazały, że monitory usytuowane były w sposób uniemożliwiający wgląd do danych przez osoby nieuprawnione. Powyższe działania spełniały wymogi § 19 ust. 2 pkt 7 rozporządzenia KRI.

(akta kontroli str. 594)

6. W Starostwie ustanowiono zasady ochrony danych osobowych w pracy zdalnej oraz zasady bezpiecznego użytkowania sprzętu IT przeznaczonego do pracy zdalnej, co było zgodne z § 19 ust. 2 pkt 8 rozporządzenia KRI. Wprowadzone zasady minimalizowały ryzyko kradzieży informacji w tym urządzeń mobilnych i miały zapewnić bezpieczną pracę w formie zdalnej.

(akta kontroli str. 9-16, 98-100)

7. Ustalono, że w Urzędzie nie stosuje się rozwiązań polegających na wykorzystywaniu specjalnego oprogramowania odpowiedzialnego za szyfrowanie danych zgromadzonych na dyskach twardych komputerów przenośnych (dalszy opis w sekcji *Stwierdzone nieprawidłowości).*

(akta kontroli str. 49-58)

8. Serwery wykorzystywane w Urzędzie zlokalizowane były w wyodrębnionych pomieszczeniach (serwerowniach), do których dostęp miało dwóch informatyków Starostwa. W trakcie oględzin jednej z dwóch serwerowni ustalono, że nie była prowadzona ewidencja wejść/wyjść oraz stwierdzono ryzyko związane z potencjalnymi zagrożeniami fizycznymi lub środowiskowymi dla tego pomieszczenia (dalszy opis w sekcji *Stwierdzone nieprawidłowości).*

(akta kontroli str. 61-73, 595)

---

[25] Zgodnie z rekomendacją ustaloną w PBI w zakresie złożoności haseł do wymogów ustanowienia hasła należy: minimum osiem znaków, które nie powinny być łatwe do zidentyfikowania, z rekomendacją do 12 znaków. Hasło powinno składać się z dużych i małych liter, cyfr oraz co najmniej jednego znaku specjalnego.

[26] Bestia JST, Resto, Symfonia ERP Kadry i Płace 2024.

9. W toku kontroli dokonano analizy 12 umów[27] zawartych w okresie objętym kontrolą, obejmujących swym zakresem serwis/utrzymanie/obsługę sprzętu i oprogramowania Urzędu oraz świadczenie usług informatycznych. W ramach ww. umów wykonawcy mogli mieć dostęp do informacji/danych Urzędu, np. dostęp do systemu komunikacji, danych zawartych na dyskach twardych, zasobów poczty elektronicznej Urzędu, danych zawartych w systemach. Ustalono, że tylko w czterech umowach zawarto klauzulę zapewniającą bezpieczeństwo informacji w trakcie trwania umowy oraz po jej zakończeniu (dalszy opis w sekcji *Stwierdzone nieprawidłowości*).

(akta kontroli str. 49-60, 596-664)

10. Jak poinformował Sekretarz Powiatu *zgodnie z przyjętą praktyką w Urzędzie, każdy sprzęt IT jaki jest przekazywany poza jednostkę (do serwisu lub zbycie sprzętu) jest odpowiednio przygotowywany do tego procesu poprzez demontaż nośników pamięci (dysków twardych) zawierających wszelakie dane podlegające ochronie. Wymontowane dyski twarde są odpowiednio opisywane i przechowywane (…).* Ponadto w PBI określono m.in.: że urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie a w przypadku naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawiane są przez podmiot przetwarzający, z którym zawarto umowę powierzenia przetwarzania danych. Ustalono, że w przypadku przekazywania sprzętu IT poza jednostkę stosowane rozwiązania są zgodne z § 19 ust. 2 pkt 7 i 9 rozporządzenia KRI oraz załącznikiem A normy PN/ISO/IEC 27001:2017, punkt A.11.2.7

(akta kontroli str. 9-16)

11. W *Instrukcji Zarządzania SI* określono *procedurę tworzenia kopii zapasowych danych oraz programów i narzędzi służących do przetwarzania danych osobowych w Systemie Informatycznym.* Zakres odpowiedzialności za tworzenie, przechowywanie kopii zapasowych, a także prowadzenie ewidencji ich wykonania przypisano ASI. W wyniku oględzin oprogramowania służącego do tworzenia kopii zapasowych oraz miejsca przechowywania sporządzonych kopii stwierdzono ryzyko związane z potencjalnymi zagrożeniami w tym zakresie. Ponadto stwierdzono, że przyjęta i stosowana w Urzędzie praktyka jest inna niż metodologia przyjęta w procedurze określonej w PBI (dalszy opis w sekcji *Stwierdzone nieprawidłowości*).

(akta kontroli str. 30-42, 61-67, 88-118, 665-668)

12. W ramach obowiązujących w Urzędzie uregulowań nie zostały określone zasady monitorowania stanu pojemności przestrzeni dyskowej w serwerach Urzędu. Ustalono jednak, że stosownie do zalecenia, sformułowanego w pkt A.12.1.3 załącznika A normy PN-ISO/IEC 27001:2017, pojemność była na bieżąco monitorowana przez informatyków. Ponadto Sekretarz Powiatu, wyjaśnił, że *Procedury związane z monitorowaniem pojemności nośników pamięci serwerów oraz informowaniem o konieczności podjęcia działań w związku z wyczerpywaniem się tej pamięci, zostaną wprowadzone po zakupie odpowiedniego oprogramowania umożliwiającego takie monitorowanie, co zaplanowane jest w ramach konkursu „Cyberbezpieczny Samorząd" oraz po wdrożeniu i przeszkoleniu pracowników działu IT przez dostawcę lub producenta oprogramowania, które jest dedykowane do monitoringu zasobów dyskowych.*

[27] Zbadano 8 umów na obsługę IT Starostwa, jedną na usługi doradcze w związku z realizacją projektu „Cyberbezpieczny Samorząd", dwie na świadczenie usługi dostępu do internetu, jedną na wykonanie diagnozy cyberbezpieczeństwa.

Ponadto wskazał, że *W przypadku przekroczenia 80% zajętości dysków, dział IT informuje kierownictwo Urzędu/osoby decyzyjne w sprawie zakupów, o konieczności pozyskania nowych dysków, które pozwolą na powiększenie oraz zabezpieczenie krytycznego progu wymaganego dla serwerów w Urzędzie.*

(akta kontroli str. 30-42, 68-73, 669-680)

13. W Starostwie w ramach zapewnienia ciągłości działania zostały zidentyfikowane kluczowe elementy infrastruktury i usługi IT. Ponadto Sekretarz Powiatu wskazał, że *każde z (…) urządzeń pracuje pod kontrolą zasilacza UPS albo w formie rackowej w danej szafie (…) UPS pozwala podtrzymać zasilanie około 30 minut.*

(akta kontroli str. 68-73)

Stwierdzone nieprawidłowości

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

1. W Starostwie nie stosowano rozwiązań polegających na szyfrowaniu danych zgromadzonych na dyskach twardych komputerów przenośnych, co było niezgodne z § 19 ust. 2 pkt 9 i 11 rozporządzenia KRI.

   Zgodnie z § 19 ust. 2 pkt 9 i 11 rozporządzenia KRI, *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań: zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie; ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.*

   Sekretarz Powiatu wyjaśnił, że *na chwilę obecną w Urzędzie nie stosuje się rozwiązania polegającego na wykorzystywaniu specjalnego oprogramowania odpowiedzialnego za szyfrowanie danych, z uwagi na zbyt małą wydajność posiadanych urządzeń. Wprowadzenie takiego rozwiązania zwiększyłoby spadek tej wydajności i znacząco utrudniło pracę. Urząd podejmuje systematyczne działania mające na celu wymianę przestarzałego sprzętu, jednakże te uzależnione są od środków finansowych jakimi dysponuje urząd.*

   (akta kontroli str. 49-58)

2. Ustalono, iż w przypadku ośmiu umów nie zawarto w nich *zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji*, co było niezgodne z § 20 ust. 2 pkt 10 rozporządzenia KRI[28].

   Sekretarz Powiatu wyjaśnił, że w przypadku umów o świadczenie usług informatycznych na rzecz Starostwa *nie zawarto klauzuli zapewniającej bezpieczeństwo informacji. Z osobami, które obecnie świadczą obsługę informatyczną w ramach zawartych umów zostały podpisane upoważnienia do przetwarzania danych osobowych, w których znajduje się oświadczenie osoby upoważnionej w którym (…) zobowiązuję się do zachowania poufności, nieujawniania osobom nieupoważnionym i zachowania w tajemnicy wszelkich danych, z którymi mam styczność podczas wykonywania zadań służbowych lub będę mieć dostęp, a nie przeznaczonych do publicznego rozpowszechniania.*

   (akta kontroli str. 49-60, 596-664)

3. Stwierdzono, że dwóch spośród dziewięciu byłych pracowników Starostwa posiadało aktywne konta, jeden w systemie informatycznym Bestia, a jeden

[28] Według stanu prawnego obowiązującego w okresie zawierania umów, w obowiązującym stanie prawnym § 19 ust. 2 pkt 10 rozporządzenia KRI.

w usłudze Active Directory, co było niezgodne z § 19 ust. 2 pkt 5 rozporządzenia KRI stanowiącym, *że Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań: bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.*

Sekretarz Powiatu wyjaśnił, że *Polecenia cofnięcia uprawnień do systemów informatycznych zostały sporządzone na koniec zatrudnienia danego pracownika. Wnioski są przekazywane do ASI. W przypadku (…) aktywne konto mogło służyć jedynie do weryfikacji informacji z programu Bestia, natomiast w przypadku (…) doszło do niezamierzonego pominięcia zablokowania konta, co zostało ujawnione w trakcie kontroli i w obecności Kontrolera dokonano wyłączenia tego konta (…).*

(akta kontroli str. 61-67, 570-585)

4. Część zastosowanych zabezpieczeń fizycznych serwerowni, w niewystarczającym stopniu chroniła to pomieszczenie[29], co zwiększało ryzyko ujawnienia, modyfikacji, usunięcia lub zniszczenia informacji, będących w posiadaniu Urzędu. Było to niezgodne z §19 ust. 2 pkt 9 rozporządzenia KRI.

   Sekretarz Powiatu wyjaśnił, że (…) *w planach jest modernizacja serwerowni (…).*

   (akta kontroli str. 61-73, 595)

5. Niedostosowanie procedur w zakresie tworzenia i przechowywania kopii zapasowych do faktycznie stosowanej praktyki w Urzędzie w tym zakresie, a także niewystarczające działania w zakresie testowania i przechowywania kopii zapasowych w celu zapewnienia ciągłości działania Urzędu[30], co było niezgodne z §19 ust. 2 pkt 12 lit. b) i e) oraz §19 ust. 2 pkt 7 rozporządzenia KRI.

   Sekretarz Powiatu wyjaśnił, że *Polityka Bezpieczeństwa Informacji zostanie zaktualizowana w najbliższym czasie o informacje na temat kopii zapasowych, sposób ich wykonywania i przechowywania. Starostwo ze środków pozyskanych z grantu zakupi drugi serwer NAS Synology oraz oprogramowanie Veeam w najnowszej wersji, które pozwoli wraz z nowym serwerem Dell na jeszcze lepsze zabezpieczenie kopii (…). Testowanie kopii było wykonywane na początku konfiguracji serwera NAS, ale zostało zatrzymane z powodu zbyt długiego oraz czasochłonnego procesu testowania oraz weryfikacji przez NAS, co wpływało na spowolnienie oraz często kolidowało z zaplanowaną kopią dnia następnego tych samych danych. Aktualnie Starostwo także nie posiada dodatkowego serwera w celu odtworzenia maszyn wirtualnych, których kopie zostały wykonane co pozwoliłoby na weryfikację poprawności odtworzenia i poprawności działania kopii (…).*

   (akta kontroli str. 30-42, 61-67, 88-118, 665-668)

OCENA CZĄSTKOWA

Najwyższa Izba kontroli ocenia negatywnie działalność Starostwa w zakresie wdrożonych i wykorzystywanych rozwiązań organizacyjnych i technicznych zapewniających bezpieczeństwo informacji oraz ciągłość działania. Działania w zakresie testowania i przechowywania kopii zapasowych w celu zapewnienia ciągłości działania Urzędu były niewystarczające. W przypadku serwerowni niewystarczająco minimalizowano ryzyka związane z potencjalnymi zagrożeniami fizycznymi i środowiskowymi. W ośmiu umowach na obsługę IT nie zawarto

[29] Szczegółowe ustalenia w tym zakresie zostały przekazane w trakcie czynności kontrolnych Sekretarzowi Powiatu oraz Staroście Powiatu Sochaczewskiego pismem KAP.410.3.2.2024/8 z dnia 11 lipca 2024 r.

[30] Szczegóły w tym zakresie przekazano Sekretarzowi Powiatu podczas czynności kontrolnym oraz Staroście Powiatu Sochaczewskiego pismem KAP.410.3.2.2024/7 z dnia 10 lipca 2024r.

postanowień zobowiązujących wykonawców do zachowania poufności. Nie szyfrowano danych na komputerach przenośnych.

W Urzędzie natomiast prawidłowo realizowano zadania w zakresie: zabezpieczenia komputerów przed możliwością instalowania dowolnego oprogramowania przez użytkowników, monitorowania zajętości dysków, a ponadto zastosowano rozwiązania dotyczące zbycia lub przekazania sprzętu IT poza Urząd zapewniające bezpieczeństwo informacji. Ustawienie monitorów objętych badaniem zapewniało, że dane wyświetlane na ekranie nie były widoczne dla osób nieuprawnionych.

OBSZAR

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

1. W Urzędzie nie prowadzono okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji (dalszy opis w sekcji *Stwierdzone nieprawidłowości*).

(akta kontroli str. 17-25, 43-48)

2. W Urzędzie nie opracowano procedur zarządzania incydentami (dalszy opis w sekcji *Stwierdzone nieprawidłowości*).

(akta kontroli str. 17-25, 30-48)

3. Według stanu na dzień 10 lipca 2024 r. w Urzędzie było zatrudnionych 108 osób uczestniczących w procesie przetwarzania informacji[31]. IOD prowadził szkolenia w celu zapoznania wszystkich pracowników Urzędu z przepisami z zakresu ochrony danych osobowych, zasadami bezpiecznego przetwarzania danych osobowych na stanowisku pracy[32]. W toku kontroli ustalono, że tylko pracownicy obsługi działu IT uczestniczyli w szkoleniach z zakresu bezpieczeństwa informacji[33] (dalszy opis w sekcji *Stwierdzone nieprawidłowości*).

(akta kontroli str. 9-25, 49-59, 681-687)

4. Stosownie do wymogów przewidzianych w § 20 ust. 2 pkt 14 rozporządzenia KRI[34] w Starostwie w 2023 r. przeprowadzono audyt wewnętrzny z zakresu bezpieczeństwa informacji. W *Sprawozdaniu z audytu wewnętrznego zadania zapewniającego Ocenę bezpieczeństwa informacji w Starostwie Powiatowym w Sochaczewie* audytor sformułował zalecenia dotyczące m.in. wdrożenia procedur zarządzania incydentami, opracowanie i wdrożenie całościowego Systemu Zarządzania Bezpieczeństwem Informacji, wdrożenia procedur dotyczących zachowania ciągłości działania. Sekretarz Powiatu wyjaśnił, że *obecnie jesteśmy na etapie weryfikacji i analiz obszarów związanych z systemami teleinformatycznymi oraz obszarów postępowania z naruszeniami w obszarze ochrony danych. W ramach konkursu „Cyberbezpieczny Samorząd", zamierzamy skorzystać z usług firm zewnętrznych specjalizujących się we wskazanej tematyce, posiadającej doświadczenie w opracowywaniu i wdrażaniu kompleksowej dokumentacji związanej z Systemem Zarządzania Bezpieczeństwem Informacji, aby wprowadzone procedury w jak najlepszym stopniu odpowiadały wymaganiom związanym z KRI oraz aby wypełnić zalecenia po-audytowe.*

---

31 W tym trzy osoby obsługujące dział IT i jedna osoba wykonująca zadania z zakresu obsługi prawnej zamówień publicznych zatrudnione były na umowę zlecenie.

32 Celem szkolenia było m.in.: zapoznanie uczestników z ogólnym rozporządzeniem o ochronie danych oraz dokumentacją opisującą zasady przetwarzania danych w Urzędzie.

33 M.in.: Bezpieczeństwo i ochrona przed ransomware, Cyberbezpieczny Urząd z EXATEL.

34 Według stanu prawnego obowiązującego na dzień przeprowadzenia audytu, obecnie: §19 ust. 2 pkt 14 rozporządzenia KRI.

(akta kontroli str. 9-16, 30-42, 306-318)

Stwierdzone nieprawidłowości

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

1. Nieprzeprowadzanie analizy ryzyka utraty integralności, poufności lub dostępności informacji, co było działaniem niezgodnym z §19 ust. 2 pkt 3 rozporządzenia KRI.

   Zgodnie z §19 ust. 2 pkt 3 rozporządzenia KRI *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań: przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analiz.*

   Sekretarz Powiatu wyjaśnił, że *dotychczas w Urzędzie funkcjonowała praktyka, że analizy ryzyka w zakresie bieżącego wskazywania zagrożeń związanych z bezpieczeństwem informacji i ochrony danych osobowych są wykonywane każdorazowo przy naruszeniu.*

   W toku kontroli, ustalono, że nie wystąpiły incydenty związane z naruszeniem bezpieczeństwa informacji.

   (akta kontroli str. 17-25, 43-48)

2. Nie opracowano i nie wdrożono procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji, co było działaniem niezgodnym z §19 ust. 2 pkt 13 rozporządzenia KRI.

   Zgodnie z ww. przepisem *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań: bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących*.

   Sekretarz Powiatu wyjaśnił, że *każdy z pracowników Urzędu zgłasza wystąpienie incydentu bezpośrednio do IOD, który przeprowadza postępowania wyjaśniające w przypadku wystąpienia incydentu. Informację o sposobie zgłoszenia incydentu do IOD, pracownicy otrzymują na szkoleniu z zakresu ochrony danych osobowych prowadzonych przez IOD.* Ponadto wyjaśnił, że *na ten moment incydenty w zakresie bezpieczeństwa informacji elektronicznych są zgłaszane Sekretarzowi w porozumieniu z działem IT, który decyduje, jak zareagować oraz komu zgłosić dalej dane problemy (…) Należy dodać, iż do chwili obecnej nie wystąpiły wskazane incydenty*.

   (akta kontroli str. 17-25, 30-48)

3. W okresie objętym kontrolą w Starostwie nie prowadzono szkoleń dla pracowników Urzędu z zakresu bezpieczeństwa informacji, co stanowiło naruszenie §19 ust. 2 pkt 6 rozporządzenia KRI, zgodnie z którym *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań: zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: a) zagrożenia bezpieczeństwa informacji, b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, c) stosowanie środków*

zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

Sekretarz Powiatu wyjaśnił, że *pracownicy, którzy biorą udział w procesie przetwarzania informacji zapoznają się z Polityką Bezpieczeństwa Informacji. Elementem składowym tego dokumentu jest Załącznik nr 12, który zawiera informacje dot. Instrukcji Zarządzania Systemem Informatycznym Starostwa Powiatowego w Sochaczewie. Instrukcja określa zasady i tryb wykonywania czynności w Systemie Informatycznym Starostwa Powiatowego w Sochaczewie związanych z ochroną danych osobowych, co wiąże się z bezpieczeństwem informacji. ASI przesyła również do pracowników istotne informacje związane z cyberbezpieczeństwem i bezpieczeństwem informacji, które otrzyma np. podczas szkoleń. W celu zwiększenia wiedzy i świadomości pracowników mamy zaplanowane przeprowadzenie szkolenia dla wszystkich pracowników w zakresie cyberbezpieczeństwa w ramach programu „Cyberbezpieczny Samorząd". Mając na uwadze fakt, że specjalistyczne szkolenia stanowią znaczne koszty, to nie jest możliwe częste ich organizowanie (…).*

(akta kontroli str. 9-25, 49-59, 681-692)

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli ocenia negatywnie działalność Starostwa w zakresie zapobiegania incydentom bezpieczeństwa informacji, ze względu na: nieprowadzenie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, a także brak wdrożenia kompleksowej procedury bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji oraz niezapewnienie pracownikom zaangażowanym w proces przetwarzania informacji odpowiednich szkoleń.

W Urzędzie przeprowadzono okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji, co było zgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI[35].

[35] Według stanu prawnego obowiązującego na dzień przeprowadzenia audytu, obecnie: §19 ust. 2 pkt 14 rozporządzenia KRI.

IV. Wnioski

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

Wnioski

1. Opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji o którym mowa w § 19 ust. 1 w związku z ust. 3 rozporządzenia KRI, uwzględniającego zalecenia normy PN-ISO/IEC 27001 i norm z nią związanych (PN-ISO/IEC 27002, PN-ISO/IEC 27005, PN-ISO/IEC 24762).
2. Zaktualizowanie PBI oraz procedur w niej określonych pod kątem faktycznie stosowanych praktyk w Urzędzie, m.in. z zakresu tworzenia i przechowywania kopii zapasowych.
3. Prowadzenie aktualnej i kompletnej inwentaryzacji sprzętu informatycznego obejmującej jego rodzaj i konfigurację.
4. Dostosowanie zakresu zadań i obowiązków osoby pełniącej funkcje zastępcy IOD tak aby uniknąć konfliktu interesów.
5. Prowadzenie analiz ryzyka w związku z potrzebą zachowania ciągłości działania systemów informatycznych i podejmowanie działań minimalizujących stwierdzone ryzyko.
6. Ustanowienie polityk ciągłości działania oraz opracowanie i wdrożenie planów zapewnienia ciągłości działania, planów odtworzeniowych oraz zapewnienie ich okresowego testowania.
7. Zapewnienie niezwłocznego odbierania uprawnień do systemów informatycznych byłym pracownikom Starostwa.
8. Zapewnienie szyfrowania danych zgromadzonych na komputerach przenośnych.
9. Regularne testowanie kopii zapasowych oraz przechowywanie ich poza miejscem wytworzenia.
10. Prowadzenie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji i podejmowanie działań minimalizujących stwierdzone ryzyko.
11. Opracowanie i wdrożenie procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji.
12. Zawieranie w umowach o świadczenie usług informatycznych postanowień gwarantujących odpowiedni poziom bezpieczeństwa informacji.
13. Prowadzenie ewidencji osób przebywających w pomieszczeniu serwerowni oraz wyeliminowanie czynników zwiększających ryzyka związane z zagrożeniami fizycznymi i środowiskowymi w tym pomieszczeniu.
14. Zapewnienie pracownikom zaangażowanym w proces przetwarzania informacji odpowiednich szkoleń w tym zakresie.

V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

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

Obowiązek poinformowania NIK o sposobie wykonania wniosków

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

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

Warszawa, 2 sierpnia 2024 r.

Najwyższa Izba Kontroli
Departament Administracji Publicznej
w zastępstwie Dyrektora
Agnieszka Klimowicz
p.o. Wicedyrektor

/podpisano elektronicznie/

Kontroler
Łukasz Hertel
Główny specjalista kontroli państwowej

/podpisano elektronicznie/