NAJWYŻSZA IZBA KONTROLI
DELEGATURA W BYDGOSZCZY

LBY.410.12.2.2024

Jarosław Tadych
Starosta Sępoleński

Starostwo Powiatowe
w Sępólnie Krajeńskim
ul. T. Kościuszki 11
89-400 Sępólno Krajeńskie

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 Sępólnie Krajeńskim[1], ul. T. Kościuszki 11, 89-400 Sępólno Krajeńskie
Kierownik jednostki kontrolowanej	Jarosław Tadych, Starosta Sępoleński, od 29 stycznia 2014 r.
Zakres przedmiotowy kontroli	Rozwiązania organizacyjne i techniczne w zakresie zapewnienia bezpieczeństwa przetwarzania informacji oraz zapewnienia ciągłości działania w Urzędzie i ich stosowania.
Okres objęty kontrolą	Od 1 stycznia 2023 r. do dnia zakończenia kontroli w 2024 r.[2]
Podstawa prawna podjęcia kontroli	art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[3]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Bydgoszczy
Kontroler	Karolina Lahutta, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LBY/95/2024 z 31 maja 2024 r.

(akta kontroli str.1-10)

II. Ocena ogólna[4] kontrolowanej działalności

OCENA OGÓLNA

W kontrolowanym okresie w Starostwie podejmowano działania na rzecz zapewnienia bezpieczeństwa informacji i ciągłości działania. Skoncentrowano je jednak wokół ochrony danych osobowych. W Starostwie obowiązywała Polityka Bezpieczeństwa Przetwarzania Danych Osobowych[5] odwołująca się do szeregu procedur wewnętrznych, w szczególności dotyczących zarządzania systemem informatycznym. Odniesiono się w nich do najważniejszych zagadnień związanych z bezpieczeństwem informacji takich jak: zarządzanie uprawnieniami, uwierzytelnianie dostępu, tworzenie kopii zapasowych, przygotowanie sprzętu do wydania na zewnątrz. Posiadano również ocenę ryzyka dla utraty atrybutów bezpieczeństwa informacji, a jednocześnie naruszenia praw i wolności osób fizycznych, z opisem stosowanych w Starostwie środków obniżających jego poziom. Istotną słabością przyjętych rozwiązań było nieobjęcie nimi informacji spoza katalogu danych osobowych. Wynikało to z niepełnej identyfikacji zasobów informacyjnych podlegających ochronie. Ponadto niektóre procedury, w szczególności dotyczące zarządzania uprawnieniami i kopiami zapasowymi oraz plan ciągłości działania były nieprecyzyjne. W Starostwie wyznaczono osoby odpowiedzialne za bezpieczeństwo informacji, w tym Inspektora Ochrony Danych[6], któremu zapewniono niezależność i możliwość działania w sytuacji braku konfliktu interesów. Kontrola wykazała jednak nieprawidłowości we wdrażaniu środków zapewnienia bezpieczeństwa informacji, w tym stanowiących naruszenia rozporządzenia Rady Ministrów z dnia 21 maja 2024

[1] Dalej: „Starostwo".
[2] Czynności kontrolne zakończono 30 lipca 2024 r.
[3] Dz. U. z 2022 r. poz. 623, dalej: ustawa o NIK
[4] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[5] Dalej: „PBPDO".
[6] Dalej: „IOD".

r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[7] oraz poprzednio obowiązującego rozporządzenia z 12 kwietnia 2012 r.[8] Stwierdzone nieprawidłowości dotyczyły w szczególności:

- stosowania przez dwóch pracowników haseł dostępu do systemu informatycznego nieodpowiadającego wymogom PBPDO;
- nadaniu jednemu użytkownikowi (z 13 analizowanych) nadmiernych uprawnień w systemie operacyjnym komputera;
- opóźnień w odbieraniu uprawnień do pracy w systemach teleinformatycznych;
- naruszenia przepisów wewnętrznych przy przechowywaniu kopii zapasowych;
- nieustanowienia zasad gwarantujących bezpieczną pracę na odległość;
- niewdrożenia środków technicznych i organizacyjnych minimalizujących ryzyko wskazanych jako rozwiązania stosowane w dokumencie *Ocena ryzyka naruszenia praw i wolności osób fizycznych;*
- niezawarcia w dwóch umowach utrzymania oprogramowania zapisów zobowiązujących wykonawcę do zagwarantowania odpowiedniego poziomu bezpieczeństwa wszystkich informacji, do jakich może mieć dostęp w ramach wykonywania umowy.

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

OBSZAR

1. Organizacja bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych

Opis stanu faktycznego

1.1. W Starostwie nie dokonano pełnej identyfikacji aktywów informacyjnych wymagających ochrony. Przeprowadzono ją częściowo w odniesieniu do danych osobowych[10]. Nie spisano jednakże innych informacji wymagających ochrony, takich jak powierzone przez kontrahentów tajemnice przedsiębiorstwa, zasady bezpieczeństwa fizycznego i informatycznego w jednostce, informacje finansowe z deklaracji podatkowych itp.

(akta kontroli str. 212-337, 340, 585)

1.2. W kontrolowanym okresie w Starostwie nie opracowano systemu zarządzania bezpieczeństwem informacji[11] w rozumieniu dokumentu, który obejmowałby wszystkie strategie, regulaminy i instrukcje związane z bezpieczeństwem informacji oraz uwzględniał wszystkie informacje, jakie były przetwarzane w jednostce. Obowiązujące w Starostwie procedury w większości dotyczyły wyłącznie bezpieczeństwa danych osobowych. Stanowiły one uporządkowany zbiór, którego głównym dokumentem była *Polityka bezpieczeństwa przetwarzania danych osobowych*. Odwoływała się ona do procedur i wytycznych opracowanych wyłącznie

[7] Dz. U. z 2024 r., poz. 773. Dalej: „rozporządzenie KRI z 2024 r.".
[8] Tj. 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). Dalej: „rozporządzenie KRI z 2012 r.".
[9] Oceny cząstkowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena cząstkowa może być sformułowana jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej.
[10] Wymienione zostały w pkt 5 rozdziału 4 PBPDO oraz w rejestrach czynności przetwarzania danych osobowych i upoważnień do przetwarzania danych osobowych.
[11] Dalej: „SZBI".

dla ochrony danych osobowych, jak i nielicznych dokumentów o charakterze ogólnym, m.in. procedury zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem. Dodatkowo w Starostwie obowiązywały regulacje związane z ochroną informacji niejawnych oraz zasady ochrony zbiorów ksiąg rachunkowych. Taka struktura dokumentacji powodowała, że brakowało niektórych szczegółowych procedur dla ochrony informacji niebędących danymi osobowymi, co opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 212-337, 340-364, 384-389)

Zadanie opracowania i stałej aktualizacji dokumentacji związanej z przetwarzaniem danych oraz instrukcji dotyczących bezpieczeństwa danych osobowych przypisano w zakresie obowiązków IOD.

(akta kontroli str. 99)

1.3. W kontrolowanym okresie, podstawowymi regulacjami wewnętrznymi dotyczącymi ochrony danych osobowych były zaktualizowane w marcu 2022 r. *Polityka bezpieczeństwa przetwarzania danych osobowych – dokument główny* oraz *Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych*[12]. Uzupełniały je: procedury nadawania uprawnień do przetwarzania danych osobowych, w tym nadawania uprawnień w systemach informatycznych, procedura postępowania w przypadku naruszenia ochrony danych osobowych, ocena ryzyka naruszenia praw i wolności osób fizycznych[13], wytyczne dla pracowników dotyczące ochrony danych osobowych[14] oraz prowadzone rejestry: czynności przetwarzania danych osobowych, osób upoważnionych do przetwarzania danych osobowych, pomieszczeń, w których wykonywane są operacje przetwarzania danych osobowych, naruszeń ochrony danych osobowych.

W dniu zatwierdzenia IOD przekazał procedury naczelnikom poszczególnych wydziałów Starostwa w celu wewnętrznego rozpowszechnienia i stosowania przez podległych pracowników.

(akta kontroli str. 212-337, 384)

Wprowadzone procedury stanowiły realizację obowiązków określonych w art. 30 i art. 35 RODO[15] oraz były elementem rozliczalności zapewnienia w Starostwie realizacji wymogów wynikających z art. 29, 32 i 33 RODO[16].

W prowadzonym rejestrze umów powierzenia nie odnotowano części zawartych w tym zakresie umów. Szczegółowe ustalenia zawarto w sekcji *Stwierdzone nieprawidłowości*.

---

[12] Odnosząca się do kwestii: Zabezpieczenia infrastruktury informatycznej i telekomunikacyjnej, Zabezpieczenia baz danych i oprogramowania przetwarzającego dane osobowe, Procedury dostępu podmiotów zewnętrznych, Procedury korzystania z Internetu, procedury korzystania z poczty elektronicznej. Metod i środków uwierzytelniania, procedury rozpoczęcia, zawieszenia i zakończenia pracy, procedury tworzenia kopii zapasowych, sposoby, miejsca i okresu przechowywania elektronicznych nośników informacji i wydruków, procedury zabezpieczenia systemu informatycznego w tym przed wirusami komputerowymi, procedury wykonywania przeglądów i konserwacji.

[13] Odpowiadająca również dla kategorii danych D i E wymogom formalnym dla dokumentu: Ocena skutków dla ochrony danych osobowych (DPIA).

[14] Zawierające zestaw nakazów i zakazów związanych z przetwarzaniem danych osobowych w systemach informatycznych. Dodatkowo procedury pustego biurka i czystego ekranu.

[15] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) Dz. Urz. UE.L2016 Nr 119, poz. 1, ze sprostowaniami. Dalej: „RODO".

[16] Nie sformułowano natomiast procedur odnoszących się do realizacji praw osób, których dane osobowe dotyczą, ograniczając się jedynie do przytoczenia przepisów z RODO i nie przedstawiając szczegółowych rozwiązań w jaki sposób należy ją zrealizować w Starostwie.

(akta kontroli str. 212-337, 367-374, 438-486)

1.4.-1.7. W Starostwie opracowano plan postępowania w sytuacji wystąpienia ryzyk mogących zakłócić ciągłość działania: a) dla przetwarzania danych osobowych w systemach informatycznych: awaria systemów informatycznych, awaria sprzętu informatycznego, brak zasilania elektrycznego z sieci energetycznej, brak dostępu do sieci internetowej, b) dla przetwarzania danych osobowych bez udziału systemów informatycznych: brak dostępu do pomieszczeń, w których przetwarzane są dane osobowe. Akceptowalny czas przywrócenia ciągłości działania określono wyłącznie dla sytuacji awarii sprzętu, co szczegółowo opisano w sekcji *Stwierdzone nieprawidłowości*.

Nie opracowano polityk zapewnienia ciągłości działania. Opracowane plany ciągłości działania nie były testowane, co szczegółowo opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 302-306)

Dodatkowo w Starostwie, na podstawie § 16 pkt 1 rozporządzenia Rady Ministrów z dnia 27 kwietnia 2004 r. w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym[17], opracowano plan przemieszczania i zapewniania warunków funkcjonowania Starosty Sępoleńskiego na głównym stanowisku kierowania w zapasowym miejscu pracy.

(akta kontroli str. 669-672)

1.8. Starosta podał, że wynikający z § 19 ust. 2 pkt 1 rozporządzenia w sprawie KRI z 2024 r. oraz § 20 ust. 2 pkt 1 rozporządzenia w sprawie KRI z 2012 r. obowiązek zapewnienia aktualizacji regulacji wewnętrznych dotyczących bezpieczeństwa informacji realizowano poprzez ich bieżącą analizę. Wicestarosta dodał, że w szczególności dokonano analizy dokumentacji związanej z zapewnieniem bezpieczeństwa informacji przed złożeniem wniosku aplikacyjnego pn. *Podniesienie poziomu cyberbezpieczeństwa Starostwa Powiatowego w Sępólnie Krajeńskim*, realizowanego w ramach programu *Cyberbezpieczny Samorząd* oraz, że w wyniku przeglądu uznano za zasadne pozyskanie środków zewnętrznych na opracowanie, wdrożenie, profesjonalny przegląd i aktualizację dokumentacji SZBI.

Czynności przeglądu nie były dokumentowane. Obowiązku takiego nie wprowadzały procedury wewnętrzne.

(akta kontroli str. 586, 595)

1.9. Obowiązki i odpowiedzialność z tytułu wdrażania rozwiązań w zakresie zapewnienia bezpieczeństwa informacji oraz zapewnienia ciągłości działania przydzielone[18] były w kontrolowanym okresie Administratorowi Systemów Informatycznych[19]. W zakresie obowiązków ASI zdefiniowano zadania związane m.in. z formułowaniem sposobu określania uprawnień w systemach informatycznych, realizacją decyzji dotyczących nadawania uprawnień dostępu do danych i wybranych funkcji narzędzi służących do ich przetwarzania, planowania inwestycji oraz dostaw i usług niezbędnych dla utrzymania i rozwoju środowiska IT w Starostwie, planowaniem i wykonywaniem zadań związanych z tworzeniem kopii bezpieczeństwa systemów i danych, monitorowaniem stanu środowiska IT, sprzętu IT, oprogramowania oraz aktywności sieciowej użytkowników, monitorowaniem legalności oprogramowania na stacjach roboczych użytkowników, systematycznym aktualizowaniem oprogramowania systemowego, aplikacyjnego i ochronnego,

[17] Dz. U. z 2004 r., Nr 98, poz. 978, ze zm.
[18] Na podstawie zarządzenia nr 37/2022 od 28 grudnia 2022 r. na ASI wyznaczona została osoba zatrudniona na stanowisku informatyka.
[19] Dalej: „ASI".

przygotowaniem we współpracy z IOD instrukcji dla użytkowników systemów informatycznych zgodnych z celami i metodologią wdrożonej polityki bezpieczeństwa informacji, prowadzeniem szkoleń stanowiskowych na temat bezpiecznych zachowań użytkowników w środowisku systemu IT.

Wyznaczono również Zastępcę ASI, przypisując mu zadania związane z nadawaniem i odbieraniem uprawnień w systemach informatycznych oraz tworzeniem kopii bezpieczeństwa.

Osoby wyznaczone posiadały wykształcenie kierunkowe informatyczne oraz uczestniczyły w wielu szkoleniach z zakresu cyberbezpieczeństwa i ochrony danych osobowych. Dodatkowo Zastępca ASI ukończył w grudniu 2023 r. wyższe studia magisterskie na kierunku *Zintegrowany system bezpieczeństwa narodowego* w specjalności *Cyberbezpieczeństwo*.

(akta kontroli str. 83-90, 100-103, 375-376, 565)

1.10. Stosownie do art. 8 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[20] w zw. z art. 37 ust. 1 lit a RODO w Starostwie wyznaczony[21] został inspektor ochrony danych osobowych. Był on etatowym pracownikiem Starostwa, któremu obok funkcji IOD powierzono również obowiązki na stanowisku inspektora w Biurze Rady Powiatu. Osoba, której powierzono funkcję IOD skończyła czterodniowe szkolenie w celu przygotowania do pełnienia funkcji IOD oraz kilka szkoleń jednodniowych w zakresie ochrony danych osobowych.

(akta kontroli str. 15, 97-99, 104-106, 377-381)

Dopełniono obowiązku publikacji danych kontaktowych IOD, określonego art. 11 ustawy o ochronie danych osobowych w zw. z art. 37 ust. 7 RODO. W Biuletynie Informacji Publicznej i na stronie internetowej Starostwa wyświetlała się automatycznie klauzula informacyjna zawierająca imię, nazwisko oraz telefon i adres email IOD.

(akta kontroli str. 382-383)

1.11. W strukturze organizacyjnej Starostwa IOD wyodrębniony był jako oddzielne stanowisko podlegające bezpośrednio Staroście. Odpowiadało to wymogom art. 38 ust. 3 RODO. Zadania IOD wskazane zostały w § 49 regulaminu organizacyjnego Starostwa[22] i obejmowały obowiązki określone w art. 39 ust. 1 RODO. Powtórzone one zostały w zakresie czynności, uprawnień i odpowiedzialności pracownika. Dodatkowo w dokumencie tym uznano, że wykonywanie czynności przypisanych pracownikowi z tytułu zajmowania stanowiska inspektora w Biurze Rady Powiatu nie jest związane z określaniem sposobów i celów przetwarzania danych.

W celu zapewnienia IOD wykonywania obowiązków w sposób niezależny i skuteczny w Starostwie obowiązywała ponadto pisemna polityka przeciwdziałania konfliktowi interesów w przedmiocie powoływania i zdolności do pełnienia funkcji IOD.

(akta kontroli str. 21-28, 74-78, 97-99, 238-239)

1.12. W kontrolowanym okresie w Starostwie dopełniony był również obowiązek wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa[23], określony art. 21 ust. 1 ustawy z dnia

[20] Dz. U. z 2019 r., poz. 1781. Dalej: „ustawa o ochronie danych osobowych".
[21] Zarządzeniem nr 16/2018 Starosty Sępoleńskiego z 25 maja 2018 r. w sprawie wyznaczenia Inspektora Ochrony Danych.
[22] Wprowadzonego uchwałą nr 38/120/2020 Zarządu Powiatu w Sępólnie Krajeńskim z dnia 23 października 2020 r. w sprawie uchwalenia Regulaminu Organizacyjnego Starostwa Powiatowego w Sępólnie Krajeńskim, obowiązującego od 1 listopada 2020 r.
[23] Dwie osoby kontaktowe zgłoszone były od 3 marca 2021 r.

5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[24]. Była ona odpowiedzialna jedynie za zgłaszanie incydentów występujących w Starostwie, tj. nie skorzystano z przewidzianej art. 21 ust. 2 i 3 ustawy o KSC możliwości wyznaczenia jednej osoby dla wszystkich jednostek organizacyjnych Powiatu oraz jednostek podległych lub nadzorowanych przez jego organy. Tymczasem spośród 17 jednostek 14 nie miało do momentu wszczęcia kontroli NIK wyznaczonej osoby do kontaktu. Szczegółowe ustalenia w tym zakresie zawarto w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 15, 79-82, 85, 95, 419-421, 434)

1.13. Wprowadzona w Starostwie PBPDO nie zawierała zapisów odnośnie sporządzenia dodatkowych dokumentów wykonawczych. Wszystkie dokumenty, do których się odwoływała stanowiły załączniki do dokumentu głównego.

(akta kontroli str. 212-337)

1.14. W kontrolowanym okresie w Starostwie nie korzystano z oprogramowania wspierającego inwentaryzację sprzętu. Inwentaryzacja oparta była na prowadzonych w układzie tabelarycznym zestawieniach sprzętu wg rodzajów z dodatkowymi kartami konfiguracji dla poszczególnych urządzeń przedstawiającymi takie dane jak miejsce lokalizacji, rodzaj sprzętu, model sprzętu, numer seryjny, system operacyjny, adres IP, użytkownik, parametry techniczne: procesor, pamięć, dysk twardy, ewentualne urządzenia peryferyjne, relacje z podstawowym oprogramowaniem. Dodatkowo prowadzony był wykaz oprogramowania na licencje teleinformatyczne.

Oględziny 15 sprzętów[25] potwierdziły aktualność danych zawartych na kartach konfiguracji. W wykazie licencji pominięto natomiast jedno wykorzystywane oprogramowanie, co szczegółowo opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 347, 487-490, 587, 644-668)

1.15. Starostwo przystąpiło do programu *Cyberbezpieczny Samorząd*. Umowę o powierzenie grantu podpisano w toku kontroli NIK, tj. w czerwcu 2024 r. Zakłada ona wydatkowanie w terminie 24 miesięcy kwoty 623,0 tys. zł (100% dofinansowanie zewnętrzne) na podniesienie poziomu bezpieczeństwa i zarządzania ryzykiem związanym z cyberbezpieczeństwem w obszarach organizacyjnym, kompetencyjnym i technicznym, tj. m.in. opracowanie, wdrożenie, przegląd i aktualizację SZBI, audyt zgodności z wymogami KRI, szkolenia specjalistyczne pracowników działu IT, szkolenia z zakresu cyberbezpieczeństwa dla kadry kierowniczej i pracowników, organizację kampanii phishingowych dla pracowników oraz zakup i wdrożenie urządzenia do backupu, urządzenia do zbierania logów, oprogramowania antywirusowego oraz urządzeń sieciowych typu switch.

Efekty Projektu ocenione zostaną przy użyciu mierników produktu odnoszących się m.in. do liczby: przeszkolonych pracowników, systemów służących zwiększeniu poziomu bezpieczeństwa informacji, użytkowników nowych i zmodernizowanych usług, produktów publicznych i procesów cyfrowych.

(akta kontroli str. 15-17, 491-514)

Stwierdzone nieprawidłowości

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

1. W Starostwie nie dokonano pełnej identyfikacji aktywów informacyjnych wymagających ochrony. Przeprowadzono ją tylko w odniesieniu do danych

[24] Dz. U. z 2024 r., poz. 1077. Dalej: „ustawa o KSC".
[25] 10 komputerów, jednego serwera, dwóch laptopów, routera i jednej drukarki

osobowych. Nie spisano jednakże innych informacji wymagających ochrony. Nie dokonano również ich klasyfikacji z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na utratę atrybutów bezpieczeństwa, co należy uznać za działanie nierzetelne.

Starosta wyjaśnił m.in., że przyczyną powyższego była ocena, że zidentyfikowane zostały wszystkie zbiory danych podlegające ochronie. Dodał, że jeżeli w Starostwie istniały zbiory danych, których identyfikację pominięto, to wynikało to z braku świadomości w tym zakresie.

(akta kontroli str. 212-374, 585)

W odniesieniu do powyższych wyjaśnień NIK zauważa, że identyfikacja zbiorów danych jest kluczowa dla budowy SZBI, w myśl zasady, że aby coś chronić trzeba być świadomym posiadania zasobu i jego znaczenia. Ochrony wymagają również zbiory informacji i pojedyncze informacje nieobejmujące danych osobowych i informacji niejawnych takie jak chociażby: powierzone Starostwu tajemnice przedsiębiorstw, konfiguracje zabezpieczeń sprzętu i budynków, ewidencja stowarzyszeń, dane z deklaracji podatkowych.

2. W Starostwie nie opracowano Systemu Zarządzania Bezpieczeństwem Informacji, o którym mowa w § 19 ust. 1 rozporządzenia w sprawie KRI z 2024 r., a wcześniej § 20 ust. 1 rozporządzenia w sprawie KRI z 2012 r. Przyjęte regulacje ograniczały się w najważniejszych aspektach do kwestii zabezpieczenia danych osobowych oraz danych niejawnych i nie obejmowały bezpieczeństwa innych informacji przetwarzanych przez jednostkę. Było to następstwem niezidentyfikowania wszystkich posiadanych i przetwarzanych przez Starostwo zbiorów danych.
   Starosta wyjaśnił m.in., że przyczyną powyższego było przekonanie o wypełnianiu przez obowiązujące procedury wymogów wynikających z przepisów.

   (akta kontroli str. 212-374, 585)

3. W ramach sprawowanego nadzoru Starosta nie zapewnił, aby wszystkie jednostki organizacyjne Powiatu oraz jednostki podległe i nadzorowane przez jego organy wypełniły obowiązek wynikający z art. 21 ust. 1 i 22 ust. 1 pkt 5 ustawy o KSC, tj. wyznaczyły i zgłosiły osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Do czasu wszczęcia niniejszej kontroli zgłoszenia takiego nie dokonało 14 z 17 jednostek.

   Starosta wyjaśnił, że w jednostkach organizacyjnych i nadzorowanych przez organy Powiatu nie przeprowadzono kontroli związanych z zapewnieniem bezpieczeństwa informacji, w związku z powyższym fakt braku zgłoszeń nie został wykryty. Podał również, że jednostki zostaną zobowiązane do bezzwłocznego dokonania zgłoszenia.

   W toku kontroli dziewięć jednostek dokonało zgłoszenia.

   (akta kontroli str. 15, 79-82, 85, 95, 419-421, 434)

4. W prowadzonym w Starostwie rejestrze umów powierzenia nie odnotowano czterech z pięciu poddanych analizie umów powierzenia przetwarzania danych osobowych obowiązujących w kontrolowanym okresie, co należy uznać za działanie nierzetelne.

   Starosta wyjaśnił, że wynikało to z uchybienia pracowników merytorycznych, którzy nie przekazali dokumentów IOD. Podał również, że w trakcie kontroli rejestr został uzupełniony.

   (akta kontroli str. 373-374, 435-486, 558)

5. Na liście posiadanych licencji obejmującej w dniu poprzedzającym rozpoczęcie kontroli 15 pozycji, nie ujęto oprogramowania wykorzystywanego do ewidencjonowania i inwentaryzacji środków trwałych, co było działaniem nierzetelnym.

   Starosta wyjaśnił, że przyczyną nieujęcia oprogramowania na wykazie było uchybienie pracownika wynikające z odległej daty zakupu oprogramowania oraz obecnie braku wsparcia producenta dla systemu.

   (akta kontroli str. 347, 487-490, 587)

6. Plan ciągłości działania Starostwa sporządzony został nierzetelnie, gdyż nie definiował krytycznych procesów i ich minimalnych akceptowalnych konfiguracji niezbędnych do wznowienia działania oraz docelowych czasów wznowienia działalności. Ponadto nie był testowany, co również należy uznać za działanie nierzetelne.

   Brak ww. elementów w planie ciągłości działania Starosta wyjaśnił brakiem doświadczenia pracownika odpowiedzialnego za jego opracowanie. Dodał, że mając na uwadze złożoność tematyki związanej z zapewnieniem ciągłości działania, Starostwo w ramach programu *Cyberbezpieczny Samorząd* planuje przegląd i aktualizację dokumentacji SZBI.

   Zaniechanie testowania planów ciągłości Starosta wyjaśnił brakiem takiego obowiązku, wynikającym m.in. z niewdrożenia norm ISO. Dodał jednakże, że planuje się przeprowadzenie testów w IV kwartale 2024 r. w ramach ćwiczeń związanych z zarządzaniem kryzysowym.

   (akta kontroli str. 302-306, 585-586)

   W odniesieniu do wskazanych wyjaśnień NIK zauważa, że testowanie planów ciągłości działania powinno być rozpatrywane w kategoriach rzetelności, jako narzędzie potwierdzenia, że jednostka jest przygotowana na wystąpienie sytuacji awaryjnej, osoby znają swoje role, a założone rozwiązania się sprawdzą.

7. Przyjęta od 1 marca 2024 r. struktura organizacyjna nie spełniała wymogów standardu A.3. *Struktura organizacyjna* załącznika do komunikatu Nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych[26]. Przekazując zmianą zakresu obowiązków zadania w zakresie informatyzacji Wydziału Geodezji, Kartografii i Nieruchomości Starostwa pracownikowi tego wydziału, nakazano wykonywanie czynności pod ścisłym nadzorem ASI, który w strukturze organizacyjnej nie występował jako odrębne stanowisko oraz nie był bezpośrednim przełożonym ww. pracownika. Zadanie ścisłego nadzoru nie było powtórzone w zakresie czynności i obowiązków pracownika pełniącego funkcję ASI oraz nie wynikało z innych dokumentów i procedur, gdyż te nie uwzględniały kwestii formalnego przekazania części zadań ASI innemu pracownikowi. Dodatkowo ASI nie miał kompletu narzędzi do sprawowania nadzoru, w szczególności uprawnień administratora do systemu dziedzinowego wykorzystywanego przez Wydział Geodezji, Kartografii i Nieruchomości Starostwa.

   Starosta wyjaśnił, że założeniem pracodawcy było przekazanie przez ASI pracownikowi Wydziału Geodezji, Kartografii i Nieruchomości wiedzy merytorycznej i praktycznej związanej z wykonywanymi zadaniami, w tym w zakresie obsługi i nadzoru nad wykorzystywanym przez Wydział systemem. ASI sprawuje nadzór nad siecią informatyczną Starostwa i w tym zakresie nadzoruje pracę wszystkich pracowników. W najbliższym czasie w Starostwie planowana jest aktualizacja Regulaminu Organizacyjnego związana m.in.

[26] Dz.Urz. Ministerstwa Finansów z 2009 r. Nr 15 poz. 84

z przeniesieniem Wydziału Geodezji, Kartografii i Nieruchomości do nowej lokalizacji. Stanowisko pracownika Wydziału (którego obciążono zadaniami informatycznymi) zostanie wyodrębnione i właściwie umiejscowione. Dodał, że zapis „ścisły nadzór" nie oddaje w prawidłowy sposób intencji pracodawcy i zostanie zmieniony.

(akta kontroli str. 23-78, 83-87, 390-395, 588)

OCENA CZĄSTKOWA

W kontrolowanym okresie w Starostwie wdrożono środki organizacyjne mające na celu zapewnienie bezpieczeństwa informacji i ciągłości działania. Szczególnej ochronie poddano dane osobowe, dla których stworzono PBPDO oraz spisano instrukcję zarządzania systemem informatycznym, w którym te dane są przetwarzane. Powołano IOD zapewniając mu niezależność i wykluczając działanie w sytuacji konfliktu interesów. Wyznaczono również osoby odpowiedzialne za zapewnienie bezpieczeństwa informacji i kontakty z podmiotami krajowego systemu cyberbezpieczeństwa. Byli to pracownicy posiadający odpowiednie kwalifikacje i doświadczenie zawodowe. Starostwo posiadało przygotowany plan ciągłości działania. Nie opracowano jednak i nie wdrożono uregulowań dotyczących ochrony danych innych niż dane osobowe i informacje niejawne.

OBSZAR

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

Opis stanu faktycznego

2.1. W Starostwie stosowano praktykę ograniczania uprzywilejowanego dostępu do systemów informatycznych pracownikom niebędącym pracownikami służb informatycznych. Badanie w zakresie zapobiegania możliwości zainstalowania nieautoryzowanego oprogramowania na 13 urządzeniach, w tym siedmiu komputerach i sześciu laptopach wykazało, że w 12 przypadkach zastosowano mechanizmy blokujące. W jednym przypadku pracownikowi pozostawiono uprawnienia administratora, mimo iż nie było to konieczne z punktu widzenia realizowanych przez niego obowiązków. Szczegółowe ustalenia w tym zakresie zawarto w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 515-517, 577-581)

W kontrolowanym okresie Starostwo nie dysponowało służbowymi telefonami komórkowymi. Udostępniało jedynie wybranym pracownikom służbowe karty SIM. W procedurze ich używania wpisano zakaz instalowania obcego oprogramowania w telefonie ze służbową kartą SIM, chyba że jest to konieczne do wykonywania obowiązków służbowych oraz prawidłowego działania poszczególnych programów i aplikacji, w tym niewykorzystywania internetu w celach służbowych, oraz obowiązek odpowiedniego zabezpieczenia dostępu do danych istotnych dla Starostwa przechowywanych na urządzeniu, w szczególności poprzez zastosowanie blokady hasłem.

(akta kontroli str. 385-389)

2.2.–2.3. Wprowadzone zostały również procedury nadawania i odbierania uprawnień w systemach informatycznych Starostwa[27]. Określały one obowiązki dyrektorów wydziałów i ASI w procesie zarządzania uprawnieniami oraz sporządzanie kart uprawnień. Procedury te dopuszczały jednak ustne wnioskowanie o nadawanie uprawnień, ponadto nie określały sposobu postępowania w przypadkach

[27] Procedura nadawania uprawnień do przetwarzania danych osobowych w systemach informatycznych w Starostwie Powiatowym w Sępólnie Krajeńskim stanowiąca załącznik nr 17 do PBPDO.

administrowania systemem przez administratorów zewnętrznych (dostawców oprogramowania). W rezultacie brak było dokumentacji z wnioskowania o przyznanie dostępu o systemów informatycznych, a karty uprawnień nie były sporządzane w odniesieniu do części przypadków, tj. nie były praktykowane w przypadkach nadawania uprawnień do systemów administrowanych przez ich dostawców. Szczegółowe ustalenia w tym zakresie opisano w sekcji *Stwierdzone nieprawidłowości*.

Wprowadzone procedury nieprecyzyjnie określały również proces odbierania uprawnień. Zobowiązując administratorów systemów informatycznych do tej czynności nie określały osób odpowiedzialnych za przekazanie informacji o takiej konieczności, czasu, w jakim uprawnienia powinny zostać odebrane, sposobu udokumentowania czynności, a przede wszystkim sposobu postępowania w przypadku administrowania systemami przez dostawców oprogramowania. Szczegółowe ustalenia w tym zakresie zawarto w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 309-310, 422, 470, 476, 595-596, 627)

Badanie na próbie 15 pracowników wykonujących zadania w systemach informatycznych Starostwa wykazało, że w jednym przypadku przyznane zostały uprawnienia do systemu nieodpowiadające zakresowi obowiązków. Szczegółowe ustalenia zawarto w sekcji *Stwierdzone nieprawidłowości*.

Badanie na próbie trzech pracowników, którzy zakończyli zatrudnienie w Starostwie[28] wykazało, że w dwóch przypadkach uprawnienia nie zostały odebrane niezwłocznie, co szczegółowo opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 590-592, 600-626, 632-639)

2.4. W celu zapewnienia ochrony informacji dostęp do systemów operacyjnych komputerów Starostwa oraz zbiorów danych w systemach dziedzinowych oparto na mechanizmie uwierzytelniania.

Badanie zabezpieczeń dostępu do trzech wybranych systemów dziedzinowych oraz dostępu do systemów operacyjnych na 10 stacjach roboczych wykazało, że:

- stosowano metody uwierzytelniania dostępu;
- zasady bezpieczeństwa haseł do systemu operacyjnego zostały skonfigurowane za pomocą narzędzi administracyjnych wymuszających długość i okres zmiany hasła. Wprowadzone wymogi dla długości haseł były wyższe niż przewidywała PBPDO, ponadto niejednolicie ustawiono – nieokreślone w PBPDO - wymagania co do historii zmian haseł;
- hasła dostępu do systemów operacyjnych na wszystkich 10 stanowiskach odpowiadały pod względem długości wymogom PBPDO, natomiast w przypadku systemów dziedzinowych zgodność zachowano w ośmiu przypadkach. W dwóch przypadkach stosowane hasła nie odpowiadały wymogom PBPDO, co szczegółowo opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 326-327, 518-523)

2.5. Przyjęte w Starostwie procedury zwracały uwagę na ryzyko utraty poufności informacji na skutek nieprawidłowego ustawienia monitorów komputerowych i nakazywały odpowiednie zachowania w tej kwestii. Nakazywano również

[28] Podano wyłącznie dane w odniesieniu do systemów, które pozwalały na jednoznaczne ustalenie daty odbioru uprawnień. Pomięto dwóch pracowników, których uprawnienia zostały odebrane w systemie po zakończeniu zatrudnienia, jednak z uwagi na cechy programu nie można ustalić daty zablokowania uprawnień.

wywoływanie blokowanego hasłem wygaszacza ekranu przed opuszczeniem stanowiska pracy.

Oględziny stanowisk pracy na sali obsługi interesantów Wydziału Komunikacji i Dróg wykazały, że monitory usytuowane były w sposób uniemożliwiający wgląd danych przez osoby nieuprawnione. Powyższe działania spełniały wymogi § 19 ust. 2 pkt 7 rozporządzenia w sprawie KRI z 2024 r.

(akta kontroli str. 301, 307, 328, 413)

2.6. W Starostwie nie opracowano procedur dotyczących bezpiecznej pracy przy przetwarzaniu mobilnym i na odległość. Szczegółowe ustalenia w tym zakresie zawarto w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 212-337, 341-342)

2.7. W Starostwie nie stosowano rozwiązań polegających na szyfrowaniu danych zgromadzonych na urządzeniach mobilnych. Jak podał Starosta wynikało to z faktu korzystania z laptopów wyłącznie w budynku Starostwa, za wyjątkiem jednego służącego celom związanym z prezentacjami i wystąpieniami publicznymi oraz dwóch wykorzystywanych na cele kwalifikacji wojskowej, w ramach której oprogramowanie instalowane było przez Wojskowe Centrum Rekrutacji. W opracowanym we wrześniu 2022 r. dokumencie *Ocena ryzyka naruszenia praw i wolności osób fizycznych*[29] szyfrowanie urządzeń przenośnych wskazane było jako środek minimalizujący ryzyko naruszenia atrybutów bezpieczeństwa danych, co szczegółowo opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 342-343, 544)

2.8. Realizując wymóg § 19 ust. 2 pkt 9 rozporządzenia w sprawie KRI z 2024 r. (wcześniej § 20 ust. 2 pkt 9 rozporządzenia w sprawie KRI z 2012 r.) w Starostwie wprowadzono środki organizacyjne, fizyczne i techniczne w celu zabezpieczenia informacji znajdujących się na serwerach. Serwerownia znajdowała się w odrębnym, nieoznakowanym pomieszczeniu, a dostęp do niego został ograniczony. Wprowadzono środki ochrony dostępu oraz ewidencjonowania wejść/wyjść zarówno przez pracowników, jak i osób z zewnątrz.

W pomieszczeniu zastosowano ponadto środki zabezpieczenia przed czynnikami środowiskowymi: dwa klimatyzatory, czujniki dymu, czujniki zalania, zasilacze awaryjne (UPS-y), urządzenia gaśnicze do sprzętu elektronicznego.

(akta kontroli str. 396-412)

2.9. W umowach utrzymania oprogramowania zawierano zapisy dotyczące ochrony danych osobowych. W dwóch z czterech obowiązujących w kontrolowanym okresie, a poddanych badaniu, umowach utrzymania oprogramowania zawarto również zapisy zobowiązujące wykonawcę do zachowania w tajemnicy informacji, do jakich może mieć dostęp w ramach wykonywania umowy, innych niż dane osobowe. Zapisów takich nie zawarto w dwóch kolejnych umowach, co szczegółowo opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 435-486, 558)

2.10. W kontrolowanym okresie w Starostwie obowiązywała procedura dotycząca przekazywania sprzętu poza jednostkę. Zobowiązywała ona do wymontowania lub wyczyszczenia nośników informacji przed przekazaniem sprzętu poza obszar organizacji, a jeśli to niemożliwe - nadzorowanie procesu naprawy[30].

[29] Stanowił on załącznik nr 9 do PBPDO.

[30] Pkt 13.5 i 13.6 i pkt 14.11. Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

W latach 2023-2024 nie wydawano sprzętu poza jednostkę do naprawy lub ponownego użycia. Wszystkie urządzenia serwisowane były przez informatyka Starostwa.

(akta kontroli str. 331-334, 558, 588)

2.11.-2.12. W Starostwie ustanowione zostały również polityki w zakresie kopii zapasowych[31]. Odnosiły się one do backupów pięciu systemów dziedzinowych wykorzystywanych w Starostwie, nie regulując kwestii trzech kolejnych. Procedury nie określały przy tym w stosunku do części systemów niezbędnych zagadnień, takich jak częstotliwość wykonywania czy okres przechowywania kopii. Szczegółowe ustalenia w tym zakresie zawarto w sekcji *Stwierdzone nieprawidłowości*.

Dokument *Ocena ryzyka naruszeń praw i wolności osób fizycznych* przewidywała mechanizm obniżający ryzyko utraty dostępu do informacji oparty na zasadzie 3-2-1-backup. Nie była ona jednak odniesiona do spisanych procedur wykonywania kopii zapasowych, ani przestrzegana w rzeczywistości. Również inne postanowienia procedur w zakresie kopii zapasowych nie były stosowane w praktyce. Szczegółowe ustalenia w tym zakresie zawarto w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 269-270, 328-330, 530-539)

Procedury przewidywały zapisywanie jednej ze sporządzonych kopii na nośnik zewnętrzny i jej przechowywanie w odrębnym pomieszczeniu. Znajdowało się ono poza lokalizacją siedziby Starostwa. W lokalizacji zewnętrznej wprowadzono zabezpieczenia fizyczne, techniczne i organizacyjne ograniczające dostęp do kopii zapasowych, jednak dostęp ten nie był ewidencjonowany.

Nośniki zewnętrzne, na których przechowywano kopie bezpieczeństwa przewożone w lokalizację zewnętrzną nie były szyfrowane mimo deklaracji zawartej w dokumencie *Ocena ryzyka naruszenia praw i wolności osób fizycznych*, co szczegółowo opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 269, 282, 528-529, 556)

Przeprowadzone w toku kontroli badanie odzyskiwania danych z kopii zapasowej dla jednego wybranego systemu zakończyło się pomyślnym odtworzeniem danych.

(akta kontroli str. 540)

2.13. Obowiązujące w kontrolowanym okresie procedury nie przewidywały monitorowania pojemności nośników pamięci serwerów. Oględziny trzech serwerów wykazały, że na jednym z nich przestrzeń dyskowa zajęta była w 25%, na pozostałych dwóch znajdowały się natomiast partycje zajęte w udziale przekraczającym 80%. Szczegółowe ustalenia w tym zakresie zawarto w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 212-337, 524-527)

2.14. W ramach zapewnienia ciągłości działania nie zidentyfikowano kluczowych elementów infrastruktury i usług IT oraz nie zidentyfikowano czasów przywrócenia do działania poszczególnych systemów informacyjnych. Szczegółowe ustalenia zawarto w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 302-306, 586)

Stwierdzone nieprawidłowości

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

[31] Rozdział 11 Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

1. Uprawnienia nadane użytkownikowi jednego z 13 objętych oględzinami urządzeń umożliwiały mu instalację dowolnego oprogramowania i aplikacji, mimo że potrzeba posiadania takich uprawnień nie wynikała z jego obowiązków. Naruszało to § 19 ust. 2 pkt 4 rozporządzenia w sprawie KRI z 2024 r. (wcześniej § 20 ust. 2 pkt 4 rozporządzenia w sprawie KRI z 2012 r.). Było to ponadto niezgodne z pkt 1 *Procedury nadawania uprawnień do przetwarzania danych osobowych w systemach informatycznych w Starostwie Powiatowym w Sępólnie Krajeńskim*, zgodnie z którym nadawanie uprawnień do korzystania z systemu informatycznego odbywa się zgodnie z zasadą wiedzy koniecznej i zasadą minimalnych uprawnień.

   W trakcie kontroli uprawnienia administratora zostały odebrane.

   Starosta wyjaśnił, że pozostawienie użytkownikowi uprawnień administratora wynikało z niedopatrzenia. Wicestarosta dodał, że urządzenie to (laptop) było wykorzystywane sporadycznie i nie stanowiło podstawowego narzędzia pracy pracownika.

   (akta kontroli str. 309, 421, 515-523, 577-581, 596)

2. W jednym z 15 objętych kontrolą przypadków pracownikowi nadano uprawnienia do pracy w systemie informatycznym, mimo że nie było to niezbędne z punktu widzenia jego obowiązków służbowych, tj. wyznaczając mu zadania związane jedynie z udostępnianiem informacji z zasobu, przydzielono mu również uprawnienia do modyfikacji danych. Było to niezgodne z § 19 ust. 2 pkt 4 rozporządzenia w sprawie KRI z 2024 r. (wcześniej § 20 ust. 2 pkt 4 rozporządzenia w sprawie KRI z 2012 r.) oraz pkt 1 *Procedury nadawania uprawnień do przetwarzania danych osobowych w systemach informatycznych w Starostwie Powiatowym w Sępólnie Krajeńskim.*

   Starosta wyjaśnił, że nastąpiło to przez pomyłkę administratora systemu. Wskazał również, że uprawnienia zostały odebrane.

   (str. 309, 564, 590-592, 600-626)

3. W dwóch z trzech badanych przypadków uprawnienia do pracy w systemie informatycznym odebrane zostały pracownikom po upływie odpowiednio 48 i 77 dni od ustania zatrudnienia. Naruszało to § 20 ust. 2 pkt 5 rozporządzenia w sprawie KRI z 2012 r., który nakazywał bezzwłoczną zmianę uprawnień[32].

   Starosta wyjaśnił, że brak natychmiastowego odebrania uprawnień wynikał ze zmian organizacyjnych spowodowanych zmianą na stanowisku Dyrektora Wydziału oraz chwilowymi brakami kadrowymi w tym okresie, skutkującymi nadmiarem prac bieżących.

   (str. 309, 564, 605-618)

4. Procedura zarządzania uprawnieniami do przetwarzania danych osobowych w systemach informatycznych w Starostwie nie była w pełni rzetelna, gdyż:
   - nie regulowała procesu nadawania i cofania uprawnień w sytuacji, gdy administratorem systemu, posiadającym uprawnienia do nadawania i cofania uprawnień był podmiot zewnętrzny. W rezultacie nadawanie i odbieranie uprawnień w wykorzystywanych systemach finansowo-księgowo-płacowych odbywało się na podstawie telefonicznych poleceń, z których nie pozostawał ślad rewizyjny. W ww. sytuacjach nie były również sporządzane przewidziane wewnętrzną procedurą karty uprawnień;
   - nie wskazywała osób odpowiedzialnych za przepływ informacji o konieczności nadania lub odebrania uprawnień, czasu, w jakim zakres

[32] W PBPDO nie zdefiniowano wymogów odnośnie do czasu odebrania uprawnień.

uprawnień powinien zostać zmieniony oraz sposobu udokumentowania tych czynności.

Starosta wyjaśnił, że uwagi dotyczące braku określenia sposobu postępowania dla sytuacji, gdy ASI nie posiada do konkretnych systemów informatycznych uprawnień administratora, od których uzależniona jest możliwość nadawania i odbierania uprawnień zostaną w najbliższym czasie wyeliminowane. Jako przyczynę nieokreślenia w procedurach zarządzania uprawnieniami oczekiwanego czasu odbierania uprawnień w związku z ustaniem zatrudnienia podał przeoczenie.

(str. 309-310, 422, 470, 476, 554-558, 564, 595-596, 627)

5. Hasła stosowane do uwierzytelniania dostępu do systemu dziedzinowego w dwóch z 10 przypadków nie odpowiadały pod względem długości i struktury wymogom określonym w rozdziale 9 *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych*.

   Starosta wyjaśnił, że przyczyną powyższego było nieustawienie w systemie odpowiednich parametrów (konfiguracji zasad dotyczących siły haseł). Dodał, że już w dniu oględzin hasła zostały zmienione, a trzy dni później dostawca oprogramowania wprowadził do systemu parametry zarządzania hasłami.

   Parametry te odpowiadały wymogom PBPDO.

   (akta kontroli str. 327, 421, 518-523)

6. W Starostwie nie ustanowiono podstawowych zasad gwarantujących bezpieczną pracę przy pracy na odległość, co naruszało § 19 ust. 2 pkt 8 rozporządzenia w sprawie KRI z 2024 r. (wcześniej § 20 ust. 2 pkt 8 rozporządzenia w sprawie KRI z 2012 r.)

   Starosta wyjaśnił m.in., że nie ustanowiono i wdrożono zasad, gdyż Starostwo nie ma możliwości sprzętowych – nie zabezpiecza pracownikom bezpiecznego kanału komunikacji z infrastrukturą informatyczną, w związku z powyższym nie jest możliwe systemowe podejście do pracy zdalnej. Dodał, że będzie podejmował indywidualne rozstrzygnięcia dotyczące wyrażenia zgody na pracę zdalną mając na uwadze zakres obowiązków pracownika oraz możliwości zapewnienia bezpiecznego kanału komunikacji oraz infrastruktury niezbędnej do wykonywania zadań.

   (akta kontroli str. 213-337, 341-342)

   W odniesieniu do powyższych wyjaśnień NIK zauważa, że praca zdalna jest równorzędną formą pracy, stąd niezbędne jest ustanowienie zasad jej bezpiecznego wykonywania, również w kontekście tych sporadycznych, indywidualnie rozpatrywanych przypadków. Procedury powinny być natomiast dostosowane do aktualnych realiów wykonywania tej pracy, uwzględniających występujące ograniczenia.

7. W dwóch z czterech obowiązujących w kontrolowanym okresie, a poddanych badaniu umowach utrzymania oprogramowania[33], nie zawarto zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji, do jakich może mieć dostęp w ramach wykonywania umowy, innych niż dane osobowe. Naruszało to § 20 ust. 2 pkt 10 rozporządzenia w sprawie KRI z 2012 r.

   Starosta wyjaśnił, że w ww. umowach nie zawarto zobowiązania do zachowania w tajemnicy danych innych niż dane osobowe, gdyż pracownik merytoryczny nie zgłosił takiej potrzeby dostawcy licencji. Dostawca opracował wzór umowy licencyjnej, który przekazuje wszystkim kontrahentom.

[33] Zawartych odpowiednio 15 i 23 lutego 2024 r.

(akta kontroli str. 435-486, 558)

W odniesieniu do powyższych wyjaśnień NIK zauważa, że Starostwo jako strona umowy na dostawę i utrzymania oprogramowania, ma prawo do kształtowania jej postanowień i żądania ich modyfikacji.

8. W Starostwie nie monitorowano pojemności nośników dla zapewnienia właściwej wydajności systemu, co należy uznać za działanie nierzetelne. Badanie zapełnienia wybranych trzech serwerów wykazało, że w dwóch przypadkach zajętość jednej z wyodrębnionych partycji przekraczała 80%[34].

   Starosta wyjaśnił, że przyczyną nieopracowania procedury monitorowania pojemności pamięci masowych było przeoczenia, a procedury weryfikacji pojemności zapełnienia dysków zostaną opracowane. W odniesieniu do stwierdzonych stanów faktycznych stwierdził, że w pierwszym przypadku twórca oprogramowania nie zgłaszał zastrzeżeń co do zapełnienia partycji. W kwestii drugiego serwera podał natomiast, że zapełnienie wynika z całościowego wykonywania kopii zapasowych, a przy tworzeniu kolejnych kopii najstarsze są usuwane.

   (akta kontroli str. 212-337, 524-527, 549)

9. W Starostwie nie wdrożono działań minimalizujących ryzyko deklarowanych jako wykorzystywane w *Ocenie ryzyka naruszenia praw i wolności osób fizycznych*, co naruszało § 19 ust. 2 pkt 3 rozporządzenia w sprawie KRI z 2024 r., (wcześniej § 20 ust. 2 pkt 3 rozporządzenia w sprawie KRI z 2012 r.). Dotyczyło to:

   - braku szyfrowania dysków, na których dane osobowe przetransportowywane były w inne miejsce, w tym również braku wprowadzenia obowiązku szyfrowania w instrukcji sporządzania kopii zapasowych, tj. rozwiązań wskazanych jako przyjęte w odpowiedzi na ryzyko zgubienia elektronicznych nośników z danymi dla danych zaliczonych do kategorii B i D;
   - braku szyfrowania urządzeń mobilnych służących do przetwarzania danych, tj. rozwiązań wskazanych jako przyjęte w odpowiedzi na ryzyko zgubienia elektronicznych nośników z danymi dla danych zaliczonych do kategorii B i D;
   - sporządzania kopii zapasowych wg metody 3-2-1, tj. rozwiązań wskazanych jako przyjęte w odpowiedzi na ryzyko zniszczenia urządzeń lub nośników elektronicznych dla danych zaliczonych do kategorii B.

   W kwestii braku szyfrowania nośników zewnętrznych, na których przewożone są kopie bezpieczeństwa oraz laptopów Starosta wyjaśnił, że wynika to z uchybień/niedopatrzeń pracowników. Dodał również, że procedury sporządzania kopii zapasowych zostaną przeanalizowane i zaktualizowane. Ustalone zostaną nowe, adekwatne do przepisów i potrzeb zasady sporządzania, przechowywania i testowania kopii zapasowych.

   (akta kontroli str. 269, 282, 548, 556, 587)

10. Kopie zapasowe wykonywano w Starostwie z naruszeniem wymogów wprowadzonych PBPDO. I tak:

    - przechowywana była tylko w dwóch egzemplarzach jedna kopia (z jednego dnia) programu z bazą danych zasobu geodezyjnego i kartograficznego, co naruszało wymogi rozdziału 11 *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania*

[34] Na jednej znajdował się system operacyjny, druga wykorzystywana była do zapisywania kopii zapasowych.

danych osobowych zobowiązującego do cotygodniowego sporządzania kopii oraz przechowywania ich przez miesiąc. Jednocześnie naruszony został § 11 pkt 3 rozporządzenia Ministra Rozwoju, Pracy i Technologii z dnia 2 kwietnia 2021 r. w sprawie organizacji i trybu prowadzenia państwowego zasobu geodezyjnego i kartograficznego[35], nakazujący przechowywanie co najmniej dwóch ostatnich kopii bezpieczeństwa w pomieszczeniach zlokalizowanych poza budynkiem, w którym są przechowywane materiały zasobu;

- nie przegrano na dysk zewnętrzny w 15 przypadkach[36] kopii baz danych z programu, w którym prowadzi się rejestr VAT, w 12 przypadkach[37] kopii z programu, w którym prowadzone są księgi rachunkowe Starostwa, co było wymagane przepisami rozdziału 11 *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.*

Starosta i Wicestarosta wyjaśnili, że uchybienia w zakresie nieprzegrywania kopii na dysk zewnętrzny wynikają z niedopatrzenia pracowników.

(akta kontroli str. 329, 530-539, 547-548, 595)

11. Obowiązujące w kontrolowanym okresie w Starostwie procedury nierzetelnie regulowały kwestie sporządzania kopii zapasowych, gdyż:
    - nie zawierały w odniesieniu do większości programów zapisów dotyczących częstotliwości sporządzania, okresu przechowywania oraz zasad testowania kopii zapasowych, w tym również dokumentowania tych testów[38];
    - nie określały w ogóle zasad sporządzania backupów dla trzech wykorzystywanych w Starostwie programów (EZD, SJOBesti@, systemy wykorzystywane do obsługi placówek oświatowych);
    - przewidywały w odniesieniu do backupów jednego z programów zadania po stronie Starostwa, mimo iż cały proces został przejęty przez administrację rządową, która dostarczała system.

    Za nierzetelne NIK uznała również niesporządzenie przez okres ponad roku[39] chociażby jednej kopii bezpieczeństwa bazy danych z programu, w którym prowadzone były sprawy kadrowo-płacowe Starostwa oraz kopii bazy danych z programu SJOBesti@. NIK zauważa, że należy regularnie wykonywać i testować kopie zapasowe.

    Starosta wyjaśnił, że obowiązujące procedury wymagają aktualizacji i dostosowania do potrzeb jednostki. Dodał, że w ramach program *Cyberbezpieczny Samorząd* Powiat pozyskał środki na opracowanie, wdrożenie, przegląd i aktualizację SZBI.

    Wskazał, że kopii bezpieczeństwa z programu kadrowo-płacowego oraz programu SJOBesti@ nie wykonano z powodu uchybienia pracowników merytorycznych. Dodał, że procedury w tym zakresie zostaną bezzwłocznie przeanalizowane i ustalone zostaną nowe zasady sporządzania, przechowywania i testowania kopii zapasowych.

---

[35] Dz. U. z 2021 r., poz. 820, ze zm.

[36] Kopie z dnia 11.05.2024, 12.05.2024, 04.06.2024, 05.06.2024, 06.06.2024, 09.06.2024, 08.06.2024, 07.06.2024, 10.06.2024, 11.06.2024, 12.06.2024, 13.06.2024, 18.06.2024, 19.06.2024, 24.06.2024

[37] Kopie z dnia 04.06.2024, 05.06.2024, 06.06.2024, 09.06.2024, 08.06.2024, 07.06.2024, 10.06.2024, 11.06.2024, 12.06.2024, 13.06.2024, 18.06.2024, 19.06.2024.

[38] Stosownych zapisów nie zawarto również w polityce rachunkowości Starostwa. W rozdziale 4 tego dokumentu w odniesieniu do kopii zapasowych wprowadzono jedynie obowiązek ich sporządzania, nie określając w sposób definitywny wymogów co do częstotliwości sporządzenia (zdefiniowaną ją jako przykład).

[39] Od 13 czerwca 2023 r. do 23 czerwca 2023 r.

(akta kontroli str. 328-330, 530-539, 544-546, 548, 564, 628-629)

12. W Starostwie nie zidentyfikowano kluczowych elementów infrastruktury i usług IT oraz nie zidentyfikowano czasów przywrócenia do działania poszczególnych

Starosta wyjaśnił, że wynikało to z braku doświadczenia pracowników.

(akta kontroli: 586)

OCENA CZĄSTKOWA

W Starostwie podejmowano działania mające na celu ochronę atrybutów informacji, choć pojawiły się nieprawidłowości w realizacji przyjętych procedur oraz obowiązków nałożonych rozporządzeniem w sprawie KRI. Stwierdzono bowiem niezachowanie zasad dotyczących: ograniczania pracownikom niebędącym pracownikami IT uprawnień uprzywilejowanych, blokowania możliwości stosowania słabych haseł, wykonywania kopii zapasowych baz danych z systemów czy bezzwłocznego odbierania uprawnień do pracy w systemach informatycznych. Nie ustanowiono ponadto zasad bezpiecznej pracy przy pracy na odległość oraz nie wdrożono części rozwiązań zadeklarowanych jako stosowane w ocenie ryzyka. Wprowadzono natomiast środki organizacyjne, fizyczne i techniczne w celu zabezpieczenia informacji znajdujących się na serwerach.

OBSZAR

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

3.1. Wynikający z § 19 ust. 2 pkt 3 rozporządzenia w sprawie KRI z 2024 r. oraz § 20 ust. 2 pkt 3 rozporządzenia w sprawie KRI z 2012 r. obowiązek prowadzenia okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji zrealizowano w Starostwie potwierdzając w lutym 2024 r. aktualność ryzyk określonych w opracowanym we wrześniu 2022 r. dokumencie *Ocena ryzyka naruszenia praw i wolności osób fizycznych.* W dokumencie tym pogrupowano informacje będące danymi osobowymi ze względu na znaczenie i formę przechowywania, a następnie w odniesieniu do każdej z grup: [1] zidentyfikowano ryzyka utraty atrybutów bezpieczeństwa informacji, [2] ustalono poziom ryzyka pierwotnego, [3] opisano zastosowane zabezpieczenia obniżające poziom ryzyka oraz ustalono poziom ryzyka po zastosowaniu zabezpieczeń. Przyjęto ponadto plan postępowania z ryzykiem.

(akta kontroli str. 249-299)

3.2. W kontrolowanym okresie w Starostwie ustanowione zostały zasady zarządzania incydentami związanymi z bezpieczeństwem informacji, w szczególności w systemach informacyjnych. Kwestie te regulowały: *Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem* oraz *Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych*, stanowiące odpowiednio załączniki nr 18 i 4 PBPDO. Tym samym wypełniony został obowiązek wynikający z art. 22 ust.1 pkt 1 ustawy o KSC w związku z § 19 ust. 2 pkt 13 rozporządzenia w sprawie KRI z 2012 r. (wcześniej § 20 ust. 2 pkt 13 rozporządzenia w sprawie KRI z 2012 r.)

(akta kontroli str. 234-237, 311-319)

W okresie objętym kontrolą w prowadzonym przez ASI rejestrze incydentów naruszenia bezpieczeństwa informacji odnotowano jeden przypadek. Dotyczył on próby pozyskania w 2024 r. poufnych informacji na zapytanie wysłane z konta email podszywającego się pod Starostę. Zdarzenie zostało zgłoszone do CSIRT NASK[40] z zachowaniem terminu wynikającego z art. 22 ust. 1 pkt 2 ustawy o KSC.

[40] Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy wyznaczony do

(akta kontroli str. 418-431)

3.3. W kontrolowanym okresie pracownicy Starostwa uczestniczyli w siedmiu szkoleniach z zakresu bezpieczeństwa informacji. Ich tematyka dotyczyła: cyberzagrożeń i sposobów ochrony przed tymi zagrożeniami, Krajowych Ram Interoperacyjności, ciągłości działania. Łącznie objęto nimi 14 spośród 51 (27%) pracowników Starostwa uczestniczących w procesie przetwarzania informacji. Szczegółowy opis w tym zakresie zawarto w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 17-19, 565-576)

3.4. W 2023 r. okresowy audyt bezpieczeństwa informacji przeprowadzony został w Starostwie przez dwuosobowy zespół, w skład którego weszli ASI i IOD. Audyt ten nie miał przymiotu niezależności, co szczegółowo opisano w sekcji *Stwierdzone nieprawidłowości*. Audyt wykazał trzy słabości, nie wydano jednak zaleceń w celu ich poprawy.

(akta kontroli str.107-111)

Stwierdzone nieprawidłowości

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

1. W 2023 r. okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji przeprowadzony został przez pracowników odpowiadających za przedmiot audytu, co pozbawiło go przymiotu niezależności i obiektywizmu. Tym samym nierzetelnie zrealizowano wymóg określony § 20 ust. 2 pkt 14 rozporządzenia w sprawie KRI z 2012 r.[41]

   Starosta wyjaśnił, że planowano przeprowadzić w grudniu 2023 r. niezależny audyt wewnętrzny z zakresu bezpieczeństwa informacji. Ze względu na ograniczone możliwości finansowe zadanie zamierzano zrealizować ze środków zewnętrznych w ramach programu *Cyberbezpieczny Samorząd*. Wniosek aplikacyjny Powiatu został oceniony pozytywnie dopiero 1 lutego 2024 r.

   (akta kontroli str.19-20, 107-111, 342)

2. W Starostwie jedynie w niewielkim zakresie zorganizowano szkolenia osób zaangażowanych w proces przetwarzania informacji, czym naruszono § 20 ust. 2 pkt 6 rozporządzenia w sprawie KRI z 2012 r. oraz § 19 ust. 2 pkt 6 rozporządzenia w sprawie KRI z 2024 r. W roku 2023 w szkoleniach tych uczestniczyły dwie, a w okresie od stycznia do maja 2024 r. – 14 spośród odpowiednio 53 i 51 osób zaangażowanych w proces przetwarzania informacji.

   Starosta wyjaśnił, że pracownicy Starostwa mają dostęp do systemu informacji prawnej, w tym do bezpłatnych szkoleń i webinariów, także z zakresu cyberbezpieczeństwa. Starostwo jest ponadto członkiem *Klubu Bezpieczny Samorząd z EXATEL*. W ramach klubu dostępne są poradniki dotyczące cyberbezpieczeństwa. Pracownicy mogą na bieżąco zapoznać się z treściami publikowanymi przez Narodowy Instytut Cyberbezpieczeństwa. Podał również, że w związku z przystąpieniem do programu Cyberbezpieczny Samorząd w najbliższym czasie wszyscy pracownicy Starostwa wezmą udział w szkoleniach. Zaplanowano ponadto szkolenia specjalistyczne dla pracowników IT.

   (akta kontroli str.17-19, 565-576)

koordynowania obsługi incydentów zgłaszanych przez jednostki sektora finansów publicznych na podstawie art. 26 ust. 6 ustawy o KSC.

[41] Por. Wspólne stanowisko Departamentu Informatyzacji MAiC i Departamentu Audytu Sektora Finansów Publicznych MF odnośnie zapewnienia audytu wewnętrznego w zakresie bezpieczeństwa informacji Audyt bezpieczeństwa informacji - Metodyka - Audyt wewnętrzny w sektorze publicznym - Ministerstwo Finansów (mf.gov.pl) dostęp 17.06.2024 r.

OCENA CZĄSTKOWA

W Starostwie cyklicznie podejmowane były działania w celu zapobiegania incydentom bezpieczeństwa informacji. W szczególności prowadzone były analizy ryzyka utraty atrybutów bezpieczeństwa informacji, audyty wewnętrzne w zakresie bezpieczeństwa informacji, szkolenia pracowników. Część z tych działań zrealizowano jednak w sposób nieodpowiadający wymogom rozporządzenia w sprawie KRI z 2012 r. Szkoleniami objęto bowiem niewielki odsetek pracowników zaangażowanych w proces przetwarzania informacji, a audyt pozbawiono cechy niezależności. Ponadto w analizie ryzyka utraty atrybutów bezpieczeństwa uwzględniano przy ocenie ryzyka rozwiązania mające za zadanie obniżenie poziomu zagrożenia, które nie były stosowane w jednostce.

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 nie formułuje uwag.

Wnioski

1. Przeanalizowanie i uzupełnienie dokumentacji dotyczącej bezpieczeństwa informacji, w szczególności o procedurę zapewnienia bezpiecznej pracy przy przetwarzaniu mobilnym i na odległość.
2. Zapewnienie stosowania środków zadeklarowanych jako wykorzystywane do obniżenia ryzyka w dokumencie *Ocena ryzyka naruszenia i praw i wolności osób fizycznych*.
3. Zapewnienie przestrzegania procedur wewnętrznych w zakresie wykonywania i przechowywania kopii zapasowych, uwierzytelniania i ograniczania dostępu do danych.
4. Zawieranie w umowach z dostawcami oprogramowania klauzul zapewniających bezpieczeństwo danych również spoza katalogu danych osobowych.
5. Zwiększenie udziału pracowników w szkoleniach z zakresu cyberbezpieczeństwa.
6. Zapewnienie niezależnych audytów bezpieczeństwa informacji.
7. Podjęcie działań w celu obniżenia i utrzymania zajęcia poszczególnych partycji dysków twardych do poziomów bezpiecznych z punktu widzenia wydajności systemu (poniżej 80%).
8. Weryfikacja kompletności wykazu licencji na wykorzystywane w Starostwie oprogramowanie.

V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Delegatury w Bydgoszczy. 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 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.

Bydgoszcz, 22 sierpnia 2024 r.

Dyrektor
Najwyższa Izba Kontroli
Delegatura w Bydgoszczy

Kontroler
(-) Karolina Lahutta
gł. specjalista k.p.

(-) z up. Adam Kończak
p.o. Wicedyrektor