NAJWYŻSZA IZBA KONTROLI
DELEGATURA W BYDGOSZCZY

LBY.410.12.3.2024

Michał Grabski
Wójt Gminy Osie

Urząd Gminy w Osiu
Ul. Dworcowa 6
86-150 Osie

WYSTĄPIENIE POKONTROLNE

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

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Gminy w Osiu[1], ul. Dworcowa 6, 86-150 Osie
Kierownik jednostki kontrolowanej	Michał Grabski , Wójt Gminy Osie[2], od 1 maja 1995 r.
Zakres przedmiotowy kontroli	Rozwiązanie organizacyjne i techniczne w zakresie zapewnienia bezpieczeństwa przetwarzania informacji oraz zapewnienia ciągłości działania w urzędzie i ich stosowanie
Okres objęty kontrolą	Od 1 stycznia 2023 r. do dnia zakończenia kontroli w 2024 r.[3] (także okresy wcześniejsze w zakresie uczestnictwa w programie Cyfrowa Gmina).
Podstawa prawna podjęcia kontroli	art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[4]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Bydgoszczy
Kontroler	Adam Ruciński, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LBY/89/2024 z 23 maja 2024 r.

(akta kontroli str. 1-3)

II. Ocena ogólna[5] kontrolowanej działalności

OCENA OGÓLNA

W okresie objętym kontrolą Urząd podejmował działania na rzecz zapewnienia bezpieczeństwa informacji, w tym danych osobowych, systemów teleinformatycznych oraz ciągłości działania.

Jednostka zidentyfikowała zbiory zawierające dane osobowe oraz wskazała programy zastosowane do ich przetwarzania. Przygotowano ponadto kluczowe regulacje wewnętrzne tworzące systemu zarządzania bezpieczeństwem informacji w jednostce. Nie prowadzono jednak, poza *Polityką bezpieczeństwa danych osobowych*[6], przeglądu oraz aktualizacji przyjętych procedur i regulaminów. W Urzędzie wyznaczono osoby odpowiedzialne za bezpieczeństwo informacji, w tym *Inspektora Ochrony Danych*[7], któremu zapewniono niezależność. *IOD*, od 28 lutego 2023 r., miał także możliwość działania bez ryzyka wystąpienia konfliktu interesów. NIK ocenia negatywnie brak zapewnienia przez Urząd takiej możliwości przed ww. terminem.

Jednostka wykonywała także działania mające na celu ochronę zasobów informacyjnych. Zidentyfikowano jednak nieprawidłowości w realizacji przyjętych procedur i obowiązków, w tym naruszających regulacje rozporządzenia Rady

[1] Dalej: „Urząd" lub „jednostka".
[2] Dalej: „Wójt" lub „kierownik jednostki".
[3] Czynności kontrolne zakończono 13 września 2024 r.
[4] Dz. U. z 2022 r. poz. 623, dalej: ustawa o NIK.
[5] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[6] Dalej; „*PBDO*".
[7] Dalej: „*IOD*".

Ministrów z dnia 21 maja 2024 r.[8] oraz poprzedzającego go rozporządzenia Rady Ministrów z 12 kwietnia 2012 r[9], co zdaniem NIK należy oceniać negatywnie. Stwierdzono bowiem m.in. niezachowanie zasad dotyczących możliwości instalowania nieautoryzowanego oprogramowania, tworzenia i weryfikacji haseł, szyfrowania laptopów, przygotowania serwerowni oraz tworzenia, przechowywania i testowania kopii zapasowych, a także monitowania pojemności nośników pamięci serwerów.

W jednostce podejmowano kroki w celu zapobiegania incydentom bezpieczeństwa informacji, szczególnie w zakresie analizy ryzyka utraty atrybutów bezpieczeństwa. W 2023 r. nie przeprowadzono jednak audytu bezpieczeństwa informacji, a proces ewidencji incydentów związanych z bezpieczeństwem informacji był prowadzony w sposób nierzetelny.

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

OBSZAR

1. Organizacja bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych

Opis stanu faktycznego

1.1. Urząd zidentyfikował wyłącznie zbiory zawierające dane osobowe oraz wskazał programy zastosowane do przetwarzania tych danych w treści *PBDO*[11], o czym szerzej w sekcji *Stwierdzone nieprawidłowości.*
Wójt podał, że poszczególnych zbiorów nie kategoryzowano ze względu na znaczenie, ponieważ w *Polityce Bezpieczeństwa Informacji*[12] dokonano klasyfikacji czynności przetwarzania[13]. Dzięki temu w każdym zbiorze można było zdefiniować po kilka czynności przetwarzania. Ww. wskazał ponadto, że z tego też powodu poszczególnym zbiorom nie przypisywano, zgodnego z ich wagą, odpowiedniego poziomu ochrony.

(akta kontroli str. 251-255, 337-341)

1.2. W dniu 29 listopada 2022 r., zgodnie z § 20 ust. 1 w zw. z ust. 3 KRI z 2012 r., w Urzędzie wprowadzono pakiet regulacji wewnętrznych, które składały się na system zarządzania bezpieczeństwa informacji[14] obowiązujący w jednostce. *SBI* obejmowało:

1) Politykę bezpieczeństwa Informacji wraz z *Procedurą zarządzania ryzykiem bezpieczeństwa informacji*[15], *Planem ciągłości działania*[16] oraz

[8] 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 2024 r., poz. 773, dalej: „*KRI z 2024 r.*"
[9] Rozporządzenia z dnia 12 kwietnia 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, obowiązujące do 22 maja 2024 r., Dz.U. z 2017 r., poz. 2247, dalej: „*KRI z 2012 r.*"
[10] Oceny cząstkowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena cząstkowa może być sformułowana jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej.
[11] Załącznik nr 3 do Zarządzenia nr 2/2022 Wójta Gminy Osie z dnia 29 listopada 2022 r. w sprawie wdrożenia dokumentacji systemu zarządzania bezpieczeństwem informacji w Urzędzie Gminy Osie, dalej: „*SBI*".
[12] Dalej: „PBI".
[13] zgodnie z Komunikatem Prezesa Urzędu Ochrony Danych Osobowych z 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony[13] oraz wytycznych Grupy roboczej art. 29 WP 248 rew. 01 17/PL.
[14] dalej: „*SBI*".
[15] Dalej: „*PZBI*".
[16] Dalej: „*PCD*".

regulaminami: *Nadzoru nad bezpieczeństwem informacji, Pracy zdalnej*[17] *i Zarządzania incydentami w zakresie bezpieczeństwa informacji*[18].

2) *Politykę Bezpieczeństwa Teleinformatycznego*[19] z załączonymi regulaminami: *Ochrony haseł administracyjnych, Testów bezpieczeństwa*[20]*, Użytkownika informacji*[21]*, Wymagań serwerowni*[22]*, Wymagań systemowych, Zarządzania kopiami zapasowymi*[23] oraz *Nadawania, modyfikowania, odbierania i przeglądania uprawnień do systemów*[24].

3) *PBDO*.

Wszystkie ww. dokumenty zostały zatwierdzone przez Wójta, a następnie przekazane do wiadomości pracownikom zaangażowanym w proces przetwarzania informacji[25].

(akta kontroli str. 76-336, 351-353, 886)

Zastępca Wójta odpowiadał za nadzorowanie bezpieczeństwa informacji[26] w jednostce. Referatowi organizacyjnemu[27] przypisano odpowiedzialność za zadania w obszarze informatyki i cyberbezpieczeństwa. Ponadto zobowiązano kierowników poszczególnych komórek organizacyjnych do prowadzenia i aktualizacji baz danych (wg kompetencji merytorycznych)[28] oraz do przeglądu dokumentacji dotyczącej systemu zarządzania bezpieczeństwem informacji[29].

(akta kontroli str. 4-336, 798)

1.3. Podstawową regulacją wewnętrzną w zakresie ochrony danych osobowych w Urzędzie była, przyjęta w listopadzie 2022 r., *PBDO*[30]. Uzupełniał ją: wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar na którym przetwarzane są dane osobowe, wykaz zbiorów danych osobowych, opis struktury zbiorów danych oraz rejestr czynności przetwarzania[31]. Do dokumentacji dołączone również zostały wzory upoważnień nadawanych przez *Administratora Danych* oraz oświadczeń o zachowaniu tajemnicy danych osobowych[32]. Ponadto załączono ewidencję osób przetwarzających dane, Rejestr kategorii czynności przetwarzania, wzór umowy powierzenia przetwarzania danych osobowych oraz Instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych[33]

(akta kontroli str. 236-335)

---

[17] Dalej: „*RPZ*"
[18] Dalej: „RZI"
[19] Załącznik nr 2 do *SBI*, dalej: „*PBT*".
[20] Dalej: „*RTB*".
[21] Dalej: „*RUI*".
[22] Dalej: „*RWS*"
[23] Dalej: „*RZKZ*"
[24] Dalej: „*RNU*"
[25] W 2022 r. zapoznanie się z ww. dokumentami potwierdziło 18 pracowników, w 2023 r. - dwoje nowo zatrudnionych. Jedna osoba - w okresie od przyjęcia procedur do ustania jej zatrudnienia (7 lutego 2023 r.) - pozostawała na urlopie macierzyńskim.
[26] Zgodnie z § 8 ust. 2 PBI.
[27] Zgodnie z § 19 Zarządzenia nr 2/18 Wójta Gminy Osie z dnia 12 grudnia 2018 r. w sprawie nadania regulaminu organizacyjnego Urzędu Gminy Osie (ze zm.), a następnie Zarządzenia nr 345/23 Wójta Gminy Osie z dnia 16 lutego 2023 r. w sprawie nadania regulaminu organizacyjnego Urzędu Gminy Osie (ze zm.), dalej; „*Regulamin organizacyjny*".
[27] Określała zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
[28] § 13 pkt 4 ww. *Regulaminu organizacyjnego*.
[29] § 10 Regulaminu nadzoru nad bezpieczeństwem Informacji, dalej: „*RNBI*".
[30] Określała zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
[31] Załączniki nr 1 - 4 *PBDO*.
[32] Załącznik nr 5 - 6 *PBDO*.
[33] Załącznik nr 7 -10 *PBDO*.

Wprowadzone procedury stanowiły realizację obowiązków określonych w art. 30 oraz art. 35 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)[34] oraz były elementem realizacji wymogów wynikających z art. 29, 32 i 33 *RODO*.

(akta kontroli str. 236 - 383)

1.4. W latach 2023-2024[35] w Urzędzie nie były prowadzone analizy ryzyka w związku z potrzebą zachowania ciągłości działania systemów informatycznych.

Wójt podał, że w 2022 r. w ramach projektu Cyfrowa Gmina, opracowano raport cyberbezpieczeństwa. W ramach realizacji ww. zadania dokonano analizy zgodności bezpieczeństwa informacji w Gminie Osie w zakresie wymaganym przez *KRI z 2012 r.* Badaniu poddano funkcjonujące zasady i procedury dotyczące zarządzania bezpieczeństwem informacji, w tym przetwarzania danych osobowych. Między innymi przeprowadzono testy bezpieczeństwa infrastruktury informatycznej oraz opracowano dokumentację zarządzania bezpieczeństwem informacji. Urząd przyjął, że wykonawca zadania wykonał je ze starannością przyjętą w obrocie profesjonalnym oraz aktualną wiedzą i kwalifikacjami.

(akta kontroli str. 337-342, 384, 466-540)

1.5. W badanym okresie Urząd nie ustanowił polityk ciągłości działania. Wójt wyjaśnił, że w procesie tworzenia systemu zarządzania bezpieczeństwem informacji nie wdrożono ww. polityk, ponieważ nie było to obowiązkowe.

(akta kontroli str. 337-342, 384)

1.6.-1.7. W Urzędzie opracowano plan postępowania w sytuacji wystąpienia ryzyk mogących zakłócić ciągłość działania w przypadku: a) zaniku dostawy prądu, b) braku dostępności usług internetowych, c) utraty dostępu do zasobów programowych, d) rozległego uszkodzenia infrastruktury. Określono ponadto procedurę zgłaszania awarii oraz czas reakcji[36]w zależności o rodzaju i kategorii infrastruktury.

Wójt wyjaśnił m.in., że w *Planie ciągłości działania*[37] ograniczono się do wybranych zdarzeń ponieważ założono, że prawdopodobieństwo wystąpienia innych zagrożeń było niewielkie. Nie określono akceptowalnego czasu przywracania ciągłości działania systemów informatycznych, a opracowane *PCD* nie były testowane, o czym szerzej w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 150-155, 337- 343, 385-386, 337-342)

1.8. W badanym okresie[38] Urząd objął procesem aktualizacji regulacji wewnętrznych wyłącznie załączniki do *PBDO*, tj. ewidencję upoważnień, rejestr czynności przetwarzania, wykaz zbioru danych oraz opis struktury zbioru danych[39]. Przeglądowi i aktualizacji w zakresie zmieniającego się otoczenia nie podlegały pozostałe polityki i regulaminy wchodzące w skład ww. systemu, o czym szerzej w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 345-350, 387)

[34] Dz. Urz. UE.L2016 Nr 119, poz. 1, ze sprostowaniami. Dalej: „*RODO*".
[35] Stan na 28 sierpnia 2024 r.
[36] Awaria krytyczna- natychmiast, awaria zwykła – bez zbędnej zwłoki, awaria jednostkowa – w kolejności.
[37] Dalej: „*PCD*".
[38] Stan na 29 lipca 2024 r.
[39] W okresie od 2 stycznia 2023 r. do 19 lipca 2024 r. wykonano łącznie 10 aktualizacji .

1.9. Obowiązki i odpowiedzialność z tytułu wdrażania rozwiązań w zakresie zapewnienia bezpieczeństwa informacji oraz zapewnienia ciągłości działania, w kontrolowanym okresie, przydzielono *Administratorowi Systemów Informatycznych* oraz *Administratorowi Systemu Teleinformatycznego*[40]. W zakresie obowiązków ASI zdefiniowano zadania związane m.in. z nadzorem nad stosowaniem polityk ochrony danych osobowych w zakresie bezpieczeństwa teleinformatycznego, kontroli przestrzegania przez pracowników procedur bezpieczeństwa systemów informatycznych oraz ochrony informacji przetwarzanej i przechowywanej na serwerach, komputerach stacjonarnych i przenośnych. Ponadto jego obowiązkiem było także nadzorowanie wykonywania kopii awaryjnych, procesu ich przechowywania oraz okresowego sprawdzania, a także monitorowania napraw, konserwacji oraz likwidacji urządzeń komputerowych, na których zapisane są dane osobowe i inne informacje chronione i sprawdzanie systemu pod kątem obecności wirusów, szkodliwego lub nielegalnego oprogramowania.

Do zadań AST należało m.in. sprawdzanie poprawności działania systemów, wdrażanie procedur bezpieczeństwa oraz nadzór nad funkcjonowaniem systemu teleinformatycznego. Ww. osoba miała również opracowywać plany napraw, informować o stwierdzonych naruszeniach bezpieczeństwa oraz wykrytych wirusach oraz proponować zmiany poprawiające bezpieczeństwo systemu teleinformatycznego.

Osoba wyznaczona do realizacji ww. zadań posiadała wykształcenie kierunkowe informatyczne[41] oraz uczestniczyła w szkoleniach z zakresu cyberbezpieczeństwa i ochrony danych osobowych.

(akta kontroli str. 49-58, 388, 774)

1.10. Stosownie do art. 8 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[42] w zw. z art. 37 ust. 1 lit a RODO w Urzędzie wyznaczony[43] został *IOD*. Do 27 lutego 2023 r. ww. obowiązki pełniła etatowa pracownik Urzędu, której obok funkcji *IOD* powierzono także zadania na stanowisku Zastępcy Wójta i podinspektora ds. działalności gospodarczej i rozwoju gminy, o czym szerzej w sekcji *Stwierdzone nieprawidłowości*. Ww. osoba w 2018 r. skończyła Studia Podyplomowe Ochrony Danych Osobowych w Praktyce oraz odbyła szkolenia w zakresie ochrony danych osobowych. Od 28 lutego 2023 r. funkcję *IOD*, na podstawie umów cywilnych[44], wykonywała osoba spoza Urzędu. Ww. posiadała również odpowiednie przygotowanie zawodowe. Ukończyła w 2018 r. dwusemestralne studia podyplomowe[45] oraz wykonywała zadania *IOD* w jednej ze szkół podstawowych na terenie Osia.

(akta kontroli str. 71-73, 771, 778-779, 812, 822-871)

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

(akta kontroli str. 382-383, 873-884)

---

[40] Wójt pismem z 1 sierpnia 2019 r. wyznaczył Administratora Systemów Informatycznych (dalej: „*ASI*"), a wyznaczenie Administratora Systemu Teleinformatycznego (dalej: „*AST*") nastąpiło 14 grudnia 2021 r. na podstawie Zarządzenia nr 232/21 w sprawie wyznaczenia osób funkcyjnych odpowiedzialnych za weryfikacje i bieżącą kontrolę zgodności funkcjonowania Systemu Teleinformatycznego. Obowiązki ASI i AST wykonywał pracownik zatrudniony na stanowisku inspektora ds. informatyki i promocji, dalej: „Informatyk".

[41] Specjalność – sieci komputerowe.

[42] Dz. U. z 2019 r., poz. 1781. Dalej: „ustawa o ochronie danych osobowych".

[43] Powierzenie obowiązków *IOD* nastąpiło pismem Wójta z 3 stycznia 2022 r.

[44] Zawartych 27 lutego 2023 r. i 26 czerwca 2024 r..

[45] Ochrona Danych Osobowych w Praktyce.

1.11. W strukturze organizacyjnej Urzędu osoba wykonująca zadania Inspektora została przyporządkowana bezpośrednio Wójtowi. Zadania *IOD* zostały wskazane w § 25 Regulaminu organizacyjnego oraz w zakresie obowiązków pracownika. Ww. obowiązki, zgodnie z art. 39 ust. 1 oraz art. 38 ust. 4 RODO zostały również powtórzone w treści umowy z 27 lutego 2023 r. na wykonywanie obowiązków *IOD*. Od 28 lutego 2023 r. *IOD* wykonywał obowiązki, w sposób, który nie powodował konfliktu interesów, o czym szerzej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 22, 44, 87, 71-73, 820-871, 932-933)

1.12. W kontrolowanym okresie, zgodnie z art. 21 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[46], Urząd wyznaczył osobę odpowiedzialną za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa[47]. Do zadań ww. osoby należało zgłaszanie incydentów występujących w Urzędzie. Wójt nie skorzystał natomiast z możliwości przewidzianej art. 21 ust. 2 i 3 ustawy KSC w zakresie wyznaczenia jednej osoby dla wszystkich jednostek organizacyjnych Gminy Osie oraz jednostek podległych lub nadzorowanych przez jego organy. Wójt wyjaśnił m.in., że w jego opinii było bardziej uzasadnione, aby każda jednostka wyznaczyła swojego pracownika, co w sytuacji zagrożenia pozwalała na szybszą reakcję. Do 31 sierpnia 2024 r. żaden z ww. podmiotów nie dokonał jednak takiego zgłoszenia, o czym szerzej w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 74-75, 392-393, 821-823, 885, 888)

1.13. Wprowadzona w Urzędzie *PBI* nie zawierała zapisów odnośnie konieczności sporządzenia dodatkowych dokumentów wykonawczych. Wszystkie dokumenty, do których się odwoływała stanowiły załączniki do dokumentu głównego.

(akta kontroli str. 78-187)

1.14. W kontrolowanym okresie Urząd nie dysponował pełnymi informacjami o zasobach informatycznych obejmujących ich rodzaj i konfigurację. Podstawowym dokumentem opisującym historię użytkowania sprzętu informatycznego były karty wyposażenia, które m.in. zawierały nazwę urządzenia, numer inwentarzowy oraz jego ogólną charakterystykę[48]. Oględziny 15 jednostek sprzętu[49] wykazały, że pięć komputerów zostało objętych elektroniczną inwentaryzacją sprzętu i oprogramowania w specjalistycznym oprogramowaniu, o czym szerzej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 338,343, 398-465, 598-612)

1.15. Gmina przystąpiła do programu *Cyberbezpieczny Samorząd*. Umowę o powierzeniu grantu podpisano 24 kwietnia 2024 r. Zakładała ona wydatkowanie w terminie 24 miesięcy[50] kwoty 479,7 tys. zł (udział własny – 38,3 tys. zł) na zwiększenie poziomu cyberbezpieczeństwa w Urzędzie i Gminnym Ośrodku Pomocy Społecznej w Osiu[51].

Na zwiększenie poziomu cyberbezpieczństwa w obszarze organizacyjnym obu jednostek (Zadanie nr 1) przewidziano 92,9 tys. zł . Za tę kwotę planowano dokonanie kompleksowego przeglądu i aktualizacji dokumentacji systemu zarządzania bezpieczeństwem informacji oraz zlecenie usługi inżyniera projektu.

---

[46] Dz. U. z 2024 r., poz. 1077. Dalej: „ustawa KSC".

[47] Wyznaczenie osoby za utrzymanie kontaktów - 26 stycznia 2021 r., zgłoszenie osoby kontaktowej do CSIRT NASK -28 stycznia 2021 r.

[48] Do inwentaryzacji składników majątkowych w jednostce wykorzystywano program RADIX STW+3.31.580.

[49] 10 komputerów, dwóch laptopów, routera, serwera i drukarki

[50] Nie później niż do 30 czerwca 2026 r.

[51] Dalej: „GOPS".

Zwiększenie poziomu cyberbezpieczeństwa w obszarze technologicznym Urzędu (Zadanie nr 2) miało kosztować 360,7 tys. zł. Zakładano m.in.: a) wdrożenie pełnego systemu kopii zapasowych, modernizacji infrastruktury do backupu oraz sporządzenie dokumentacji odtworzeniowej, b) modernizację sieci LAN, c) wdrożenie Fortigate wraz z VPN, d) wdrożenie ESET z modułem XDR oraz zewnętrzną usługę Security Office, e) wdrożenie DLP oraz konfigurację polityk bezpieczeństwa, f) zakup i konfigurację Agregatu i UPS, g) wdrożenie i konfigurację Zabbix.
W planach przyjęto także zwiększenie poziomu cyberbezpieczeństwa w obszarze kompetencyjnym Urzędu (Zadanie nr 3) poprzez przeszkolenie pracowników z zakresu cyberbezpieczeństwa wraz z testami phishingowymi oraz szkolenia dla administratora.
Efekty projektu miały zostać ocenione przy użyciu mierników w zakresie i wymiarze zadeklarowanym dla poszczególnych zadań we wniosku o przyznanie grantu.

(akta kontroli str. 466-596)

Stwierdzone nieprawidłowości

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

1. W procedurze zarządzania bezpieczeństwem informacji identyfikację informacji wymagających ochrony ograniczono do zbiorów zawierających dane osobowe, co było niezgodne z § 19 ust. 2 pkt 9 *KRI z 2024 r.* (uprzednio § 20 ust. 2 pkt 9 *KRI z 2012 r.*), który zobowiązywał jednostkę do zabezpieczenia wszystkich posiadanych informacji.

   Wójt podał m.in., że nastąpiło to przez nieuwagę.

   (akta kontroli str. 76-336, 820-823)

2. *PCD*, stosowany w Urzędzie w badanym okresie, został sporządzony nierzetelnie, gdyż nie określał akceptowalnego czasu przywrócenia ciągłości działania systemów informatycznych. Ponadto nie był testowany, co również należy uznać za działanie nierzetelne. Na skutek ww. zaniechań Urząd nie znał faktycznego czasu potrzebnego do ponownego uruchomienia systemów informatycznych niezbędnych do prawidłowego funkcjonowania jednostki. Nie posiadał również wiedzy, czy w sytuacji wystąpienia incydentu procedury *PCD* zadziałają prawidłowo.

   Wójt wyjaśnił, że nieokreślenie akceptowalnego czasu przywrócenia ciągłości działania systemów informatycznych nastąpiło przez nieuwagę. Ponadto podał, że nieprowadzenie testów wynikało z natłoku obowiązków informatyka.

   (akta kontroli str. 150-155, 385-386, 337-342, 801,807,926, 929)

3. W latach 2023-2024[52] Urząd nie dokonywał aktualizacji i przeglądu regulacji wchodzących w skład *SBI* (z wyłączeniem *PBDO*) pomimo, że § 19 ust. 2 pkt 1 *KRI z 2024 r.*(uprzednio § 20 ust. 2 pkt 1 *KRI z 2012 r.*) zobowiązywał jednostkę do zapewnienia aktualizacji regulacji wewnętrznych w zakresie zmieniającego się otoczenia.

   Wójt podał, że całość dokumentacji miała zostać zaktualizowana w zapowiadanym do realizacji w 2023 r. programie *Cyberbezpieczny Samorząd*. Na skutek jego opóźnienia Urząd nie wykonał tego zadania w zakładanym terminie i planował jego przeprowadzenie w czwartym kwartale 2024 r.

   NIK zwraca uwagę, że z powodu pojawiających się cyberzagrożeń oraz kolejnych zmian technologicznych niezbędny jest stały przegląd i aktualizacja przyjętych procedur, gdyż ewentualne zaniechania mogą wpływać na

[52] Stan na 29 lipca 2024 r.

gwarantowany przez Urząd poziom poufności, dostępności oraz integralności gromadzonych informacji.

(akta kontroli str. 76- 336, 345-350, 387, 886)

4. Do 27 lutego 2023 r. obowiązki *IOD* wykonywała osoba pełniąca funkcję Zastępcy Wójta, co było niezgodne z art. 38 ust. 6 *RODO*, który zobowiązywał Urząd do niepowierzenia *IOD* zadań i obowiązków powodujących konflikt interesów.

   Wójt podał m.in., że ww. artykuł pozwalał *IOD* powierzyć inne obowiązki, które nie powodowały konfliktu interesów. Wskazał również, że *IOD* wykonywał swoje zadania od maja 2018 r. Przed powołaniem *IOD* na stanowisko Zastępcy Wójta, Urząd analizował konsekwencje takiego działania. Zwrócił także uwagę, że upoważnienie wydane Zastępcy Wójta dawało jedynie możliwość kierowania Urzędem pod nieobecność Wójta i Sekretarza Gminy. Ponadto ww. osoba nie została upoważniona do przetwarzania danych osobowych w imieniu administratora. Wójt poinformował ponadto, że nie wystąpiła przesłanka wynikająca z art. 28g ust. 1 ustawy z 8 marca 1990 r. o samorządzie gminnym[53] albo art. 15zzz ustawy z 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych[54], która powodowałaby przejęcie kompetencji Wójta.

   NIK zwraca jednak uwagę, że sytuacja *IOD* w Urzędzie uległa zmianie z chwilą wydania (w listopadzie 2022 r.) *SBI*. Zgodnie bowiem z § 8 ust. 2 *PBI* Zastępca Wójta odpowiadała za nadzorowanie bezpieczeństwa informacji w Urzędzie. Tym samym do jej obowiązków należało także nadzorowanie procesu określania celów i sposobów przetwarzania danych osobowych, ponieważ były one elementem przyjętego w Urzędzie *SBI*.

   (akta kontroli: 22, 44, 87, 71-73, 820-871)

5. Wójt, w ramach sprawowanego nadzoru, nie zapewnił, aby wszystkie jednostki organizacyjne Gminy oraz jednostki podległe i nadzorowane przez jego organy wypełniły obowiązek wynikający z art. 21 ust. 1 i 22 ust. 1 pkt 5 ustawy KSC, tj. wyznaczyły i zgłosiły osoby odpowiedzialne za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Do dnia 31 sierpnia 2024 r. tego obowiązku nie wypełniła żadna z siedmiu jednostek podległych organom Gminy.

   Wójt wyjaśnił m.in, że nastąpiło to przez nieuwagę.

   W toku kontroli wszystkie ww. jednostki dokonały powyższego zgłoszenia

   (akta kontroli str. 820-823, 888, 934-935)

6. Urząd nie posiadał pełnej wiedzy na temat konfiguracji 10 z 15 objętych badaniem urządzeń[55], ponieważ nie zostały one uwzględnione w programie do elektronicznej inwentaryzacji sprzętu i oprogramowania, co było niezgodne z § 19 ust. 2 pkt 2 *KRI z 2024 r.* (uprzednio § 20 ust. 2 pkt 2 *KRI z 2012 r.*). Ustalono ponadto, że:
   - numery inwentarzowe pięciu komputerów uwidocznione w systemie nVision15 nie odpowiadały zapisom w kartach inwentarzowych,
   - laptop powierzony Wójtowi był faktycznie w posiadaniu innej osoby, a umieszczony na tej jednostce numer inwentarzowy nie odpowiadał numeracji wykazanej w karcie inwentarzowej,

[53] Dz.U z 2024 r., poz. 609, ze zm.
[54] Dz.U z 2024 r., poz. 340, ze zm.
[55] Trzech laptopów i trzech komputerów, urządzenia FortiGate-60F, drukarki, routera, serwera.

– laptop użytkowany przez jednostkę OSP nie posiadał oznaczeń inwentarzowych, które zostały wykazane w karcie inwentarzowej tego sprzętu, a router w ogóle nie posiadał takich oznaczeń,
– laptop powierzony kierownikowi referatu organizacyjnego był faktycznie użytkowany przez informatyka.

Wszystkie ww. zaniechania były działaniami nierzetelnymi, w wyniku których Urząd nie posiadał pełnej wiedzy możliwej do wykorzystania w procesie konieczności przeprowadzania konfiguracji poszczególnych urządzeń.

Wójt podał, że ww. niezgodności powstały omyłkowo i zostały już w toku kontroli usunięte.

(akta kontroli str. 337-343, 398-465, 598-612)

OCENA CZĄSTKOWA

W kontrolowanym okresie w jednostce wdrożono środki organizacyjne służące zapewnieniu bezpieczeństwa informacji, w tym danych osobowych, systemów teleinformatycznych oraz ciągłości działania. Powołano *IOD* zapewniając mu niezależność oraz wykluczając (od 28 lutego 2023 r.) jego działanie w sytuacji działania konfliktów interesów. Wyznaczono ponadto osobę odpowiedzialną za zapewnienie bezpieczeństwa informacji. Była to osoba posiadające odpowiednie kwalifikacje i doświadczenie zawodowe. W urzędzie wyznaczono także osobę odpowiedzialną za kontakty z podmiotami krajowego systemu cyberbezpieczeństwa. Wójt nie zapewnił jednak, by obowiązek ten wykonały podległe i nadzorowane przez niego jednostki organizacyjne. Urząd posiadał ponadto przygotowany PCD. Nie mniej poza *PBDO* nie dokonano jednak przeglądu i aktualizacji procedur.

OBSZAR

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

Opis stanu faktycznego

2.1. W Urzędzie prowadzono politykę nadawania pracownikom określonych uprawnień w celu dostępu do systemów informatycznych. Badanie w zakresie zapobiegania możliwości zainstalowania nieautoryzowanego oprogramowania na 10 urządzeniach, w tym: pięciu komputerach przenośnych i pięciu stacjonarnych wykazało, że w sześciu przypadkach zastosowano skuteczne mechanizmy blokujące. W pozostałych czterech przypadkach (urządzenia przenośne) możliwe było zainstalowanie pobranego oprogramowania, o czym szerzej w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 344, 394-397,613-658, 930, 940-941)

W badanym okresie pracownicy Urzędu korzystali ze służbowych smartfonów (17 w 2023 r. i 16 w 2024 r.). Wójt podał, że ww. urządzenia były wykorzystywane wyłącznie do połączeń głosowych. Nie były na nich przetwarzane informacje służbowe i z tego powodu nie zostały zabezpieczone przed instalacją dowolnego oprogramowania. W jednostce nie korzystano z tabletów.

(akta kontroli str. 344, 347-348. 926-929)

2.2. W badanym okresie w Urzędzie obowiązywały procedury nadawania i odbierania uprawnień w systemach informatycznych pracownikom Urzędu[56]. Kwestie obsługi i autoryzacji wniosków powierzono *ASI*, natomiast bezpośredni przełożeni odpowiadali za zgodność uprawnień pracowników z ich obowiązkami.

[56] Regulamin nadawania, modyfikacji, odbierania i przeglądu uprawnień w systemach informatycznych, dalej: „RNSI".

Urząd nie opracował zasad dostępu do systemów dla podmiotów zewnętrznych, o czym szerzej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 236-239, 613-614, 807-811)

Badanie na próbie 16 pracowników wykonujących zadania w systemach informatycznych jednostki wykazało, że we wszystkich przypadkach przyznane zostały uprawnienia do systemu odpowiadające zakresowi obowiązków. W jednym przypadku, doszło do zmiany uprawnień pracownika. Ww. zmiana nastąpiła 33 dni[57] od zmiany stanowiska. Wójt podał, że zmiana zakresu uprawnień nastąpiła z opóźnieniem, ponieważ pracownik na zwolnione przez siebie stanowisko wprowadzał nowo zatrudnioną osobę. Z tego powodu mimo zmiany zakresu obowiązków ww. osoba musiała przez określony czas dysponować dostępem do dotychczas obsługiwanych systemów.

(akta kontroli str. 613-658, 801-811)

2.3. Weryfikacja dokumentacji trzech pracowników, którzy zakończyli zatrudnienie w Urzędzie[58] wykazała, że nie mieli oni możliwości pracy w systemach zawierających przetwarzane informacje. Było to zgodne z § 19 ust. 2 pkt 4 i 5 *KRI z 2024* r. (uprzednio§ 20 ust. 2 pkt 4 i 5 *KRI z 2012 r.*).

(akta kontroli str. 658, 802, 808, 938-939)

2.4. W celu zapewnienia ochrony przetwarzanych informacji przed nieuprawnionym dostępem do systemów operacyjnych komputerów oraz systemów informatycznych zarządzanych przez Urząd stosowano metodę uwierzytelniania (identyfikator i hasło). Badanie zabezpieczeń dostępu do systemów operacyjnych na 10 stacjach roboczych wykazało, że dla dziewięciu jednostek komputerowych zastosowano metody uwierzytelniania dostępu przy czym w trzech przypadkach nie odpowiadały one ustalonym w Urzędzie zasadom. Dodatkowa weryfikacja stosowania haseł w trzech wybranych programach dziedzinowych wykazała, że faktycznie stosowane w Urzędzie reguły tworzenia haseł odbiegały od zasad określonych w *PBT* i *RUI*, o czym szerzej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 188-198, 394- 397, 659-662, 930)

2.5. Przyjęte w Urzędzie reguły postępowania z informacjami przetwarzanymi w systemach teleinformatycznych[59] zalecały ustawianie monitorów w sposób uniemożliwiający wgląd osobom postronnym. Nakazywano również stosowanie zasady czystego ekranu, tj. w trakcie pracy na stanowisku miały być otwarte jedynie niezbędne aplikacje i programy, a w sytuacji tymczasowego zaprzestania pracy użytkownik zobowiązany był uruchomić, chroniony hasłem, wygaszacz ekranu.

(akta kontroli str. 209-217)

Oględziny pięciu stanowisk pracy w miejscach, gdzie dostęp mają klienci Urzędu wykazały brak możliwości wglądu do danych przez osoby nieuprawnione. W czterech przypadkach wymóg ten spełniono dzięki odpowiedniemu usytuowaniu monitorów komputerowych, a w jednym poprzez nałożenie filtra prywatyzującego ekran. Powyższe działania spełniały wymogi § 19 ust. 2 pkt 7 *KRI z 2024 r.*

(akta kontroli str. 666-674)

[57] Do zmiany stanowiska doszło w lipca 2023 r, a zmiana uprawnień nastąpiła 3 sierpnia 2023 r.

[58] 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.

[59] Regulamin użytkownika informacji, dalej; „*RUI*".

2.6. W Urzędzie opracowano procedurę dotyczącą pracy zdalnej[60]. *RPZ* regulował m.in. ogólne zasady korzystania ze sprzętu informatycznego oraz zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość. Przy czym nie określono w niej zasad korzystania ze sprzętu informatycznego minimalizujące ryzyka kradzieży środków przetwarzania informacji, w tym urządzeń mobilnych. Nie wprowadzono również rozwiązań informatycznych zapewniających bezpieczną pracę użytkowników w formie pracy zdalnej, o czym szerzej w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 163-171, 675, 803-814)

2.7. Wójt wyjaśnił, że spośród pięciu laptopów należących do Urzędu, trzy urządzenia podłączane do sieci wewnętrznej zostały zaszyfrowane. Kolejne dwa pozostające w faktycznej dyspozycji OSP, nie były szyfrowane ponieważ nie używano ich w Urzędzie, o czym szerzej w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 339-343, 926-929, 931)

2.8. Realizując wymóg § 19 ust. 2 pkt 9 *KRI z 2024 r.* (wcześniej § 20 ust. 2 pkt 9 *KRI z 2012 r.*) w Urzędzie stosowano środki organizacyjne, fizyczne i techniczne służące zabezpieczeniu informacji znajdujących się na serwerach.

Serwerownia znajdowała się w odrębnym, nieoznakowanym pomieszczeniu, a dostęp do niego był ograniczony. W pomieszczeniu zastosowano środku zabezpieczające przed czynnikami środowiskowymi: jeden klimatyzator, czujnik dymu, gaśnica oraz zasilacze awaryjne. W toku oględzin stwierdzono ponadto, że pomieszczenie serwerowni nie odpowiadało wszystkim przyjętym przez Urząd zasadom, o czym szerzej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 218-222, 676-685, 803, 809)

2.9. W jednej z czterech umów zawartych w sprawie zamówienia usług serwisowych Urząd zamieścił zapisy gwarantujące odpowiedni poziom bezpieczeństwa danych osobowych. W żadnej z umów nie wprowadzono zapisów zobowiązujących wykonawców do zachowania w tajemnicy informacji, do jakich mógł mieć dostęp w ramach wykonywania umowy, innych niż dane osobowe, co szerzej opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 697-719, 889)

2.10. W toku badania ustalono, że w 2023 r. Urząd przekazał jeden nowy laptop na potrzeby żłobka w Osiu. Dwa kolejne urządzenia były użytkowane przez jednostki OSP. Zgodnie z oświadczeniem Wójta powyższe urządzenia nie zawierały informacji przetwarzanych w Urzędzie. Nie przekazywano również ww. urządzeń do serwisowania lub naprawy. W kontrolowanym okresie w Urzędzie nie obowiązywała procedura dotycząca przekazywania sprzętu poza jednostkę. Wójt wyjaśnił, że dotychczas nie było potrzeby przekazywania sprzętu poza jednostkę, wobec tego taka regulacja nie została przygotowana i wdrożona.

(akta kontroli str. 720-727, 804, 908, 929)

2.11. W celu zapewnienia ciągłości działania w Urzędzie przyjęto Regulamin zarządzania kopiami zapasowymi, który ustalał polityki w zakresie tworzenia i przechowywania kopii zapasowych. W *RZKP* ustalono ponadto podstawowe zasady (wytyczne) sporządzania kopii zapasowych oraz ustalono harmonogram ich wykonywania (kopie dzienne, miesięczne, roczne)[61]. Nie określono natomiast zasad,

[60] Regulamin pracy zdalnej, dalej: *RPZ*

[61] W zakresie danych: Profile użytkowników systemu głównego, zasoby plikowe oprogramowania (systemów informatycznych), Kopie baz danych w plikach, Systemy operacyjne serwerów).

jak długo powinny być one przechowywane oraz kto powinien mieć do nich dostęp, o czym szerzej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. , 229-235, 804, 809, 855, 923-929)

2.12. Przyjęte procedury przewidywały tworzenie (zapisywanie) kopii zapasowych w chmurze oraz ich przechowywania w odrębnym pomieszczeniu. Oględziny wykazały, że ww. w przypadku jednego z serwerów zasady te nie były w pełni przestrzegane, o czym szerzej w sekcji *Stwierdzone nieprawidłowości.*

Przeprowadzone w toku kontroli badanie odzyskiwania danych z kopii zapasowej dla jednego wybranego systemu z 30 kwietnia 2024 r. nie było możliwe z powodu braku kopii zapasowej (możliwe było odtworzenia danych od 21 maja 2024 r.), o czym szerzej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 206-208, 229-235)

W badanym okresie nie prowadzono testowania kopii zapasowych danych i oprogramowania aplikacyjnego, w którym przetwarzane były dane. Szerzej na temat ww. niezgodności w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 206-208, 229-235, 815-816, 936-937)

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 50,18 %, na pozostałych dwóch znajdowały się natomiast partycje zajęte w udziale przekraczającym 85%, co szerzej opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 729-756)

2.13. W ramach zapewnienia ciągłości działania nie zidentyfikowano kluczowych elementów infrastruktury i usług IT oraz nie zidentyfikowano czasów przywrócenia do działania poszczególnych systemów informacyjnych.

Wójt podał, że czas przywracania ciągłości działania systemów informatycznych nie został określony na skutek nieuwagi. Natomiast brak identyfikacji kluczowych elementów infrastruktury i usług IT wynikał z przekonania, że wykonał to zadanie podmiot przygotowujący w 2022 r. raport cyberbezpieczeństwa.

(akta kontroli str. 344-348, 757, 805, 810, 929)

Stwierdzone nieprawidłowości

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

1. Uprawnienia nadane użytkownikom czterech z 10 objętych oględzinami urządzeń umożliwiały im instalację dowolnego oprogramowania i aplikacji. Naruszało to § 19 ust. 2 pkt 4 *KRI z 2024 r.* (wcześniej § 20 ust. 2 pkt 4 *KRI z 2012 r.*). Ponadto było to niezgodne z § 2 *RNU*, który zobowiązywał do zapewnienie odpowiedniego bezpieczeństwa systemów informatycznych i informacji w nich przetwarzanych oraz § 2 ust. 1 pkt 1 i 14 oraz § 5 ust. 1 pkt 3 i 5 *PBI*, które zobowiązywały do ochrony aktywów (zasobów) Urzędu .

   Wójt wyjaśnił, że w przypadku dwóch komputerów pracownik nie cofnął odpowiednich uprawnień po aktualizacji ich oprogramowania. Dwa kolejne nie zostały natomiast zabezpieczone z uwagi na ich przekazanie do użytkowania jednostkom ochotniczej straży pożarnej.

   NIK zwraca uwagę, że karty wyposażenia badanych urządzeń potwierdzały, że były one w posiadaniu Urzędu. Tym samym podlegały one wymaganiom *PBI*, które nakładało obowiązek ochrony wszystkich jego aktywów. Użytkowanie

zasobów Urzędu przez podmioty trzecie, nie zwalniało zatem z konieczności utrzymania zabezpieczeń poszczególnych urządzeń na odpowiednim poziomie.

(akta kontroli str. 80-84, 236-238, 400-401, 598-599, 608-611, 801, 807, 940-941)

2. W toku badania ustalono, że w jednym z programów znajdowało się konto nieprzypisane do pracownika, a w kolejnym trzy identyfikatory nie zostały jednoznacznie powiązane z użytkownikami, co było niezgodne z § 5 ust. 1 i 2 *PBT*.

   Wójt podał, że konieczność utworzenia takich kont wynikała z potrzeb pracownika firmy prowadzącej serwis oprogramowania lub wymogów oprogramowania (były niezbędne do prawidłowego funkcjonowania systemu) Wskazał ponadto, że ww. kwestie omyłkowo pominięto przy tworzeniu *RNU*.

   NIK nie kwestionuje konieczności tworzenia ww. kont. Zwraca jednak uwagę, że w *PBT* Urząd jednoznacznie wymagał przypisania konta do osoby i nie określił wyjątków od tej zasady.

   (akta kontroli str. 186-198, 209-217, 394-397, 659-665, 802-809, 926-930)

3. Weryfikacja zabezpieczeń dostępu do systemów operacyjnych na stacjach roboczych w Urzędzie wykazała, że w przypadku jednego z 10 urządzeń nie zastosowano metody uwierzytelniania dostępu, a w przypadku trzech kolejnych długość haseł nie odpowiadała zasadom określonym w § 5 ust. 8 pkt 2 *PBT* oraz § 6 ust. 8 *RUI*.
   Ponadto w trakcie kontroli dostępu do trzech programów dziedzinowych[62] ustalono, że przy korzystaniu z ww. systemów pięcioro z 11 pracowników[63] posługiwało się hasłami z mniejszą od wymaganej liczby znaków, co nie odpowiadało wymogom określonym w § 5 ust. 8 pkt 2 *PBT* oraz § 6 ust. 8 *RUI*.
   Dodatkowo jeden z systemów nie posiadał żadnych ustawień w zakresie złożoności haseł oraz wymogów dotyczących terminu wygaśnięcia haseł. Kolejny oprócz braku określonego terminu ważności hasła wymagał mniejszej liczby znaków, niż wynikało to z regulacji wewnętrznych. W ostatnim z programów natomiast brak było możliwości wygenerowania przyjętych zasad złożoności haseł oraz okresów, w jakich powinny być one zmienione. Z oświadczenia informatyka wynikało natomiast, że przyjęte zasady wymuszały tworzenie haseł zawierających mniejszą liczbę znaków, niż przewidywały to reguły określone § 5 ust. 8 pkt 1 i 2 *PBT* oraz § 6 ust. 8 *RUI*.

   Wójt odnosząc się do sposobu dostępu do systemów operacyjnych podał, że dwa z urządzeń nie były odpowiednio zabezpieczone z powodu ich przekazania w użytkowanie jednostkom OSP, a kolejne dwa z powodu braku cofnięcia odpowiednich uprawnień po aktualizacji przez informatyka. Wyjaśniając natomiast niezgodności w dostępie do programów dziedzinowych stwierdził że informatyk nie wymuszał odpowiedniej liczby znaków zakładając, że odpowiednie hasło do systemu operacyjnego wystarczy do właściwego zabezpieczenia danych.

   NIK zwraca uwagę, że w § 5 ust. 8 *PBT* Urząd określił minimalne warunki tworzenia hasła odnoszące się do wszystkich systemów[64], Tym samym

[62] Zarządzanych przez Urząd.
[63] Dwóch w dwóch programach i jeden w trzecim.
[64] W treści regulacji wewnętrznej użyto liczby mnogiej.

odpowiednia długość hasła winna być stosowana zarówno przy dostępie do systemu operacyjnego, jak i poszczególnych programów dziedzinowych.

(akta kontroli str. 186-198, 209-217, 394-397, 659-665, 802-809, 926-930)

4. W procesie nadawania i modyfikacji uprawnień informatycznych 16 objętych badaniem pracowników nie zastosowano wniosku przewidzianego w procedurze wewnętrznej Urzędu, co było niezgodne z § 3 ust. 2 w zw. z § 5 *RNU*.

   Wójt podał, że nie wykorzystywano wniosku określonego w procedurze, ponieważ z uwagi na wielkość Urzędu wszystkie sprawy były załatwiane ustnie.

   NIK zwraca uwagę, że zgodnie z § 19 ust. 1 *KRI z 2024 r.* (wcześniej § 20 ust. 1 *KRI z 2012 r.*) Urząd był m.in. zobowiązany do zapewnienia rozliczalności, niezaprzeczalności oraz niezawodności systemu zarządzania bezpieczeństwem informacji. Prowadzenie spraw ustnie, poza ustaloną procedurą, nie gwarantowało zgodności tego systemu z ww. wymogami.

   (akta kontroli str. 238-239, 613-614, 806, 811, 886)

5. W stosowanym w Urzędzie *RPZ* nie wprowadzono:
   - zasad korzystania ze sprzętu informatycznego minimalizujących ryzyka kradzieży środków przetwarzania informacji, w tym urządzeń mobilnych,
   - rozwiązań informatycznych zapewniających bezpieczną pracę użytkowników w formie pracy zdalnej,

   co było niezgodne z § 19 ust. 2 pkt 8 i 11 *KRI z 2024 r.* (uprzednio § 20 ust. 2 pkt 8 i 11 *KRI z 2012 r.*).

   Wójt wyjaśnił m.in., że nie ustanowiono powyższych zasad oraz nie wprowadzono odpowiednich rozwiązań, ponieważ żaden z pracowników nie wykonywał pracy zdalnie.

   NIK zwraca uwagę, że praca zdalna była równorzędną formą pracy, stąd niezbędne było ustanowienie odpowiednich zasad jej wykonywania.

   (akta kontroli str. 163-171, 675, 803, 813-814)

6. Dwa z pięciu laptopów należących do Urzędu, nie zostały zaszyfrowane, co było niezgodne z § 19 ust. 2 pkt 12 ppkt d) *KRI z 2024 r.* (uprzednio § 20 ust. 2 pkt 12 ppkt d) *KRI z 2012 r.*).
   Wójt podał, że oba laptopy nie zostały zaszyfrowane, ponieważ zostały przekazane na roboczo do użytkowania jednostkom OSP i nie zawierały żadnych danych.
   NIK zwraca uwagę, że sprzęt należący do Urzędu winien być odpowiednio zabezpieczony niezależnie od sposobu jego użytkowania, a przed jego przekazaniem należało co najmniej upewnić się, czy wszystkie jego składniki faktycznie nie zawierają informacji, czego nie zrobiono.
   (akta kontroli str. 339-343, 394-415, 602-613, 926-931)

7. W toku oględzin ustalono, że pomieszczenie serwerowni nie spełniało sześciu ustalonych przez Urząd wymogów, związanych z jej wyposażeniem, wymaganym systemem nadzoru i zasilania awaryjnego, co było niezgodne z § 2, § 4 ust. 2, 4, 7 i 10, § 5 ust. 7 oraz § 6 ust. 2 i 3 *RWS*.

   Wójt podał, że nie spełniono wszystkich wymagań dotyczących przygotowania serwerowni z uwagi na możliwości finansowe Urzędu.

   (akta kontroli str. 218-222, 676-685, 803-804, 809, 942)

8. W trzech z czterech obowiązujących w kontrolowanym okresie, a poddanych badaniu umowach serwisowych[65], nie zawarto zapisów gwarantujący odpowiedni poziom bezpieczeństwa informacji, do jakich mogli mieć dostęp pracownicy ww. podmiotów. W ostatniej z ww. umów odpowiednie zapisy natomiast ograniczono do ochrony danych osobowych[66], co było niezgodne z § 19 ust. 2 pkt 11 *KRI z 2012 r.* (uprzednio z § 20 ust. 2 pkt 11 *KRI z 2012 r.*).

   Wójt wyjaśnił m.in, że nastąpiło to na skutek nieuwagi pracownika.

   (akta kontroli str. 697-719, 697-719, 804-809, 926, 928)

9. W Urzędzie 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 dysków przekraczała 85%[67].

   Wójt podał m.in, że poziom zajętości tych serwerów był wysoki, ponieważ informatyk nie sprawdził ich pojemności.

   (akta kontroli str. 172-186, 327-329, 345, 348, 748, 926, 929)

10. W toku kontroli ustalono, że Urząd nie dysponował możliwością odtworzenia kopii danych z kwietnia 2024 r., co było niezgodne z § 4 ust. 10 pkt 3 *RZKZ*, który zobowiązywał nie rzadziej, jak raz w miesiącu zapisywać pliki baz danych na zewnętrznym nośniku. Ponadto brak było kopii zapasowych baz danych z 22 i 23 lipca 2024 r., co było niezgodne z § 4 ust. 10 pkt 2 *RZKZ,* który wymagał sporządzania codziennie kopii baz danych.

    Wójt podał, że brak kopii z kwietnia 2024 r. wynikał z błędnego zaznaczenia przez informatyka (w oprogramowaniu Xopero) okresu retencji kopii. Natomiast dwie kopie dzienne nie zostały wykonane ze względu na odłączenie przez informatyka zasilania serwerów z powodu zapowiadanych burz i wyładowań atmosferycznych.

    (akta kontroli str. 232, 730, 804, 804, 809-810)

11. W trakcie oględzin ustalono, że na jednym z serwerów zapisywane był kopie serwera wirtualnego, a kolejne z urządzeń wykorzystano do tworzenia kopii maszyn wirtualnych znajdujących się na tym serwerze. Stwierdzono ponadto, że urządzenie to służyło do przechowywania kopii baz danych z 2023 r. Ww. postępowanie było niezgodne z warunkami określonymi w § 4 ust. 2 *RZKZ*, gdzie wymagano przechowywania kopii zapasowych w innym pomieszczeniu.

    Wójt podał, że kopie maszyn wirtualnych nie zostały odmiejscowione z uwagi na koszt takiej usługi. Stwierdził ponadto, że kopie baz danych za 2023 r. były przechowywane na serwerze bazodanowym, ponieważ informatyk przez nieuwagę nie przeniósł ich na serwer zewnętrzny.

    (akta kontroli str. 729-747, 805, 809, 923-926, 928)

12. W okresie objętym kontrolą nie prowadzono w Urzędzie testów odtworzenia kopii zapasowych i oprogramowania aplikacyjnego, co było niezgodne z § 19 ust, 2 pkt 12 lit b) i e), § 19 ust. 2 pkt 2 *KRI z 2024 r.* (uprzednio § 20 ust. 2 pkt 12 lit b) i e), § 20 ust. 2 pkt 2 *KRI z 2012 r.*) w zw. z § 4 ust. 11 *RZKZ*.

[65] Zawarte 7 grudnia 2023 r., 28 lutego 2024 r., 16 maja 2024 r.
[66] W dniu zawarcia umowy (3 stycznia 2024 r.) na świadczenie usług zawarto odrębna umowę powierzenia przetwarzania danych osobowych.
[67] 87,55% oraz 96,91%.

Wójt podał, że nie przeprowadzono ww. testów przez nieuwagę informatyka

(akta kontroli str. 206-208, 229-235, 815-816, 728, 936-937)

OCENA CZĄSTKOWA

Urząd podejmował działania mające na celu ochronę zasobów informacyjnych, jednak nie były one skuteczne. Stwierdzono bowiem m.in.: niezachowanie zasad dotyczących możliwości instalowania nieautoryzowanego oprogramowania, tworzenia i weryfikacji haseł, szyfrowania laptopów, przygotowania serwerowni oraz tworzenia, przechowywania i testowania kopii zapasowych, a także monitowania pojemności nośników pamięci serwerów. W toku kontroli ustalono także, że Urząd nie zapewnił ochrony informacji, które mogli pozyskać wykonawcy umów serwisowych.

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 Urzędzie potwierdzając w listopadzie 2023 r. aktualność ryzyk określonych w opracowanym w listopadzie 2022 r. dokumencie pn. Analiza ryzyka ogólnego i ocena skutków przetwarzania danych (DPIA) W sporządzanych analizach pogrupowano zidentyfikowane ryzyka uwzględniając kontekst ich przetwarzania[68], a następnie w odniesieniu do każdej z grup: [1] zidentyfikowano kategorię zagrożenia, [2] rodzaj zagrożenia i [3] macierzy (poufność/dostępność/integralność). Następnie przeprowadzono analizę poszczególnych ryzyk oraz dokonano ich oceny. Przyjęto ponadto plan postępowania z ryzykiem.

(akta kontroli str. 92-149, 758-766)

3.2. W okresie objętym kontrolą w Urzędzie obowiązywały zasady zarządzania incydentami związanymi z bezpieczeństwem informacji. Kwestie te, zgodnie z art. 22 ust. 1 pkt 1 ustawy o KSC w zw. z § 19 ust. 2 pkt 13 *KRI z 2024 r.*[69], regulował *Regulamin zarządzania incydentami w zakresie bezpieczeństwa informacji* oraz *Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych*[70].

(akta kontroli str. 172-186, 327-329, 345, 348, 760-768, 926, 929)

W okresie objętym kontrolą w prowadzonym przez *ASI* rejestrze incydentów naruszenia bezpieczeństwa informacji nie odnotowano żadnego incydentu. Kontrola wykazała jednak, że w latach 2023-2024 (do 20 sierpnia) wystąpiło 11 takich przypadków, o czym szerzej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 760-768)

3.3. W latach 2023-2024 pracownicy Urzędu uczestniczyli w czterech szkoleniach z zakresu bezpieczeństwa informacji. Ich tematyka dotyczyła m.in. zagrożenia bezpieczeństwa informacji, skutków naruszeń oraz stosowanych środkach zapewniających bezpieczeństwo informacji. Szkoleniami objęto wszystkich pracowników zaangażowanych w proces przetwarzania informacji, przy czym w 2023 r. w ww. przedsięwzięciach uczestniczyło jedynie 15 z 22 pracowników (68,2%), o czym szerzej w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 354-356, 769-796, 817-819, 872, 890-922, 940-941)

[68] Dane osobowe związane z pracownikami [1], z usługami „na zewnątrz"[2] (np. czynności dla społeczeństwa, programy dofinansowania, itd.) i „do wewnątrz" [3] (np. kontrahenci, usługodawcy, itp.).
[69] Wcześniej § 20 ust. 2 pkt 13 rozporządzenia w sprawie KRI z 2012 r.
[70] Załącznik *nr 10 do PBDO*.

3.4. W latach 2023-2024[71] w Urzędzie nie przeprowadzono audytu wewnętrznego w zakresie bezpieczeństwa informacji, o czym szerzej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 797)

Stwierdzone nieprawidłowości

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

1. Proces ewidencji incydentów związanych z bezpieczeństwem informacji był prowadzony przez Urząd w sposób nierzetelny. Badanie wybranych rodzajów incydentów wykazało bowiem, że w latach 2023-2024[72] doszło łącznie do wystąpienia 11 incydentów[73], których nie odnotowano *w Raporcie z incydentu*[74] *oraz Rejestrze z incydentów,* co było niezgodne z zasadami określonymi w § 7 ust. 1 oraz § 8 ust. 1 *RZI* w zakresie bezpieczeństwa informacji. Na skutek ww. zaniechań Urząd nie dysponował aktualną wiedzą na temat aktualnych zagrożeń bezpieczeństwa informacji.

   Wójt podał, że o odnotowywaniu ww. incydentów nie pamiętał informatyk.

   NIK zwraca uwagę, że sporządzanie raportów z incydentów ma kluczowe znaczenie dla całego procesu bezpieczeństwa informacji. Dokumentacja zdarzeń pozwala bowiem na ich późniejszą analizę oraz zapobieganie przyszłym incydentom. Pozwala także na zwiększenie świadomości występowania ryzyk w Urzędzie oraz poprawę efektywności działań naprawczych.

   (akta kontroli str. 60, 178-179, 761, 805,)

2. W 2023 r. Urząd nie przeprowadził audytu wewnętrznego w zakresie bezpieczeństwa informacji co było niezgodnie z § 20 ust. 2 pkt 14 rozporządzenia w sprawie *KRI z 2012 r*.

   Wójt podał, że nie został on przeprowadzony z uwagi na obawę dublowania wydatków, gdyż zapowiadany w 2023 r. program *Cyberbezpieczny Samorząd* wymagał w założeniach także przeprowadzenia audytu.

   NIK zwraca uwagę, że w 2023 r. na Urzędzie ciążył obowiązek wykonania audytu, niezależnie od źródła jego finansowania. Urząd winien zatem tak zaplanować swoje działania, aby niezależnie od sposobu ich finansowania, wymagane ww. przepisami działania faktycznie zrealizować.

   (akta kontroli str. 344, 348, 797)

3. Urząd w 2023 r. nie udokumentował przeprowadzenia szkolenia dla 6[75] z 22 pracowników zaangażowanych w proces przetwarzania informacji. Na skutek ww. zaniechania mogło dojść do obniżenia poziomu bezpieczeństwa informacji gromadzonych przez Urząd. Ponadto pracownicy nie mieli możliwości zaktualizowania posiadanej wiedzy, co było działaniem nierzetelnym oraz niezgodnym z § 20 ust. 2 pkt 6 w zw. z ust. 3[76] *KRI z 2012 r.*

   Wójt wyjaśnił, że pracownicy brali udział w przedsięwzięciu szkoleniowym organizowanym przez NASK . Nie było możliwości skierowania na to szkolenie wszystkich osób. Pozostali pracownicy zostali przeszkoleni odrębnie przez informatyka. Przy czym Urząd nie udokumentował tego przedsięwzięcia.

---

[71] Stan na 20 sierpnia 2024 r.
[72] Stan na 30 sierpnia 2024 r.,
[73] Sześć zablokowanych kont użytkownika (dwa w 2023 r. i 4 w 2024 r.) oraz pięć awarii zasilania (trzy w 2023 r. oraz dwie w 2024 r.).
[74] Wg wzoru z załącznika nr 3 Regulaminu RZI.
[75] Jedna pracownica w 2023 r. pozostawała na urlopie macierzyńskim.
[76] Polska Norma PN-ISO/IEC 27001 w załączniku A, punkt 7.2.2 wskazywała, że wszyscy pracownicy organizacji […] powinni przejść stosowne kształcenie i szkolenie uświadamiające oraz regularnie otrzymywać aktualizacje polityk i procedur związanych z ich stanowiskiem

NIK zwraca uwagę, że na Urzędzie ciążył obowiązek stałego zarządzania bezpieczeństwem informacji, a szkolenie osób zaangażowanych w proces przetwarzania informacji zostało wskazane jako jedno z kluczowych działań umożliwiających zapewnienie odpowiedniego poziomu ww. procesu. Urząd powinien zatem, w procesie zarządzania mechanizmami kontroli zarządczej, dokumentować kluczowe procesy, w tym te dotyczące podnoszenia kompetencji zawodowych.

(akta kontroli str. 354-356, 793-796, 817-819, 940-941)

OCENA CZĄSTKOWA

W Urzędzie podejmowane były działania w celu zapobiegania incydentom bezpieczeństwa informacji. W szczególności prowadzone były analizy ryzyka utraty atrybutów bezpieczeństwa informacji oraz szkolenia pracowników. Część z tych działań zrealizowano jednak w sposób nieodpowiadający wymogom rozporządzenia w sprawie *KRI z 2012 r.* W 2023 r. nie przeprowadzono bowiem audytu bezpieczeństwa informacji, a szkoleniami objęto jedynie część pracowników zaangażowanych w proces przetwarzania informacji.

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 zaktualizowanie dokumentacji dotyczącej bezpieczeństwa informacji.
2. Zawieranie w umowach serwisowych zapisów zapewniających bezpieczeństwo danych, w tym danych osobowych.
3. Zapewnienie corocznego prowadzenia audytów bezpieczeństwa informacji.
4. Prawidłowe ewidencjonowanie incydentów bezpieczeństwa informacji.
5. Wprowadzenie mechanizmów uniemożliwiających instalację nieautoryzowanego oprogramowania.
6. Pełne wdrożenie elektronicznej inwentaryzacji sprzętu i oprogramowania.
7. Wykorzystywanie ustalonych wzorów wniosków w procesie nadawania i modyfikowania uprawnień informatycznych.
8. Przestrzeganie ustalonych reguł tworzenia haseł.
9. Zapewnienie odpowiedniego tworzenia kopii zapasowych oraz ich odpowiedniego przechowywania i testowania.
10. Regularne monitorowanie pojemności nośników danych.

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, 19 września 2024 r.

Kontroler
(-) Adam Ruciński
główny specjalista k.p.

Najwyższa Izba Kontroli
Delegatura w Bydgoszczy
(-) Tomasz Sobecki
p.o. Dyrektor