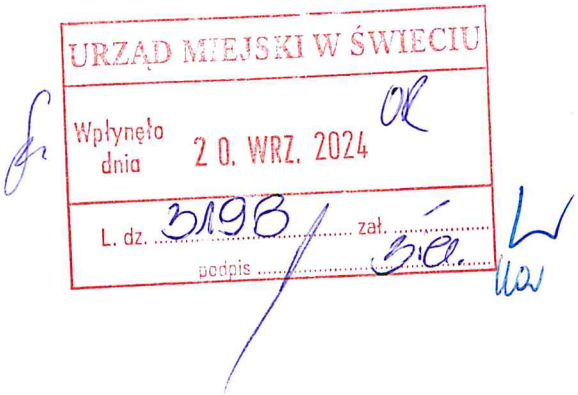
NAJWYŻSZA IZBA KONTROLI
Delegatura w Bydgoszczy

LBY.410.12.5.2024



Krzysztof Kułakowski
Burmistrz Świecia

Urząd Miejski w Świeciu
ul. Wojska Polskiego 124
86-100 – Świecie

WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Bydgoszczy
ul. Wały Jagiellońskie 12, 85-950 Bydgoszcz
T +48 52 567 58 00, F +48 52 567 58 60
lby@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miejski w Świeciu[1], ul. Wojska Polskiego 124, 86-100 Świecie
Kierownik jednostki kontrolowanej	Krzysztof Kułakowski, Burmistrz Świecia od 20 listopada 2018 r.
Zakres przedmiotowy kontroli	Rozwiązania organizacyjne i techniczne w zakresie zapewnienia bezpieczeństwa przetwarzania informacji oraz zapewnienia ciągłości działania w urzędzie i ich stosowanie
Okres objęty kontrolą	Od 1 stycznia 2023 r. do dnia zakończenia czynności kontrolnych w 2024 r.[2] (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[3]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Bydgoszczy
Kontrolerzy	Michał Trempała, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LBY/96/2024 z 6 czerwca 2024 r.

(akta kontroli str. 1-6)

[1] Dalej: „Urząd" lub „UM".
[2] Czynności kontrolne w jednostce zakończono 13 września 2024 r.
[3] Dz. U. z 2022 r. poz. 623, dalej: ustawa o NIK.

II. Ocena ogólna[4] kontrolowanej działalności

OCENA OGÓLNA

W kontrolowanym okresie w Urzędzie podejmowano działania na rzecz zapewnienia bezpieczeństwa informacji. Opracowano i wdrożono System Zarządzania Bezpieczeństwem Informacji oraz zapewniono aktualność dokumentów i polityk wchodzących w jego skład. Inspektorowi Ochrony Danych umożliwiono wykonywanie obowiązków w sposób niezależny.

W celu ochrony systemów informatycznych przed nieuprawnionym dostępem, określono i stosowano zasady bezpieczeństwa oraz politykę haseł. Pracownicy uczestniczyli w procesie przetwarzania informacji w stopniu adekwatnym do realizowanych przez nich zadań, zaś po zakończeniu zatrudnienia blokowano im dostęp do systemów informatycznych. Wprowadzono środki organizacyjne, fizyczne i techniczne zapewniające bezpieczeństwo informacji znajdujących się na serwerach. W ramach zapewnienia ciągłości działania Urzędu ustalono i stosowano zasady tworzenia i przechowywania kopii zapasowych. Opracowano także procedurę zgłaszania i postępowania z incydentami naruszenia bezpieczeństwa informacji.

Nie dokumentowano jednak prowadzonych analiz ryzyka utraty integralności, dostępności lub poufności informacji, a pracownikom zaangażowanym w proces przetwarzania informacji nie zapewniono szkoleń z zakresu cyberbezpieczeństwa. Audyt wewnętrzny w zakresie bezpieczeństwa informacji, z uwagi na powierzenie jego realizacji pracownikom odpowiadającym za przedmiot audytu, pozbawiony został przymiotu niezależności i obiektywizmu. Ponadto Burmistrz nie powołał pełnomocnika do spraw bezpieczeństwa informacji, choć zobowiązał się do tego wydając zarządzenie, a zgłoszenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa dokonano z naruszeniem ustawowego terminu. Przyjęte w UM plany zapewnienia ciągłości działania oraz plany odtworzeniowe nie były testowane, przez co ich praktycznej skuteczności nie można było zweryfikować. W Urzędzie nie przeprowadzano regularnych testów tworzonych kopii zapasowych danych i oprogramowania. Nie zidentyfikowano też kluczowych elementów infrastruktury i usług IT oraz ich zabezpieczeń pod kątem wpływu czynników zewnętrznych.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[5] kontrolowanej działalności

OBSZAR

1. Organizacja bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych

Opis stanu faktycznego

Zgodnie z regulaminem organizacyjnym UM[6] do zadań Sekretarza należało m.in. rozwijanie i koordynowanie procesu informatyzacji Urzędu, współpraca z Inspektorem Ochrony Danych Osobowych, a także nadzór nad pracą Wydziału Organizacyjnego[7]. Obowiązkiem Wydziału była m.in. organizacja i wdrażanie prac eksploatacyjnych systemów informatycznych i oprogramowania w Urzędzie.

(akta kontroli str. 7-39)

---

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

[5] 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.

[6] Wprowadzonym zarządzeniem Burmistrza nr 27/24 z 7 czerwca 2024 r. W okresie objętym kontrolą obowiązywał także regulamin organizacyjny ustalony zarządzeniami nr 1524/23 z 12 kwietnia 2023 r. oraz 457/16 z 31 marca 2016 r. (ze zmianami).

[7] Por. § 19 ust. 2 pkt 5 i 11 oraz ust. 4 regulaminu organizacyjnego.

1.1. W Urzędzie zidentyfikowano zbiory danych podlegających zabezpieczeniu[8] w tym m.in. służące do ewidencjonowania ludności, pobierania podatków i opłat lokalnych, ewidencjonowania gruntów i budynków, dróg lokalnych, systemy kadrowo-płacowe, systemy wspomagające zarządzanie budżetem Gminy czy ewidencje umów dzierżawy, najmu lub użyczenia. Zestawienie ich sporządzono w ramach audytu bezpieczeństwa informacji w grudniu 2023 r. Ujęto w nim m.in. ich nazwy, główne funkcje, zakresy stosowania (przedmiotowy i podmiotowy), powiązania z innymi systemami oraz rodzaj zabezpieczeń informatycznych. W każdym przypadku określono także skalę krytyczności systemu dla funkcjonowania Urzędu i określono poziom jego ochrony[9]. W zestawieniu pomięto jeden ze zbiorów wykorzystywany do wykonywania zadań publicznych, co szczegółowo opisano w sekcji Stwierdzone nieprawidłowości

(akta kontroli str. 240, 242-245, 468, 481-485)

1.2. W Urzędzie opracowano, ustanowiono i wdrożono w 2023 r. System Zarządzania Bezpieczeństwem Informacji (dalej „SZBI")[10] o którym mowa w § 19 ust. 1 rozporządzenia Rady Ministrów z 21 maja 2024 r. w sprawie krajowych ram interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[11]. SZBI obejmował:

- bezpieczeństwo osobowe,
- ochronę danych osobowych,
- bezpieczeństwo fizyczne,
- bezpieczeństwo teleinformatyczne,
- bezpieczeństwo prawne oraz
- zarzadzanie ryzykiem.

W okresie poprzedzającym obowiązywała Polityka Bezpieczeństwa Informacji UM z 2016 r.[12]. Podstawowym dokumentem SZBI była Polityka Bezpieczeństwa Informacji (dalej: „PBI"). Określono w niej m.in. regulaminy korzystania: z urządzeń mobilnych, przeglądarki internetowej, poczty elektronicznej czy publikowania informacji w Internecie. Dokumenty zostały zakomunikowane pracownikom UM poprzez zamieszczenie w Biuletynie Informacji Publicznej[13]. Badanie przeprowadzone na próbie 28 pracowników[14] potwierdziło, że złożyli oni oświadczenia o zapoznaniu się z treścią PBI oraz zobowiązaniu się do zachowania w poufności przetwarzanych informacji.

Zgodnie z zarządzeniem SZBI zarządzał Burmistrz w szczególności poprzez bieżącą aktualizację dokumentacji, w tym obowiązujących w Urzędzie aktów normatywnych o charakterze wewnętrzny. Kierownicy komórek organizacyjnych UM odpowiadali za wdrożenie i przestrzegacie SZBI w podległych jednostkach.

Burmistrz, mimo obowiązku wynikającego z zarządzenia o SZBI, nie powołał pełnomocnika ds. bezpieczeństwa informacji, co szczerzej opisano w sekcji Stwierdzone nieprawidłowości.

---

[8] Łącznie 29 systemów wykorzystywanych do realizacji zadań publicznych.

[9] W trzech przypadkach wskazując „średnio istotny" oraz w 26 – „istotny".

[10] Zarządzeniem Burmistrza nr 1557/23 z 11 maja 2023 r. Zarządzenie weszło w życie z dniem podjęcia. Jego wykonanie powierzono Sekretarzowi Gminy. Dalej: „zarządzenie o SZBI".

[11] Dz.U. z 2024 r. poz. 773, dalej: „rozporządzenie KRI". Wcześniej, do 22 maja 2023 r. obowiązywało rozporządzenie Rady Ministrów z 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.".

[12] Wprowadzona zarządzeniem Burmistrza nr 701/16 z 16 grudnia 2016 r.

[13] Dalej: „BIP Urzędu".

[14] Tj. 25% pracowników Urzędu.

(akta kontroli str. 40-169)

1.3. W celu wykonania obowiązku określonego w art. 24 i 25 rozporządzenia RODO[15] w UM wprowadzono Politykę Bezpieczeństwa Przetwarzania Danych Osobowych (dalej: „PBPDO")[16]. Jej wykonanie powierzono Inspektorowi Ochrony Danych. Określono w niej zasady i warunki przetwarzania danych osobowych w tym m.in. dotyczące:

- bezpieczeństwa fizycznego obszarów, w których przetwarzane są dane,
- rejestrowania czynności przetwarzania danych,
- kompetencji i zakresu obowiązków osób funkcyjnych[17],
- środków technicznych i organizacyjnych do zabezpieczenia danych (w tym zarządzania bezpieczeństwem komputerów i sieci),
- analiz ryzyka,
- przetwarzania danych osobowych w systemach informatycznych.

W PBPDO wskazano także:

1) procedurę realizacji praw osób, których dane dotyczą (w tym obowiązki informacyjne; dostęp, sprostowania i usuniecie danych),
2) instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych, instrukcję przetwarzania danych osobowych w systemach informatycznych,
3) procedurę rozpoczęcia, zawieszenia i zakończenia pracy w systemach informatycznych,
4) zasady bezpiecznego korzystania z Internetu, poczty elektronicznej, komputerów przenośnych i nośników informacji,
5) rodzaje naruszeń bezpieczeństwa systemów informatycznych i procedurę ich zgłaszania,
6) wzór rejestru czynności przetwarzania danych osobowych w UM.

Wszystkich pracowników upoważnionych do przetwarzania danych osobowych zobowiązano do zapoznania się z tym dokumentem. Zarządzenia opublikowano w BIP Urzędu.

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

(akta kontroli str. 175-224)

1.4. W UM określono procedury zarządzania ryzykiem w zakresie zagadnień finansowych, zasobów ludzkich, obszarów działalności czynników zewnętrznych[18].

Burmistrz wskazał, że w Urzędzie prowadzono analizy ryzyka w związku z potrzebą zachowania ciągłości działania systemów informatycznych. W arkuszu analizy ryzyka wskazano zagrożenia dla funkcjonowania Urzędu związane z infrastrukturą (w tym IT), pracownikami i podmiotami współpracującymi. Sporządzono także listę potencjalnych zagrożeń z podziałem na środowiskowe (niezależne od człowieka), przypadkowe i umyślne.

(akta kontroli str. 121,124, 147-154, 240, 472)

1.5. - 1.7. W załączniku do PBI określono plan ciągłości działania na wypadek pożaru. Określono zarazem plany awaryjne odtworzenia systemu informatycznego po awarii

---

[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. L. 119 z 4 maja 2016, str. 1, ze zm., dalej: „RODO".

[16] Zarządzeniami Burmistrza Świecia nr 33/19 z 9 stycznia 2019 r. oraz 1526/23 z 12 kwietnia 2023 r.

[17] Tj. Administratora Danych Osobowych, Inspektora Ochrony Danych oraz Administratora Systemu Informatycznego.

[18] Por. zarządzenie nr 358/11 z 30 grudnia 2011 r.

krytycznej, w tym zasady postępowania przy przywróceniu działania serwerów w lokalizacji podstawowej i alternatywnej, a także na wypadek braku zasilania lub utraty dostępu do Internetu.

W planie ciągłości działania wskazano sposób zgłaszania incydentów, działania awaryjne, sposoby przywrócenia działania tymczasowego oraz wznowienia działalności, a obowiązki w poszczególnych etapach przypisano ASI oraz Sekretarzowi Gminy. W przypadku zniszczenia infrastruktury informatycznej przewidziano przejście do realizacji Planu awaryjnego odtworzenia systemu informatycznego, w którym określono czas przywrócenia ciągłości jego działania[19].

Sekretarz Gminy wskazał, że o sposobach postępowania w sytuacjach awaryjnych zostali poinformowani członkowie Forum Bezpieczeństwa[20], którzy posiadają wiedzę niezbędną do zapobiegania incydentom i awariom. Wszyscy pracownicy UM zostali poinformowani o bezwzględnym obowiązku stosowania się do ich poleceń.

Opracowane plany ciągłości działania nie były testowane, co szczegółowo opisano w sekcji Stwierdzone nieprawidłowości.

(akta kontroli str. 155-157.240--241)

1.8. W urzędzie realizowano wynikający z § 19 ust. 2 pkt 1 rozporządzenia KRI obowiązek zapewnienia aktualizacji regulacji wewnętrznych stanowiących SZBI w zakresie dotyczącym zmieniającego się otoczenia. PBI została poddana przeglądowi i aktualizacji dwukrotnie w 2024 r.[21]. Uzupełnienia wynikały ze zmian personalnych[22] i organizacyjnych[23]. Dokonał ich Sekretarz Gminy zamieszczając w dokumentacji arkusz aktualizacji.

(akta kontroli str. 108)

1.9. W Urzędzie wyznaczono pracownika odpowiedzialnego za bezpieczeństwo informacji oraz zapewnienie ciągłości działania[24]. Zadania Administratora Systemów Informatycznych (dalej: „ASI") określono w zakresie czynności pracownika oraz PBI i PBPDO. Należały do nich m.in.

- sprawowanie nadzoru nad funkcjonowaniem infrastruktury sieciowej, maszyn i urządzeń informatycznych, urządzeń peryferyjnych oraz oprogramowania[25],
- prowadzenie dokumentacji związanej z zainstalowanym sprzętem komputerowym oraz oprogramowaniem,
- regularne wykonywanie lub zlecanie testów i audytów w celu potwierdzenia skuteczności istniejących zabezpieczeń,
- przedkładanie rocznych raportów o stanie urządzeń i systemów,
- przydzielanie zakresów zadań i odpowiedzialności za poszczególne systemy, elementy infrastruktury i procesy,
- wycofywanie uprawnień dostępu pracowników do systemów informatycznych (dezaktywacja identyfikatorów),
- uczestnictwo w Forum bezpieczeństwa[26],

---

[19] Tj. 3 godziny w lokalizacji podstawowej i 2 dnia w lokalizacji alternatywnej.

[20] Tj. zespołu składającego z się zgodnie z PBI z: Burmistrza, Skarbnika oraz Sekretarza Gminy, Administratora Systemów Informatycznych a także kadry kierowniczej Urzędu (w tym m.in. Komendanta Straży Miejskiej, Inspektora Ochrony Danych).

[21] Tj. 5 stycznia i 10 czerwca.

[22] Zmiana na stanowisku Inspektora Ochrony Danych.

[23] Zmiana nazwy komórki organizacyjnej UM.

[24] Zarządzeniami Burmistrza Świecia nr 455/2020 z 16 marca 2020 r. oraz 1647/23 z 16 sierpnia 2023 r.

[25] W PBI wskazano, że ASI dba, by zasoby te były sprawne, używane zgodnie z przeznaczeniem, przez osoby uprawnione, spełniały wymagania określone w przepisach, wymagania licencyjne, były na bieżąco aktualizowane, umieszczone w ewidencjach, były jak najmniej podatne na zagrożenia integralności, poufności, dostępności przetwarzanej informacji.

[26] Zespołu powołanego (zgodnie z PBI) do definiowania kierunku i działań i udzielania wsparcia dla inicjatyw w dziedzinie bezpieczeństwa informacji. Do zadań Forum należało m.in. ustanawianie zasad i celów

- dokonywanie zakupu sprzętu i materiałów komputerowych zleconych przez Sekretarza,
- wdrażanie i nadzorowanie polityki antywirusowej,
- przeciwdziałanie dostępowi osób niepowołanych do systemów informatycznych,
- doradzanie użytkownikom systemów komputerowych w zakresie bezpieczeństwa.

W zakresie wykonywanych obowiązków ASI podlegał bezpośrednio Burmistrzowi.

Dodatkowo Gmina zawarła umowy na usługi konserwacyjno-naprawcze sprzętu komputerowego, korzystanie z usług systemu BIPLO[27] oraz wykonywanie nadzoru autorskiego nad zainstalowanymi systemami informatycznymi[28].

(akta kontroli str. 118, 182-183, 227, 230, 233-234, 274, 353-355)

1.10. Zgodnie z art. 8 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[29] w zw. z art. 37 ust. 1 lit a RODO w okresie objętym kontrolą, w UM wyznaczono inspektorów ochrony danych[30] (dalej: „IOD"). W każdym przypadku funkcję tę powierzano osobom niebędącymi pracownikami Urzędu[31], a zakres ich obowiązków określano m.in. w umowach na świadczenie usług. W pierwszym przypadku zleceniobiorca oświadczył, że spełnia wymagania art. 37 ust. 5. W drugim przypadku osoba wyznaczona ukończyła studia podyplomowe w zakresie Ochrony Danych Osobowych w Praktyce oraz posiadała certyfikaty: audytora wewnętrznego systemu zarządzania bezpieczeństwem informacji ISO 27001:2013 oraz eksperta ds. ryzyka w ochronie informacji.

(akta kontroli str. 274-315)

1.11. W Urzędzie, stosowanie do wymogów art. 38 ust. 3 RODO, umożliwiono IOD wykonywanie obowiązków w sposób niezależny, a w ich działalności nie występował konflikt interesów. W zakresie pracy merytorycznej podlegali oni bezpośrednio Burmistrzowi[32]. Pełniący te obowiązki od 16 sierpnia 2023 r. zleceniobiorca sprawował także funkcję Pełnomocnika ds. Ochrony Informacji Niejawnych.

(akta kontroli str. 183, 274, 307)

1.12. Zarządzeniem z 5 października 2021 r. Burmistrz wyznaczył osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie związanym z realizacją przez UM zadań publicznych zależnych od systemu informacyjnego i systemu teleinformacyjnego wraz z przetwarzanymi w nim danymi w postaci elektronicznej. Jej dane przekazano do Zespołu Reagowania na Incydentu Bezpieczeństwa Komputerowego prowadzonego przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy (dalej: „NASK") z opóźnieniem, tj. 18 sierpnia 2022 r., co szerzej opisano w sekcji Stwierdzone nieprawidłowości.

(akta kontroli str. 227-232, 241)

1.13. Wprowadzona w UM PBI nie definiowała wymogów odnośnie sporządzenia dokumentów wykonawczych. Wszystkie dokumenty, do których się odwoływała

---

bezpieczeństwa informacji, przegląd PBI, monitorowanie istotnych zmian dla zagrożeń systemów informatycznych,

[27] Umożliwiającego prowadzenie strony BIP Urzędu.

[28] Nad 15 programami, z obowiązkiem dostarczania nowych wersji wynikających ze zmian przepisów oraz wprowadzanych przez autorów oprogramowania ulepszeń.

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

[30] Tj. zarządzeniami Burmistrza Świecia nr 455/2020 z 16 marca 2020 r. oraz 1647/23 z 16 sierpnia 2023 r.

[31] Prowadzącym działalność gospodarczą.

[32] W strukturze organizacyjnej UM IOD wyodrębniony był jako oddzielne stanowisko podlegające bezpośrednio Burmistrzowi.

stanowiły załączniki do dokumentu głównego. Wraz z PBI w Urzędzie sporządzono i wdrożono:

- Arkusz analizy ryzyka z klasyfikacją kontrolą aktywów, metodyką wyliczania i oceny ryzyk, planem postępowania oraz listą podatności i potencjalnych zagrożeń,
- Plany awaryjne odtworzenia systemy informatycznego po awarii krytycznej,
- Plan ciągłości działania na wypadek pożaru,
- Regulamin korzystania z urządzeń mobilnych,
- Regulamin korzystania z przeglądarek internetowych,
- Regulamin korzystania z poczty elektronicznej,
- Regulamin publikowania informacji w Internecie.

(akta kontroli str. 147-162)

1.14. UM posiadał informacje o zasobach informatycznych obejmujące ich rodzaj i konfigurację. W kontrolowanym okresie nie korzystano z oprogramowania wspierającego inwentaryzację sprzętu. Prowadzono ją w układzie tabelarycznym w osobnych zestawieniach. Dane o zasobach i konfiguracji urządzeń ujmowano też w ewidencji środków trwałych ze wskazaniem osób za nie odpowiedzialnych.

Burmistrz wskazał, że ASI dokonuje aktualizacji wykazu zasobów informatycznych dopisując i usuwając urządzenia wraz ze wskazaniem poszczególnych pracowników, którym oddano je na stan.

Oględziny 15 urządzeń[33] potwierdziły aktualność danych zawartych w ewidencjach i kartach środków trwałych.

(akta kontroli str. 241, 246-271)

1.15. Urząd przystąpił do rządowego programu „Cyberbezpieczny Samorząd". We wniosku złożonym 11 grudnia 2023 r. wskazano, że potrzeba realizacji projektu wynikała m.in. z konieczności rozbudowy zasobów (sprzętu i oprogramowania[34]) oraz poprawy kompetencji pracowników. Zakres rzeczowy projektu dotyczył wyłącznie obszaru technicznego. Przewidywał zakup trzech serwerów wraz z oprogramowaniem oraz Teleinformatycznego Systemu Zarządzania Bezpieczeństwem Informacji. Łączne wydatki miały wynieść 413,4 tys. zł., z czego dofinansowanie 359,7 tys. zł a wkład własny – 53,7 tys. zł.

Projekt zakładał osiągnięcie m.in. następujących wskaźników:

- liczba pracowników IT wykonujących zadania publiczne objętych wsparciem szkoleniowym – 2,
- liczba pracowników niebędących IT wykonujących zadania publiczne objętych wsparciem szkoleniowym – 28,
- liczba systemów służących poziomu zwiększeniu bezpieczeństwa informacji – 1,
- liczba użytkowników nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych – 97.

Umowa o powierzenie grantu[35] pomiędzy Skarbem Państwa[36] a Gminą została podpisana 19 lipca 2024 r. Gmina jako grantobiorca zobowiązała się zrealizować projekt w ciągu 24 miesięcy od dnia wejścia w życie umowy[37], ale nie dłużej niż do

---

[33] Tj. 10 komputerów, jednego serwera, dwóch laptopów, routera i jednej drukarki

[34] Wskazano, że UM nie posiada sprzętu do zabezpieczenia ciągłości pracy m.in. odpowiednich serwerów (które pracują na maksimum swoich możliwości), a wiele czynności związanych z inwentaryzacją sprzętu jest robione „ręcznie", co zabiera dużo czasu i może być obarczone błędami.

[35] Nr FERC.02.02-CS.01-001/23/0866/FERC.02.02-CS.01-001/23/2024.

[36] W imieniu którego działało Centrum Projektów Polska Cyfrowa z siedzibą w Warszawie.

[37] Tj. zgodnie z § 19 ust. 4 umowy z dniem podpisania przez ostatnią ze stron.

30 czerwca 2026 r. Pomiar poprawy cyberbezpieczeństwa w związku z realizacją Programu przewidziano jako porównanie planowanych zakresów zmian do stanu zrealizowanego, zgodnie z układem tzw. Ankiety dojrzałości.

7 sierpnia 2024 r. Gmina wystąpiła z wnioskiem o wypłatę przyznanej dotacji w formie jednej transzy. 14 sierpnia 2024 r. otrzymała informację o pozytywnym rozpatrzeniu wniosku. Zgodnie z umową dofinansowanie powinno zostać wypłacone w ciągu 60 dni kalendarzowych od zawarcia umowy, pod warunkiem dostarczenia poprawnie wypełnionej ankiety dojrzałości.

(akta kontroli str. 372-425)

Stwierdzone nieprawidłowości

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

1. W Urzędzie nierzetelnie sporządzono zestawienie systemów teleinformatycznych używanych do realizacji zadań publicznych, ponieważ pominięto w nim informatyczny system Wsparcia Organów Wyborczych, wykorzystywany przez pracowników Urzędu Stanu Cywilnego.

(akta kontroli str. 240, 242-245,486-489, 537)

ASI wyjaśnił, że system ten uruchamiany jest w przeglądarkach internetowych, jego baza nie znajduje się na serwerach Urzędu. Z systemu korzysta się tylko w akcjach wyborczych.

(akta kontroli str. 579)

NIK zauważa, że system Wsparcia Organów Wyborczych, nawet jeśli nie jest wykorzystywany na bieżąco, służy do realizacji zadań publicznych i analogicznie jak w przypadku pozostałych powinno określić się dla niego skalę krytyczności dla funkcjonowania Urzędu i poziom jego ochrony

2. W Urzędzie nie powołano pełnomocnika do spraw bezpieczeństwa informacji mimo wymogu wynikającego z § 3 ust. 1 pkt 2 zarządzenia SZBI.

(akta kontroli str. 106-107, 447)

Działając z upoważnienia Burmistrza Sekretarz Gminy wyjaśnił, że w PBI wyznaczono osoby odpowiedzialne za proces zabezpieczenia informacji.

(akta kontroli str. 447)

NIK zauważa, że ustanowienie SZBI w Urzędzie, zgodnie z przywołanym zarządzeniem Burmistrza, obejmowało obok sporządzenia i wdrożenia odpowiednich dokumentów, także powołanie pełnomocnika ds. bezpieczeństwa informacji. Do zadań Burmistrza związanych z należytym wdrożeniem SZBI należało określenie zakresu jego zadań oraz trybu działania.

3. Zgłoszenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa do Zespołu Reagowania na Incydentu Bezpieczeństwa Komputerowego NASK, dokonano z naruszeniem 14 dniowego terminu określonego w art. 22 ust. 1 pkt 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[38]. Zarządzeniem z 5 października 2021 r. Burmistrz wyznaczył ASI do tej roli, jednak informacje w tym zakresie zostały przekazane do NASK dopiero 18 sierpnia 2022 r. tj. po 317 dniach.

(akta kontroli str. 227-229)

Burmistrz wyjaśnił, że wynikało to z przeoczenia pracownika zobowiązanego do dokonania zgłoszenia.

(akta kontroli str. 241)

[38] Dz. U. z 2024 r. poz. 1077, dalej: „ustawa o KSC".

4. Opracowane w Urzędzie plany ciągłości działania oraz plany odtworzeniowe nie były, w okresie objętym kontrolą, testowane, co było niezgodne z pkt 23 ppkt 3 PBI, który zobowiązywał ASI do testowania rożnych scenariuszów przywracania działalności Urzędu, symulacji po wystąpieniu incydentów bezpieczeństwa lub sytuacji kryzysowych czy przeprowadzania testów odtworzeniowych i prób generalnych, w celu weryfikacji czy Urząd radzi sobie z przerwami w działaniu.

(akta kontroli str. 124, 238, 240, 577)

ASI wyjaśnił, że plany ciągłości oraz plan awaryjny nie zostały testowane w praktyce z uwagi na bardzo delikatną materię jaką jest oprogramowanie.

(akta kontroli str. 579)

NIK zauważa, że w przypadku planu zapewnienia ciągłości działania oraz planów odtworzeniowych istotne jest ich cykliczne testowanie w celu uzyskania potwierdzenia, że w sytuacji wystąpienia incydentu ciągłości działania zadziałają one prawidłowo. Tylko takie działanie, odpowiednio udokumentowane, pozwala bowiem na zidentyfikowanie słabych punktów i skuteczne ich eliminowanie.

OCENA CZĄSTKOWA

W Urzędzie opracowano i wdrożono SZBI oraz zapewniono aktualność dokumentów i polityk wchodzących w jego skład. Pracowników zapoznano z treścią tych dokumentów. Umożliwiono IOD wykonywanie obowiązków w sposób niezależny.

Burmistrz nie powołał jednak pełnomocnika do spraw bezpieczeństwa informacji, który miał być jednym z elementów SZBI, a zgłoszenia do NASK osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa dokonano z naruszeniem ustawowego terminu. Przyjęte w UM plany zapewnienia ciągłości działania oraz plany odtworzeniowe nie były testowane, przez co ich praktycznej skuteczności nie można było zweryfikować.

OBSZAR

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

Opis stanu faktycznego

2.1. W Urzędzie zapobiegano możliwości zainstalowania nieautoryzowanego oprogramowania na komputerach stacjonarnych i laptopach przez użytkowników systemów informatycznych, zgodnie z § 19 ust. 2 pkt 4 rozporządzenia KRI. Uprawnienia użytkowników 10 komputerów[39] objętych oględzinami nie pozwalały na zainstalowanie nieautoryzowanego oprogramowania. Przy próbie instalacji każdorazowo pojawiał się komunikat o konieczności podania loginu i hasła administratora.

Wykorzystywane w urzędzie tablety i smartfony nie zostały zabezpieczone przed instalacją przez użytkownika dowolnego oprogramowania. ASI wyjaśnił, że smartfony służyły jedynie do komunikowania się z petentami Urzędu oraz współpracownikami i nie były na nich przetwarzane dane. Tablety wykorzystywane były przez radnych do głosowania na sesjach.

(akta kontroli str. 135, 139, 317-318, 444, 446, 579-580)

2.2. Analiza zakresów obowiązków, uprawnień i odpowiedzialności 15 pracowników Urzędu[40] wykazała, że wszyscy, zgodnie z § 19 ust. 2 pkt 4 rozporządzenia KRI,

[39] Badaniem objęto pięć komputerów stacjonarnych oraz pięć komputerów przenośnych. Wyboru dokonano z uwzględnieniem aktualnej dostępności pracowników Urzędu (posiadających na wyposażeniu komputery przenośne) oraz sąsiadującej lokalizacji pomieszczeń (w których znajdowały się komputery stacjonarne).

[40] W tym siedmiorga na stanowiskach kierowniczych oraz dwojga pracowników, którzy w okresie objętym kontrolą zmienili komórkę organizacyjną.

uczestniczyli w procesie przetwarzania informacji w stopniu adekwatnym do realizowanych przez nich zadań.

(akta kontroli str. 490-534, 584-586)

2.3. W okresie objętym kontrolą[41] czworo pracowników zakończyło pracę w Urzędzie. Przeprowadzone oględziny wykazały, że w każdym przypadku ich dostęp do systemów informatycznych został zablokowany. Administrator Systemów Informatycznych wskazał, że dostępne w Urzędzie oprogramowanie nie pozwalało jednak na dokładne określenie czasu w jakim konta użytkowników zostały zablokowane. Podkreślił, że robił to niezwłocznie o otrzymaniu informacji o ustaniu ich stosunku pracy. O ich odejściu z pracy dowiadywał się od pracowników kadr Urzędu, w każdym przypadku uczestniczył też w rozliczeniu z powierzonego sprzętu informatycznego[42]. Było to zgodne z§ 19 ust. 2 pkt 5 rozporządzenia KRI.

(akta kontroli str. 25, 429, 432)

2.4. W celu zapewnienia ochrony systemów informatycznych przed nieuprawnionym dostępem, w PBI określono podstawowe zasady bezpieczeństwa informacji[43], politykę haseł oraz zabezpieczenia informatyczne[44]. W polityce haseł określono ich złożoność[45], zasady przechowywania, okresy w jakich podlegają one zmianom, a także zakazy dotyczące ich formułowania[46]. Komputery z systemem operacyjnym Windows były zarządzane centralnie w oparciu o mechanizm Microsoft Active Directory, w którym złożoność haseł była zapewniona formułą oprogramowania[47].

Oględziny sposobu logowania do systemu operacyjnego oraz trzech systemów informatycznych zarządzanych przez Urząd[48] wykazały, że stosowano metody uwierzytelniania dostępu. Hasła dostępu pracowników odpowiadały wymogom określonym w PBI i podlegały okresowym zmianom. Nie następowało automatyczne logowanie do komputerów i systemów bez wprowadzenia hasła.

Nie wystąpiły przypadki loginów, których nazwa nie pozwalała na bezpośrednie powiązanie z daną osobą.

(akta kontroli str. 129, 573)

2.5. Oględziny pięciu stanowisk komputerowych służących do załatwiania spraw z zakresu ewidencji ludności i dowodów osobistych, spraw meldunkowych, rejestracji urodzeń, małżeństw i zgonów a także wydawania odpisów i zaświadczeń dotyczących stanu cywilnego, wykazały, że monitory na tych stanowiskach były ustawione w taki sposób, że wyświetlane na nich dane nie były widoczne dla osób nieuprawnionych, co było zgodne z § 19 ust. 2 pkt 7 rozporządzenia KRI.

(akta kontroli str. 320-323)

2.6. W Urzędzie, zgodnie § 19 ust. 2 pkt 8 rozporządzenia KRI, ustanowiono zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość. Zarządzeniem Burmistrza[49] wprowadzono regulamin oraz instrukcję bezpiecznej

---

[41] Do 2 lipca 2024 r. tj. dnia przeprowadzenia oględzin.
[42] Podpisywał tzw. obiegówkę.
[43] Tj. 17 zasad wraz z opisem w tym np.: wiedzy koniecznej, świadomości zbiorowej, monitoringu, asekuracji, czystego ekranu.
[44] W tym np. procedury eksploatacyjne, zasady zabezpieczenia: sieci, sprzętu komputerowego i innych urządzeń informatycznych, systemów operacyjnych, aplikacji, baz danych.
[45] Tj. wymogi minimalne dla tworzenia hasła.
[46] Np. zabroniono tworzenia haseł na podstawie cech i numerów osobistych, identyfikatora użytkownika, popularnych wyrażeń językowych.
[47] Nie pozwalała ona na stworzenie hasła niespełniającego wymogów określonych w PBI.
[48] Wybranych celowo według osądu kontrolera.
[49] Nr 815/21 z 29 marca 2021 r.

i higienicznej pracy zdalnej. Zgodnie z regulaminem pracownicy byli zobowiązani do korzystania z urządzeń elektronicznych wyłącznie do wykonywania pracy, z zachowaniem wszelkich obowiązujących u pracodawcy zasad ich użytkowania. Zobowiązani byli do zabezpieczenia przed zniszczeniem sprzętu służbowego oraz pozyskaniem danych i informacji przez osoby postronne. W regulaminie określono zasady:

- przechowywania, transportu, zabezpieczenia dokumentów zawierających dane osobowe (których administratorem był pracodawca) w warunkach pracy zdalnej,
- przetwarzania dokumentów zawierających dane osobowe,
- konfigurowania domowej sieci WiFi w sposób minimalizujący ryzyko włamania.

Zarządzenie zostało opublikowane w Biuletynie Informacji Publicznej Urzędu[50].

(akta kontroli str. 340-352)

2.7. Sekretarz Gminy wskazał, że laptopy służbowe pracowników Urzędu były zabezpieczone w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym, poprzez wymóg logowania się do ich systemu operacyjnego indywidualnym loginem i hasłem. Dodał, że pracownicy nie przechowują na nich danych wrażliwych.

Poinformował także, Urząd nie posiada i nie stosuje specjalnego oprogramowania odpowiedzialnego za szyfrowanie danych zgormadzonych na dyskach twardych komputerów przenośnych. Działanie takie było zgodne z § 19 ust. 2 pkt 9 i 11 rozporządzenia KRI.

(akta kontroli str. 446)

2.8. Realizując wymóg § 19 ust. 2 pkt 9 rozporządzenia KRI w Urzędzie 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 (klimatyzator), UPS, urządzenia gaśnicze do sprzętu elektronicznego.

(akta kontroli str. 436-443)

2.9. W umowach zawieranych z podmiotami zewnętrznymi[51] zawierano zapisy gwarantujące bezpieczeństwo informacji stosownie do § 19 ust. 2 pkt 10 rozporządzenia KRI i pkt 32 PBI. Wykonawców zobowiązywano do zachowania w tajemnicy i nieudostępniania przekazywanych danych, do których uzyskali dostęp w ramach wykonywania umów, stosowania środków technicznych i organizacyjnych dla zapewnienia bezpieczeństwa powierzonych informacji, wyłączenia możliwości korzystania z usług podwykonawców bez zgody Gminy.

(akta kontroli str. 130, 353-355, 364-371, 462-467)

2.10. W PBI wskazano, że przy naprawach i konserwacjach sprzętu dokonywanych przez podmioty trzecie poza obszarem bezpiecznym[52] stosuje się przepisy właściwe dla nośników przenośnych, w szczególności istnieje obowiązek szyfrowania informacji zgromadzonych w pamięci masowej naprawianych urządzeń.

---

[50] Por. https://bip.swiecie.eu/zarzadzenie/5812/zarzadzenie-nr-815-21 (dostęp 30 lipca 2024 r.).

[51] Badaniem objęto cztery umowy: świadczenie usług serwisowych, korzystanie z usług systemu BIPLO oraz dwie dotyczące nadzoru autorskiego nad oprogramowaniem.

[52] W PBI dokonano podziału pomieszczeń Urzędu (i budynku Urzędu Stanu Cywilnego) na obszary i wyznaczono granice obszaru bezpiecznego (np. pomieszczenia biurowe, sale konferencyjne) i podwyższonego bezpieczeństwa (np. sekretariat Burmistrza oraz Kierownika USC, serwerownia, archiwum zakładowe).

Umowa na usługi konserwacyjno-naprawcze sprzętu komputerowego[53] Urzędu przewidywała wykonywanie czynności w trybie konserwacji ciągłej na podstawie książki konserwacji sprzętu komputerowego.

Sekretarz Gminy wskazał, że w okresie objętym kontrolą nie przekazywano sprzętu podmiotom zewnętrznym w celu wykonania napraw.

(akta kontroli str. 134, 353, 446)

2.11. W ramach zapewnienia ciągłości działania Urzędu ustalono zasady przechowywania kopii zapasowych. W PBI z 2016 r. wskazano, że próba odtworzeniowa wybranej kopii powinna być wykonywana nie rzadziej niż raz w miesiącu, a w cyklu kwartalnym powinno się testować wszystkie kopie zapasowe. W PBI z 2023 r. wskazano, że wykonywanie kopii zapasowych powinno odbywać się według Planu archiwizacji i wykonywania kopii zapasowych. Określono w nim, dla 17 programów wykorzystywanych w UM, lokalizację oryginału bazy danych, lokalizację jej kopii, a także metodę[54] i częstotliwość wykonywania kopii. Za proces ich tworzenia odpowiadał ASI.

ASI wskazał, że kopie lokalne systemów wykonywane są codziennie, a dodatkowo jeden raz w tygodniu wykonywana jest kopia zapisywana następnie na dysku zewnętrznym. Oględziny potwierdziły, że nośnik z kopią przechowywany był w sejfie poza miejscem wytwarzania danych, zapisane kopie odpowiadały wymogom ustalonym w PBI w zakresie metody oraz częstotliwości wykonywania.

(akta kontroli str. 68,161-162, 426-428, 587-588)

2.12. W raporcie z audytu bezpieczeństwa informacji przeprowadzonego w sierpniu 2022 r.[55] wskazano, że w Urzędzie nie przyjęto wytycznych dotyczących testowania kopii zapasowych. Zarekomendowano zarazem regularne wykonywanie testów odtwarzania systemu i aplikacji z backupu oraz ich dokumentowanie. W Urzędzie nie przeprowadzano jednak regularnych testów kopii zapasowych danych i oprogramowania aplikacyjnego, w którym przetwarzane są dane, co szerzej opisano w sekcji Stwierdzone nieprawidłowości.

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

(akta kontroli str. 426-428, 555, 577, 579)

2.13. W PBI wskazano, że pracownicy, którym powierzono środki przetwarzania informacji, systemy i zasoby informacyjne zobowiązani są do monitorowania pojemności tych systemów i zasobów oraz prognozowania przyszłych wymagań odnoszących się do nich. ASI wskazał, że Urząd nie posiada specjalnego programu do weryfikacji pojemności nośników pamięci serwerów, jednak on sam dokonuje tego na bieżąco. Oględziny trzech serwerów[56] wykazały, że wolna przestrzeń na ich dyskach wynosiła 26%, 47% oraz 72%.

(akta kontroli str. 127, 133, 449-450)

2.14. Sekretarz Gminy wskazał, że w Urzędzie nie zostały zidentyfikowane kluczowe elementy infrastruktury i usługi IT oraz ich zabezpieczenie pod kątem wpływu czynników zewnętrznych, co szerzej opisano w sekcji Stwierdzone nieprawidłowości.

W Urzędzie stosowano jednak narzędzia w celu ograniczenia wpływu czynników zewnętrznych mogących zakłócić ciągłości działania. Elementy infrastruktury informatycznej były podtrzymywane przez UPS, zastosowano zaporę sieciową oraz

---

[53] Zawarta w sierpniu 2022 r. z podmiotem zewnętrznym.

[54] W każdym przypadku (16) posiadania bazy danych na serwerze UM – metoda - „pełna", częstotliwość – „codziennie".

[55] Audyt przeprowadzony przez Centrum Bezpieczeństwa Informatycznego z siedzibą w Krasnymstawie.

[56] Tj. serwerów fizycznych SRV_HV1, SRV_HV2 oraz QNAP_Backup.

środki ochrony przed szkodliwym oprogramowaniem. Okablowanie było zabezpieczone przed celowym lub przypadkowym uszkodzeniem. Sprzęt informatyczny podlegał przeglądom i konserwacjom. W Urzędzie stosowano określoną w PBI politykę dostępu do kluczy.

Dodatkowo w związku z realizacją projektu grantowego „Cyberbezpieczny Samorząd" zaplanowano rozwiązania, które pozwolą utrzymać ciągłość działania tj. zwiększenie liczby serwerów (w tym maszyn wirtualnych), wyposażenie ich w konsolę antywirusową i konsolę kopii zapasowych, system monitorujący sieć.

(akta kontroli str. 372-373, 436-437, 446, 589)

Stwierdzone nieprawidłowości

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

1. W okresie objętym kontrolą w Urzędzie nie testowano regularnie utworzonych kopii zapasowych danych i oprogramowania, co uznać należy za nierzetelne. W PBI wskazano, że do zadań ASI należało m.in. regularne wykonywanie lub zlecanie testów i audytów w celu potwierdzenia skuteczności istniejących zabezpieczeń[57].

(akta kontroli str. 118, 577)

ASI wskazał, że w okresie objętym kontrolą dwukrotnie dokonano przywrócenia danych z kopii zapasowych na zlecenia organów kontroli[58]. Wyjaśnił zarazem, że z operacji wykonanej w 2023 r. nie sporządzono dokumentacji przez przeoczenie pracownika.

(akta kontroli str.579)

NIK zauważa, że testowanie polega na sprawdzeniu czy wykonana kopia zapasowa nie zawiera błędów a dane zostaną odtworzone w sposób prawidłowy. Procedury odtwarzania powinny być regularnie testowane, aby można było polegać na sporządzonych kopiach w przypadku konieczności awaryjnego odtworzenia.

2. W Urzędzie nie zidentyfikowano kluczowych elementów infrastruktury i usługi IT oraz ich zabezpieczenia pod kątem wpływu czynników zewnętrznych, co uznać należy za nierzetelne.

(akta kontroli str. 145-146, 444, 581)

Sekretarz Gminy przyznał, że nie dokonano identyfikacji zabezpieczeń elementów infrastruktury i usługi informatycznych pod kątem wpływu na nie czynników zewnętrznych. Podkreślił, że w Urzędzie wykonywane są codziennie kopie zapasowe baz danych i w przypadku ingerencji czynników zewnętrznych możliwe jest odtworzenie zasobów serwerowych.

ASI wskazał, że identyfikacja kluczowych elementów infrastruktury informatycznej i potencjalnych zagrożeń zostanie przeprowadzona w grudniu 2024 r.

(akta kontroli str. 446, 580)

NIK zauważa, że zarządzanie ciągłością działania ma na celu zapewnienie, że infrastruktura i usługi IT będą mogły być odtworzone do wcześniej zdefiniowanych poziomów. Z tego względu istotne jest zidentyfikowanie kluczowych dla pracy Urzędu elementów infrastruktury informatycznej, jak i usług informatycznych. Bez zdefiniowania tych kwestii nie jest możliwe skuteczne przywrócenie infrastruktury i usług IT w sytuacji wystąpienia zakłócenia ciągłości działania.

OCENA CZĄSTKOWA

W celu zapewnienia ochrony systemów informatycznych przed nieuprawnionym dostępem, w PBI określono i stosowano podstawowe zasady bezpieczeństwa informacji, politykę haseł oraz zabezpieczenia informatyczne. Pracownicy

[57] Por. pkt 11 ppkt 3 PBI dotyczący zadań i obowiązków ASI.
[58] Tj. NIK oraz Regionalnej Izby Obrachunkowej w Bydgoszczy.

uczestniczyli w procesie przetwarzania informacji w stopniu adekwatnym do realizowanych przez nich zadań, zaś po zakończeniu zatrudnienia wyłączano ich dostęp do systemów informatycznych. Wprowadzono środki organizacyjne, fizyczne i techniczne w celu zabezpieczenia informacji znajdujących się na serwerach. Określono zasady pracy zdalnej. W umowach zawieranych z podmiotami zewnętrznymi zawierano zapisy gwarantujące bezpieczeństwo informacji. W ramach zapewnienia ciągłości działania Urzędu ustalono i stosowano zasady tworzenia i przechowywania kopii zapasowych.

W Urzędzie nie przeprowadzano jednak regularnych testów tych kopii oraz nie zidentyfikowano kluczowych elementów infrastruktury i usług IT oraz ich zabezpieczeń pod kątem wpływu czynników zewnętrznych.

OBSZAR

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

3.1. W PBI sformułowano procedurę zarządzania ryzykiem oraz prowadzenia okresowych analiz bezpieczeństwa informacji[59]. Określono także sposób dokumentowania tych analiz[60]. Aktywa Urzędu podzielono na siedem kategorii[61], dla których wyznaczono katalogi możliwych zagrożeń i podatności[62]. Opracowano także metodykę wyliczania i oceny ryzyk (prawdopodobieństwa ich wystąpienia) oraz warianty postępowania z ryzykami (w tym wybór zabezpieczeń).

Sekretarz Gminu wskazał, że w Urzędzie prowadzono raz w roku analizy utraty integralności, dostępności lub poufności informacji, o której mowa w § 19 ust 2 pkt 3 rozporządzenia KRI. Nie zostały one jednak udokumentowane w sposób określony w PBI, co szerzej opisano w sekcji Stwierdzone nieprawidłowości.

Analiza w tym zakresie została przeprowadzona także w związku z przygotowaniem ankiety cyberbezpieczeństwa w ramach konkursu grantowego Cyberbezpieczny Samorząd.

(akta kontroli str. 122,147-154, 411-420, 446)

3.2. W Urzędzie ustanowione zostały zasady zarządzania incydentami związanymi z bezpieczeństwem informacji, w szczególności w systemach informacyjnych. W PBI określono typowe zagrożenia bezpieczeństwa informacji oraz danych osobowych, a także obowiązki pracowników w zakresie ich zgłaszania oraz sposoby reagowania na incydenty. Opracowano także procedury dotyczące podejmowania działań korygujących i zapobiegawczych. 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 KRI

Sekretarz Gminy oraz ASI wskazali, że w okresie objętym kontrolą nie wystąpiły przypadki incydentów z zakresu naruszenia bezpieczeństwa informacji.

(akta kontroli str. 77-79, 122-125, 446, 579)

3.3. W UM wprowadzono Politykę Szkoleniową[63] w celu podnoszenia poziomu wiedzy, umiejętności kwalifikacji zawodowych pracowników w celu zapewnienia efektywnej i profesjonalnej realizacji zadań służbowych. Określono w niej zasady dotyczące analizy potrzeb szkoleniowych a także realizacji, oceny i dokumentowania szkoleń.

---

[59] Które definiowano jako zachowanie integralności, poufności i dostępności informacji.
[60] Tj. formularz Arkusza analizy ryzyka.
[61] Tj. dokumenty, media, outsourcing, oprogramowanie, infrastruktura IT, infrastruktura (obiekty), pracownicy i współpracownicy.
[62] Od trzech do 15.
[63] Zarządzeniem Burmistrza nr 1596/23 z 27 czerwca 2023 r.

W okresie objętym kontrolą w Urzędzie nie przeprowadzono szkoleń z zakresu przetwarzania informacji, co szerzej opisano w sekcji Stwierdzone nieprawidłowości. W listopadzie 2023 r. Sekretarz Gminy odbył szkolenie dotyczące ochrony danych osobowych[64].

W kartach zapotrzebowania na szkolenia w 2024 r. kierownicy komórek organizacyjnych UM wskazali m.in.: przestrzeganie zasad cyberbezpieczeństwa (na listopad) oraz przestrzeganie zasad w zakresie ochrony danych osobowych (na wrzesień), w których ma wziąć udział 100 pracowników Urzędu. Dodatkowo zaplanowano szkolenia dotyczące udzielania informacji publicznej (dla trzech osób) oraz wdrożenia i funkcjonowania Elektronicznego Zarządzania Dokumentacją – eZD (dla 20 osób). Wydział Gospodarki Odpadami i Gospodarki Wodno-Ściekowej zawnioskował także o szkolenie online (dla pięciorga swoich pracowników) w zakresie skutecznych metod ochrony przed atakami komputerowymi. Do czasu zakończenia kontroli szkolenia te nie zostały zorganizowane.

(akta kontroli str. 227, 324-339, 451-459)

W styczniu 2024 r. zespół audytujący przedłożył Burmistrzowi sprawozdanie z audytu bezpieczeństwa informacji w UM[65]. Jego zakresem objęto:

1) wymianę informacji w postaci elektronicznej, w tym współpracę z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną,
2) zarządzanie bezpieczeństwem informacji w systemach teleinformatycznych,
3) zapewnienie dostępności informacji zawartych na stronach internetowych Urzędu dla osób z niepełnosprawnościami.

W skład zespołu audytującego poza audytorem wewnętrznym weszli także ASI oraz IOD bezpośrednio odpowiedzialni za te kwestie, co szerzej opisano w sekcji Stwierdzone nieprawidłowości.

W sprawozdaniu z audytu zawarto cztery zalecenia, tj.:

- przeszkolenie pracowników w zakresie podstaw cyberbezpieczeństwa,
- bieżącą aktualizację uprawnień pracowników w zakresie przetwarzania informacji,
- bieżącą aktualizację systemów teleinformatycznych,
- bieżącą aktualizację bazy sprzętu informatycznego oraz systematyczną wymianę sprzętu niedającego rękojmi bezpieczeństwa informacji.

Do sprawozdania dołączono zestawienie systemów teleinformatycznych używanych do realizacji zdań publicznych oraz wykaz sprzętu komputerowego. Burmistrz wskazał, że poza przeszkoleniem pracowników, pozostałe zalecenia audytu zostały zrealizowane.

(akta kontroli str. 227, 468-489)

Stwierdzone nieprawidłowości

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

1. Prowadzone w okresie objętym kontrolą analizy ryzyka nie zostały udokumentowane zgodnie z pkt 20 PBI poprzez wypełnienie Arkusza analizy ryzyka. W związku z tym Urząd nie posiadał sformalizowanych wyników dotyczących identyfikacji ryzyka, jego analiz i oceny (w tym określenia poziomu ryzyka) oraz rekomendacji postępowania koniecznych do sformułowania planu postępowania z ryzykiem.

(akta kontroli str. 122, 147-154, 581)

---

[64] Zorganizowane przez IOD.

[65] Zadanie nr 3/2023, sprawa znak: AW.1720.3.2023. W 2022 r. przeprowadzenie audytu zlecono podmiotowi zewnętrznemu.

odpowiedniego przygotowania się do realizacji zadania, w tym zapoznania się audytowanym obszarem, stosowanymi procedurami i wynikami audytów poprzednich.

OCENA CZĄSTKOWA

W Urzędzie opracowano procedurę zgłaszania i postępowania z incydentami naruszenia bezpieczeństwa informacji. Prowadzono analizy ryzyka utraty integralności, dostępności lub poufności informacji, jednak nie udokumentowano ich wyników zgodnie z zasadami określonymi w PBI. Pracownikom zaangażowanym w proces przetwarzania informacji nie zapewniono szkoleń z zakresu cyberbezpieczeństwa. Przeprowadzono audyt wewnętrzny w zakresie bezpieczeństwa informacji, jednak z uwagi na powierzenie go pracownikom odpowiadającym za przedmiot audytu, pozbawiono go przymiotu niezależności i obiektywizmu.

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. Rzetelne identyfikowanie zbiorów danych Urzędu podlegających zabezpieczeniu.
2. Powołanie pełnomocnika do spraw bezpieczeństwa informacji.
3. Prowadzenie regularnych testów planów ciągłości i planów odtworzeniowych.
4. Prowadzenie regularnych testów tworzonych kopii zapasowych danych i oprogramowania.
5. Dokonanie identyfikacji kluczowych elementów infrastruktury i usług IT oraz ich zabezpieczeń pod kątem wpływu czynników zewnętrznych.
6. Dokumentowanie prowadzonych analiz ryzyka w zakresie bezpieczeństwa informacji.
7. Zorganizowanie szkoleń dla pracowników z zakresu bezpieczeństwa przetwarzania informacji.
8. Umożliwienie prowadzenia audytów w zakresie bezpieczeństwa informacji w sposób niezależny i obiektywny.

V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Delegatury NIK 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 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

Burmistrz przyznał, że analiza ryzyka nie została udokumentowana. Wskazał, że wszystkie sprawy w tym zakresie zostaną zrealizowane do końca 2024 r. Dodał, że powodem zwłoki były organizowane wybory parlamentarne i samorządowe, które w dużym stopniu zwiększyły obowiązki Sekretarza odpowiedzialnego za te kwestie.

(akta kontroli str. 583)

NIK zauważa, że aby skutecznie zarządzać SZBI konieczne jest przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji. Kluczowa rola tych analizy wynika z faktu, że rodzaj i poziom zastosowanych zabezpieczeń jest względny. Rodzaj zastosowanych zabezpieczeń technicznych jak i ich poziom powinien wynikać z regularnego szacowania ryzyka i być dokumentowany, tak by umożliwiać wdrożenie przyjętych zabezpieczeń oraz ewaluację ich wyników.

2. W Urzędzie okresie objętym kontrolą nie zorganizowano szkolenia osób zaangażowanych w proces przetwarzania informacji, czym naruszono § 19 ust. 2 pkt 6 rozporządzenia KRI (wcześniej § 20 ust. 2 pkt 6 rozporządzenia KRI z 2012 r.).

(akta kontroli str. 333-338, 460-461)

Burmistrz wyjaśnił, że pracownicy Urzędu mają dostęp do systemu informacji prawnej czy treści publikowanych przez Narodowy Instytut Cyberbezpieczeństwa. Dodał, że wszyscy pracownicy zaangażowani w proces przetwarzania informacji wezmą udział w szkoleniach z tego zakresu w IV kwartale 2024 r.

(akta kontroli str. 572)

3. W 2023 r. okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji przeprowadzony został m.in. przez pracowników odpowiadających za przedmiot audytu, co pozbawiło go przymiotu niezależności i obiektywizmu. Tym samym niewłaściwie zrealizowano wymóg określony § 20 ust. 2 pkt 14 rozporządzenia KRI z 2012 r.[66] Audyt dotyczący zarządzanie bezpieczeństwem informacji w systemach teleinformatycznych (w tym danych osobowych) przeprowadził zespół, w skład którego weszli zarówno ASI jak i IOD bezpośrednio odpowiedzialni za te kwestie. Taka forma audytu była też niezgodna z PBI, gdzie w pkt 25 wskazano, że przestrzegana jest zasada, że audytorzy nie audytują własnej pracy.

(akta kontroli str. 468-489, 574)

Burmistrz wyjaśnił, że podjęto taką decyzję kierując się m.in. wytycznymi Ministerstwa Finansów i Ministerstwa Cyfryzacji, zgodnie z którymi powierzając zadania powinno się brać pod uwagę czy pracownicy posiadają odpowiednie kwalifikacje, doświadczenie i znajomość metodyki prowadzenia audytu wewnętrznego, a w przeciwnym przypadku korzystać z pomocy ekspertów z wewnątrz lub zewnątrz jednostki.

(akta kontroli str. 575-576)

NIK zauważa, że podstawową wartością i celem audytu, na który zwrócił także uwagę zespół audytujący[67] było dostarczanie niezależnej i obiektywnej oceny funkcjonowania SZBI. W treści sprawozdania z audytu wskazano, że w podmiotową strukturę zarządzania informacjami wchodzą IOD oraz ASI. Powołanie ich do składu zespołu audytującego sprawiło, że w istocie dokonali oni sprawdzenia efektów własnej pracy. Zgodnie z PBI na wyznaczonym audytorze spoczywa obowiązek

---

[66] 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 9 września 2024 r.

[67] Por. cele audytu opisane w pkt I sprawozdania z audytu wewnętrznego z 28 grudnia 2023 r.

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, 18 września 2024 r.

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

Kontroler:
Michał Trempała
główny specjalista kontroli państwowej