NAJWYŻSZA IZBA KONTROLI
Delegatura w Katowicach

LKA.410.14.2.2024

Pan
Adam Wójcik
Burmistrz
Miasta Pyskowice
ul. Strzelców Bytomskich 3
44-120 Pyskowice

WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Katowicach
ul. Powstańców 29, 40-039 Katowice
T +48 32 784 42 00, F +48 32 784 42 30
lka@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miejski w Pyskowicach ul. Strzelców Bytomskich 3, 44-120 Pyskowice[1].
Kierownik jednostki kontrolowanej	Adam Wójcik, Burmistrz, od 26 października 2018 r.[2] (akta kontroli str. 5 – 6)
Zakres przedmiotowy kontroli	Rozwiązania organizacyjne i techniczne w zakresie zapewnienia bezpieczeństwa przetwarzania informacji oraz zapewnienia ciągłości działania w urzędzie i ich stosowanie.
Okres objęty kontrolą	Od 1 stycznia 2023 r. do dnia zakończenia kontroli, tj. do dnia 24 lipca 2024 r. (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 Katowicach
Kontrolerzy	1. Jerzy Piasecki, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LKA/118/2024 z dnia 22 maja 2024 r. 2. Szymon Gruca, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LKA/119/2024 z dnia 22 maja 2024 r. (akta kontroli str. 1 – 4)

[1] Zwany dalej: „Urzędem”.
[2] Zwany dalej „Burmistrzem”.
[3] Dz. U. z 2022 r. poz. 623, dalej: *ustawa o NIK*.

II. Ocena ogólna[4] kontrolowanej działalności

OCENA OGÓLNA

Urząd w latach 2023-2024 podejmował prawidłowe działania w zakresie opracowania i wdrożenia procedur mających na celu zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych.

Urząd, prawidłowo i rzetelnie wdrożył przyjęte rozwiązania organizacyjne w zakresie ochrony bezpieczeństwa informacji. Dostęp do pomieszczeń i systemów informatycznych był ograniczony jedynie do osób upoważnionych, a pomieszczenia serwerowni oraz systemy informatyczne miały wdrożone zabezpieczenia. Zidentyfikowano również kluczowe i podlegające ochronie elementy infrastruktury informatycznej. Testowano scenariusze postępowania w przypadku awarii infrastruktury teletechnicznej, jak i przywracanie danych z kopii zapasowych. Przy tworzeniu kopii zapasowych zbiorów danych ograniczono się do jedynie macierzy dyskowych pomimo, że obowiązujące procedury wymagały wykorzystania w tym zakresie również taśm magnetycznych, płyt CD, DVD.
Prowadzone były analizy ryzyka w zakresie zapewnienia ciągłości działania oraz przeprowadzono stosowne audyty w tym zakresie, prowadzono rejestr incydentów oraz dokumentację z tym związaną. Pracownicy Urzędu byli przeszkoleni w zakresie zapewnienia bezpieczeństwa informacji.

Terminowo zostały wyznaczone i zgłoszone osoby odpowiedzialne za utrzymanie kontaktów z podmiotami Krajowego Systemu Cyberbezpieczeństwa, a powołany Inspektor Ochrony Danych Osobowych[5], któremu zagwarantowano niezależność, posiadał niezbędne kwalifikacje do wykonywania swych zadań. W działalności IOD nie zachodził również konflikt interesów.

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

OBSZAR

1. Organizacja bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych

Opis stanu faktycznego

1.1. W okresie objętym kontrolą Urząd zidentyfikował zbiory informacji podlegające ochronie. W zbiorach tych wskazano grupy informacji podlegające ochronie, ocenę obszarów (poufność, dostępność i integralność), wymagania bezpieczeństwa oraz poziom ochrony. Zidentyfikowano 136 takich grup.

(akta kontroli str. 7 – 58)

1.2. W Urzędzie opracowano i wdrożono System Zarządzania Bezpieczeństwem Informacji i Ochrony Danych Osobowych[7], w rozumieniu w § 20 ust. 1 w związku z ust. 3 rozporządzenia KRI[8]. Obowiązujący w Urzędzie *system bezpieczeństwa* obejmował Politykę Systemu Zarządzania Bezpieczeństwem Informacji i Ochrony Danych Osobowych oraz procedury obejmujące, m.in. Procedurę ciągłości działania, Procedurę identyfikacji oraz zarządzania ryzykiem bezpieczeństwa aktywów

[4] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej. W niniejszym wystąpieniu zastosowano ocenę w formie opisowej.
[5] Dalej: „IOD" lub „IODO".
[6] Oceny cząstkowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena cząstkowa może być sformułowana jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej.
[7] Zarządzeniem Burmistrza Miasta Pyskowice Nr RZ.120.042.2021 z dnia 21 października 2021 r., dalej: Polityka *SZBI*.
[8] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz. U. z 2017 r. poz. 2247, dalej: *KRI*.

informacyjnych, Procedurę tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania. Łącznie Polityka SZBI zawierała 19 procedur. Z ww. Polityką zapoznano nowych i obecnych pracowników Urzędu.

(akta kontroli str.59 – 244)

W Polityce SZBI wskazano, m.in. Zespół ds. opracowania, wdrożenia i utrzymania Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie, do którego zadań należało, m.in. opracowanie, wdrożenie oraz monitorowanie i doskonalenie w Urzędzie Systemu Zarządzania Bezpieczeństwem Informacji. W skład ww. zespołu weszli Pełnomocnik ds. Systemu Zarządzania Bezpieczeństwem Informacji, który równocześnie był Inspektorem Ochrony Danych Osobowych, Sekretarz urzędu, zastępca Burmistrza, kierownik biura informatyki, audytor oraz pracownik wydziału organizacyjnego.

(akta kontroli str. 69 i 245 – 248)

Urząd posiadał również inne polityki, regulaminy i procedury stanowiące elementy SZBI[9], które zostały zatwierdzone i zakomunikowane pracownikom Urzędu.

(akta kontroli str. 222 – 224 i 249 – 252)

1.3. Jak przedstawiono w pkt. 1.2. niniejszego wystąpienia pokontrolnego, Burmistrz Zarządzeniem Nr RZ.120.042.2021 z dnia 21 października 2021 r. wdrożył SZBI, który stosownie do art. 24 i 25 rozporządzenia RODO[10] uwzględniał wymogi RODO w zakresie ochrony danych osobowych. Ww. SZBI zawierała politykę ochrony danych osobowych, dokumentację dotyczącą przeglądów zastosowanych środków technicznych i organizacyjnych zabezpieczenia danych osobowych, Procedury postępowania w sprawie naruszeń ochrony danych, w tym rejestr naruszeń (w systemie servicedesk OXARI).

(akta kontroli str. 69 – 73 i 130 – 134)

Ponadto w Urzędzie prowadzono: rejestry czynności Administratora, dokumentację z dokonywanej analizy ryzyka, dokumentację dotyczącą oceny skutków przetwarzania dla zbioru monitoringu miasta, dokumentację związaną z corocznym sprawozdaniem dla Administratora Danych Osobowych w Urzędzie, dokumentację ze zgłaszanymi naruszeniami ochrony danych do organu nadzorczego.

(akta kontroli str. 253 – 279)

1.4. W 2023 r. w Urzędzie sporządzono analizę ryzyka za 2023 r. w związku z potrzebą zachowania ciągłości działania systemów informatycznych. Pełnomocnik ds. zarządzania bezpieczeństwem informacji, na podstawie przedłożonych kart ryzyk bezpieczeństwa informacji opracowanych przez kierowników komórek organizacyjnych Urzędu sporządził, rejestr zidentyfikowanych ryzyk w Urzędzie

---

[9] Do których zaliczono; regulamin pracy Urzędu Miejskiego w Pyskowicach, regulamin organizacyjny, instrukcja bezpieczeństwa pożarowego, instrukcja zabezpieczenia obiektu, postępowania z kluczami oraz korzystania z pomieszczeń Urzędu Miejskiego w Pyskowicach, instrukcja obiegu dokumentów księgowych w UM, procedura zarządzania ryzykiem, regulamin prowadzenia kontroli w UM, zasady kontroli zarządczej i procesu jej samooceny w UM, plan ochrony informacji niejawnych w UM, szczegółowe wymagania w zakresie ochrony informacji niejawnych oznaczonych klauzulą „zastrzeżone" w UM, instrukcja postępowania w przypadku zagrożenia terrorystycznego, instrukcja kancelaryjna, zasady korzystania ze służbowych telefonów komórkowych, kart sim i modemów internetowych przez pracowników UM.

[10] 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 04.05.2016, str. 1, ze zm., dalej *RODO*.

zawierający m.in. ryzyka niedopuszczalne[11]. Następnie przedłożył Burmistrzowi Kartę postępowania z ryzykami, w której wskazał działania minimalizujące ryzyko, poprzez zakup agregatu zasilającego oraz dostosowanie instalacji zasilającej budynek Urzędu. ww. plan został zatwierdzony przez Burmistrza.

(akta kontroli str. 280 – 333)

1.5. Załącznikiem Polityki SZBI była procedura ciągłości działania (PS03), w której zawarto zasady postępowania w przypadku zaistnienia zdarzeń mających wpływ na bezpieczeństwo informacji oraz ciągłości działania Urzędu. Z ww. procedurą zostali zapoznani nowi i obecni pracownicy Urzędu.

(akta kontroli str. 115 – 121)

1.6. W Urzędzie opracowano i wdrożono Scenariusze planu ciągłości działania, stanowiące załącznik nr Z1 do procedury PS03 – scenariusze planu ciągłości działania. Dotyczyły one, m.in. scenariusza pożaru budynku Urzędu (serwerowni, pomieszczeń biurowych i centrali telefonicznej), awarii zasilania elektrycznego UPS, awarii macierzy dyskowej, awarii urządzeń wielofunkcyjnej zapory sieciowej – UTM, braku łącza internetowego, awarii serwera, awarii aplikacji/usunięcie plików z serwera, awarii przełącznika sieciowego, awarii okablowania sieciowego, awarii serwera wirtualnego, awarii komputera osobistego, awarii serwera środowiska i awarii systemu kopii zapasowych.

(akta kontroli str. 334 – 363)

Nie opracowano oddzielnego Planu odtworzeniowego dla Urzędu, gdyż Plan ciągłości działania zawierał jego elementy, np. dotyczące odtworzenia pomieszczeń serwerowni czy centrali telefonicznej.

(akta kontroli str. 115 – 121)

W zawartych przez Urząd umowach z podmiotami zewnętrznymi np. na wykonanie usługi w zakresie serwisu i nadzoru autorskiego nad prawidłowością funkcjonowania oprogramowania Ratusz, tj. zintegrowanego systemu zarządzania Gminą, określono czas przywrócenia ciągłości działania systemów informatycznych. Na usunięcie awarii krytycznej przewidziano osiem godzin roboczych, a na usunięcie awarii krytycznej lub zapewnienie alternatywnego sposobu pracy w systemie 16 godzin roboczych.

(akta kontroli str. 732)

1.7. Przyjęte scenariusze planu ciągłości działania podlegały testowaniu i treningowi. W okresie objętym kontrolą przeprowadzono łącznie 16 testów Planu ciągłości działania, z których sporządzono protokoły.

I tak np. przeprowadzony test dotyczący awarii serwera wirtualnego zakładał sprawdzenie przestrzeni dyskowej hosta serwera docelowego, wyłączenie maszyny wirtualnej (1), przystąpienia do odtworzenia maszyny wirtualnej (2) z kopii zapasowej, zalogowanie się do odtworzonej maszyny wirtualnej, wyłączeniu odzyskanej maszyny wirtualnej (2) i jej usunięcie, włączenie maszyny wirtualnej (1).

We wnioskach stwierdzono, iż „test przeprowadzono poprawnie". W ww. ćwiczeniach wzięli udział wszyscy pracownicy Wydziału Biura Informatyki.

(akta kontroli str. 364 – 379)

1.8. W 2023 r. Zespół ds. Systemu Zarządzania Bezpieczeństwem Informacji odbył dziesięć spotkań, w wyniku których zarekomendowano, m.in. aktualizację Polityki bezpieczeństwa oraz wskazano na potrzebę zakupu agregatu prądotwórczego zapewniającego zasilanie awaryjne, które pozwoli na wyeliminowanie

[11] Związane z możliwością wystąpienia braku zasilania w poszczególnych komórkach organizacyjnych.

zidentyfikowanego ryzyka utraty ciągłości działania. Rekomendacje te były w trakcie realizacji podczas kontroli.

(akta kontroli str. 380 – 397)

1.9. Zarządzeniem Burmistrza z dnia 13 marca 2019 r. powołano zespół ds. opracowania, wdrożenia i utrzymania Systemu Zarządzania Bezpieczeństwem Informacji i Ochrony Danych Osobowych, w skład, którego wszedł m.in. Inspektor Ochrony Danych równocześnie pełniący obowiązki Pełnomocnika ds. SZBI.

(akta kontroli str. 2435 – 248)

Według Polityki SZBI, Pełnomocnik odpowiedzialny był za:

- nadzór nad realizacją Systemu Zarządzania Bezpieczeństwem Informacji;
- nadzór nad dokumentacją Systemu Zarządzania Bezpieczeństwem Informacji na etapie jej opracowywania, weryfikacji, aktualizacji, udostępniania i przechowywania;
- zarządzanie analizą ryzyka jako kluczowym narzędziem SZBI;
- zarządzanie zabezpieczeniami aktywów informacyjnych w sposób adekwatny do celów stosowania zabezpieczeń;
- zapewnienie, że procesy potrzebne w Systemie Zarządzania Bezpieczeństwem Informacji są ustanowione, wdrożone i utrzymywane;
- planowanie prac dotyczących systemu zarządzania i nadzór nad ich realizacją;
- przedstawianie sprawozdań dla Burmistrza Miasta Pyskowice, dotyczących funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji oraz realizacji celów, jak również informowanie o skuteczności funkcjonującego SZBI;
- zarządzanie audytami wewnętrznymi (w obszarze bezpieczeństwa informacji) w zakresie nadzorowania zespołu audytorów, planowania audytów i nadzór nad ich realizacją oraz działaniami poaudytowymi;
- inicjowanie oraz nadzorowanie działań wdrożeniowych, korygujących i zapobiegawczych;
- organizację przeglądów Systemu Zarządzania Bezpieczeństwem Informacji oraz nadzór nad realizacją ustaleń wynikających z przeglądów;
- powiadamianie kierownictwa o działalności niezgodnej z obowiązującą w Systemie Zarządzania Bezpieczeństwem Informacji;
- nadzorowanie szkoleń z zakresu Systemu Zarządzania Bezpieczeństwem Informacji.

Uprawniony był do:

- wydawania poleceń wszystkim pracownikom Urzędu Miejskiego w Pyskowicach w zakresie związanym z wdrożeniem, utrzymaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji;
- rozstrzygania sporów dotyczących stosowania wymagań zawartych w dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji oraz wydawania wiążących decyzji w tym zakresie;

- dostępu do wszystkich dokumentów występujących w Urzędzie Miejskim w Pyskowicach, których treść może być istotna z punktu widzenia funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji;
- uzyskania wyjaśnień od pracowników w zakresie realizowanych działań w ramach Systemu Zarządzania Bezpieczeństwem Informacji;
- podejmowania decyzji w kwestiach bezpieczeństwa Informacji, w zakresie nierodzącym zobowiązań finansowych; w szczególności w zakresie współpracy z pozostałymi jednostkami organizacyjnymi Urzędu Miejskiego w Pyskowicach oraz jednostkami nadrzędnymi.

(akta kontroli str. 67 – 68)

Natomiast wg zakresu czynności Pełnomocnik odpowiedzialny był m.in. za:

- organizowanie lub prowadzenie szkoleń pracowników Urzędu Miejskiego z zakresu bezpieczeństwa informacji i ochrony danych osobowych,
- tworzenie, aktualizacja i opiniowanie dokumentacji dotyczącej zasad przetwarzania danych osobowych i bezpieczeństwa informacji,
- prowadzenie spraw dotyczących Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Pyskowicach. Koordynowanie prac przy aktualizacji, opracowaniu, zatwierdzaniu i weryfikowaniu dokumentacji SZBI w celu jego właściwego funkcjonowania, utrzymywania i doskonalenia. Nadzorowanie przebiegu audytów wewnętrznych w tym zakresie,
- prowadzenie rejestru naruszeń, rejestru udostępnień danych oraz ewidencji upoważnień osób przetwarzających dane osobowe,
- prowadzenie rejestru czynności przetwarzania i kategorii czynności,
- identyfikację, ocenę oraz monitorowanie ryzyka w zakresie bezpieczeństwa danych osobowych,
- udzielanie zaleceń i konsultowanie oceny skutków dla ochrony danych przed planowanymi w Urzędzie operacjami przetwarzania danych.

(akta kontroli str. 458)

Pełnomocnik ds. SZBI, posiadał ukończone m.in. kursy i szkolenia w zakresie bezpieczeństwa informacji, np. ukończone w 2016 r. szkolenie w zakresie „Wymagania organizacyjno - dokumentacyjne Krajowych Ram Interoperacyjności", w 2019 r. w zakresie „Praktyczne warsztaty zarządzania bezpieczeństwem informacji w urzędzie", w 2020 r. w zakresie „Szacowania ryzyka w procesie „Analizy Ryzyka Ogólnego" oraz „Oceny Skutków dla Przetwarzania Danych w oparciu o wytyczne ISI 27001, a także w zakresie „Bezpieczeństwa informacji w oparciu o ustawę o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczeniem przestępczości(…)".

(akta kontroli str. 460 – 473)

Według Polityki SZBI, Administrator Systemów Informatycznych[12] z upoważnienia Burmistrza miał:
a) zarządzać systemami informatycznymi Urzędu;
b) prowadzić dokumentację wynikającą z zapisów SZBI;
c) podejmować odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa informacji;
d) określać zakres uprawnień do systemów informatycznych w porozumieniu z kierującymi poszczególnymi komórkami organizacyjnymi;

[12] Dalej; ASI

e) prowadzić, uaktualniać na bieżąco oraz przesyłać Pełnomocnikowi do spraw Systemu Zarządzania Bezpieczeństwem Informacji raporty dotyczący zdarzeń wpływających na bezpieczeństwo systemów informatycznych, w tym m.in. wykrytego oprogramowania złośliwego lub szpiegującego oprogramowania nielegalnego lub zainstalowanego bez upoważnienia, awarii systemu informatycznego lub jego nieprawidłowego działania, stwierdzenia faktu korzystania z systemu informatycznego przez osobę niepowołaną, awarii zasilania.

(akta kontroli str. 68)

Natomiast wg Procedury PS03 ASI odpowiedzialny był za opracowanie i utrzymanie scenariuszów planu ciągłości działania, za nadzór nad realizacją działań związanych z opracowaniem i utrzymaniem scenariuszów planu ciągłości działania odpowiedzialny był Pełnomocnik SZBI, a za realizację działań przewidzianych w scenariuszach planu ciągłości działania odpowiedzialne były wskazane w nim osoby.

(akta kontroli str. 117)

Wg zakresu czynności Kierownika Biura Informatyki, odpowiedzialny był on m.in. za:

- bieżącą obsługę techniczną w zakresie zapewnienia ciągłości działania systemów informatycznych,
- nadzór nad wykorzystywaniem sprzętu informatycznego oraz eksploatację programów – obsługa techniczna.

(akta kontroli str. 476 – 481)

Posiadał ukończone studia podyplomowe w zakresie informatyki w administracji publicznej. Ponadto, uczestniczył w kursach i szkolenia: „Krajowe Ramy Interoperacyjności", „Wirtualizacja środowiska serwerowego", Warsztaty techniczne „Forti Effective Day", „Cyberbezpieczeństwo – jak skutecznie chronić siebie instytucje przed cyberzagrożeniami", „wymagania Krajowych Ram Interoperacyjności w kontekście zarządzania incydentem oraz usługami IT", „Bezpieczna e-Administracja".

(akta kontroli str. 482 – 505)

Natomiast informatyk zatrudniony w Biurze Informatyki odpowiedzialny był m.in. za pełnienie obowiązków Administratora Systemu Informatycznego, obejmującego swym zakresem nadawanie uprawnień do sieci komputerowej oraz instalację oprogramowania i sprzętu komputerowego w komórkach Urzędu.

(akta kontroli str. 506 – 507)

Zatrudniony informatyk w Biurze Informatyki ukończył technikum informatyczne w 2015 r. oraz posiadał zdane egzaminy potwierdzające kwalifikacje w zakresie montażu i eksploatacji komputerów osobistych oraz urządzeń peryferyjnych oraz projektowania lokalnych sieci komputerowych i administrowania sieciami.

(akta kontroli str. 508 – 520)

1.10. Od 19 czerwca 2018 r. funkcję inspektora ochrony danych osobowych w Urzędzie pełnił pracownik, podlegający (stosownie do art. 38 ust. 3 RODO) bezpośrednio Burmistrzowi. Urząd w dniu 10 lipca 2018 r. zawiadomił Urząd Ochrony Danych Osobowych o wyznaczeniu Inspektora Ochrony Danych w Urzędzie.

(akta kontroli str. 456 i 521 – 523)

IOD posiadał doświadczenie zawodowe w zakresie ochrony danych osobowych (w okresie od 18 stycznia 2016 r. do 18 czerwca 2018 r. pełnił funkcję Administratora Bezpieczeństwa Informacji), brał udział w szkoleniach dotyczących ochrony danych osobowych[13] i ukończył kurs[14] w tym zakresie.

(akta kontroli str. 451 i 475)

1.11. IOD równocześnie pełnił obowiązki dotyczące utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, pełnił funkcję Pełnomocnika ds. zarządzania bezpieczeństwem informacji oraz prowadził sprawy związane z redagowaniem materiałów na platformie elektronicznych usług publicznych (PEUP), wykonywał zadania administratora na platformie e-PUAP, prowadził sprawy dotyczące funkcjonowania i eksploatacji urządzeń kserograficznych i faksów, prowadził sprawy z zakresu elektronicznego systemu informacji przestrzennej, prowadził sprawy dotyczące rejestracji i wyrejestrowania Inspektora Ochrony Danych w Urzędzie Ochrony Danych Osobowych[15].

(akta kontroli str. 456 – 459)

IOD wykonywał swoje obowiązki w sposób niezależny, a w jego działalności nie występował konflikt interesów. IOD nie brał również udziału w określaniu celów i sposobów przetwarzania danych osobowych. Do zadań IOD należało m.in. prowadzenie weryfikacji zgodności obowiązujących w Urzędzie procedur i dokumentacji, przygotowanie lub modyfikacja i wdrożenie niezbędnych dokumentów i procedur, szkolenie kadry zarządzającej i pracowników, nadzór nad przestrzeganiem przepisów, działania w przypadku wystąpienia incydentów i naruszeń bezpieczeństwa informacji, prowadzenie kontroli bezpieczeństwa danych, współpraca z Wydziałem Informatyki w zakresie zabezpieczeń systemu informatycznego, dokumentowanie i zgłaszanie naruszeń do UODO, udzielanie odpowiedzi na pytania i wątpliwości kadry zarządzającej i pracowników, informowanie administratora danych o wszelkich zmianach przepisów prawa oraz o potrzebach zmian w Urzędzie w zakresie ochrony danych osobowych.

(akta kontroli str. 451 – 459)

1.12. Stosownie do art. 21 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa[16] w dniu 7 lipca 2022 r. Zarządzeniem Burmistrza, wyznaczono osobę do utrzymywania kontaktów z podmiotami Krajowego Systemu Cyberbezpieczeństwa. Urząd, realizując zadanie publiczne zależne od systemu informacyjnego, stosownie do art. 22 ust. 1 pkt 5 ustawy o ksc, przekazał w dniu 8 lipca 2022 r. do CSIRT NASK, dane osoby, obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej w terminie 14 dni od dnia jej wyznaczenia.

(akta kontroli str. 524 – 528)

---

[13] W 2026 r. – Wymagania organizacyjno-dokumentacyjne Krajowych Ram Interoperacyjności, w 2027 – Obowiązkowa dokumentacja przetwarzania danych RODO, Forum Bezpieczeństwa Administracji, w 2028 r. – Nowelizacja przepisów o ochronie danych osobowych – praktyczne aspekty stosowania RODO oraz nowej ustawy o ochronie danych osobowych, RODO w zamówieniach publicznych, w 2019 r. – Praktyczne warsztaty zarządzania bezpieczeństwem informacji w urzędzie, Szacowanie ryzyka w procesie „Analizy Ryzyka Ogólnego" oraz „Oceny Skutków dla Przetwarzania Danych (DPIA), w 2020 r. – Krajowe Ramy Interoperacyjności, Bezpieczeństwa informacji w oparciu o ustawę z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (…), w 2021 r. – Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych (…), w 2023 r. – Nie Daj Się Cyber zbójom, w 2024 r. – Ochrona danych osobowych w fazie projektowania, Rejestr czynności przetwarzania – jak go właściwie prowadzić, umowa powierzenia przetwarzania danych osobowych – omówienie i ocena zapisów z umów.

[14] Ukończony w 2015 r. - Kurs Administratorów Bezpieczeństwa Informacji.

[15] Dalej; UODO.

[16] Ustawa z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa, Dz.U. z 2024 r., poz.1077, dalej: ksc.

W sprawie nie wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami Krajowego Systemu Cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jednostki jemu podległe lub przez niego nadzorowane oraz za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jej jednostki organizacyjne Burmistrz wyjaśnił, że *osoba taka nie została wyznaczona ponieważ nie dostrzeżono takiej potrzeby, a sama ustawa o KSC nie wymaga obligatoryjnego jej wyznaczenia*.

(akta kontroli str. 835)

1.13. W funkcjonującej w Urzędzie Polityce SZBI (pkt 4) wskazano procedury związane z bezpieczeństwem informacji. Składały się one z 19 następujących procedur:

1) PS01 – Nadzór nad dokumentacją i zapisami systemu zarządzania bezpieczeństwem informacji – dokument zapewniający, że wszystkie dokumenty, procedury, instrukcje potrzebne do funkcjonowania SZBI są skatalogowane, objęte nadzorem oraz zasadami stosowania.

2) PS02 – Identyfikacja oraz zarządzanie ryzykiem bezpieczeństwa aktywów informacyjnych – dokument opisujący identyfikację aktywów informacyjnych w Urzędzie, sposób zarządzania analizą ryzyka aktywów informacyjnych oraz planowanie postępowania z ryzykiem.

3) PS03 – Zarządzanie ciągłością działania – dokument opisujący identyfikację wymagań dla ciągłości i dostępności usług Urzędu.

4) PS04 – Monitorowanie, ocena i przegląd działania SZBI – dokument zawierający ogólne zasady monitorowania, oceny działań na rzecz bezpieczeństwa informacji, zasad przeprowadzania audytów wewnętrznych Bezpieczeństwa Informacji oraz przeglądu skuteczności Systemu Zarządzania Bezpieczeństwem Informacji.

5) PS05 – Zarządzanie incydentami, niezgodnościami oraz działania korygujące – dokument opisujący działania jakie należy podejmować w przypadku incydentów bądź niezgodności wynikłych w trakcie przetwarzania danych oraz dokumentowanie działań korygujących.

6) PS06 – Procedura nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym – dokument opisujący zasady nadawania i rejestrowania uprawnień dających dostęp do systemów informatycznych nie zawierających danych osobowych.

7) PS07 – Procedura nadawania uprawnień do przetwarzania danych osobowych i rejestrowania tych uprawnień w systemie informatycznym.

8) PS08 – Stosowane metody uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem.

9) PS09 – Procedura rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym.

10) PS10 – Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

11) PS11 – Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych.

12) PS12 – Sposób zabezpieczania systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie dostępu do systemów informatycznych.

13) PS13 – Procedura wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

14) PS14 – Nadzór nad połączeniami zdalnymi.

15) PS15 – Autoryzacja nowych urządzeń dopuszczonych do sieci teleinformatycznej urzędu.

16) PS16 – Zarządzanie zmianami w systemach teleinformatycznych – Procedury, instrukcje, dokumenty potrzebne do zapewnienia bezpieczeństwa informacji w Urzędzie ujęte w załączniku nr 3 PS01 (PS01-Z3)

17) PS17 – Ochrona danych podczas pracy zdalnej na sprzęcie służbowym.

18) PS18 – Procedura korzystania ze służbowej poczty elektronicznej.

19) PS19 – Procedura postępowania z urządzeniami mobilnymi.

(akta kontroli str. 66 – 67)

1.14. Przeprowadzone oględziny[17] w dniu 2 lipca 2024 r. wykazały m.in., że Urząd dysponował aktualnymi informacjami o posiadanym zasobie informatycznym oraz o jego konfiguracji. Zasoby informatyczne przypisano do osób, które odpowiadały za dany sprzęt. Było to zgodne z § 20 ust. 2 pkt 2 rozporządzenia KRI.

(akta kontroli str. 529 – 552)

1.15. Urząd złożył w dniu 13 grudnia 2023 r. wniosek o przystąpienie do rządowego programu „Cyberbezpieczny Samorząd" określając wartość zadania na kwotę 649,6 tys. zł. Kolejnym wnioskiem z dnia 10 kwietnia 2024 r. wniesiono o zmniejszenie wartości zadania o kwotę 151 tys. zł w związku niższą wartością zakupu agregatu prądotwórczego dla budynku Urzędu.

(akta kontroli str. 553 – 572)

W dniu 24 czerwca 2024 r. Burmistrz podpisał umowę na łączną wartość zadania w wysokości 498,6 tys. zł, z czego środki Unii Europejskiej i dofinansowanie z budżetu państwa miało wynieść 94% kwoty zadania (408,7 tys. zł), z przeznaczeniem na wykonanie trzech zadań, m.in. obszarze organizacyjnych[18], kompetencyjnym[19] i technicznym[20]. Według § 3 Umowy, przewidziano realizację zadania w okresie maksymalnie 24 miesięcy od dnia wejścia w życie umowy, ale nie dłużej niż do 30 czerwca 2026 r.

(akta kontroli str. 573 – 602)

Jak wyjaśnił Burmistrz, *pomiar poprawy cyberbezpieczeństwa urzędu w związku z realizacją Programu zostanie zrealizowany poprzez sporządzenie audytu wraz z ankietą potwierdzającą poprawę cyberbezpieczeństwa.*

(akta kontroli str. 835)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki, w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

OCENA CZĄSTKOWA

Urząd podejmował prawidłowe działania mające na celu zapewnienie warunków organizacji bezpieczeństwa informacji oraz zapewnienie ciągłości działania systemów informatycznych.

[17] Wybranych na podstawie doboru celowego: 10 komputerów, jednego serwera, dwóch laptopów, routera i jednej drukarki.

[18] Aktualizacja dokumentacji Polityki bezpieczeństwa, przeprowadzanie szacowania ryzyk i audytu oraz przeprowadzenie kampanii informacyjnej i promocji projektu.

[19] Przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa dla pracowników Urzędu oraz szkolenie administratorów w zakresie wdrożenia i użytkowania oprogramowania SIEM.

[20] Zakupy; odnowienie subskrypcji oprogramowania dla urządzenia UTM, zakup subskrypcji dla wykonywania kopii zapasowych, zakup i wdrożenie i utrzymanie oprogramowania SIEM, odnowienie rocznej usługi wsparcia technicznego dla posiadanego oprogramowania Veeam Backup Essentials, dostaw i montaż agregatu prądotwórczego dla budynku Urzędu oraz usługa testowania zabezpieczeń infrastruktury sieciowej.

OBSZAR

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

Opis stanu faktycznego

2.1. W wyniku przeprowadzonych w dniu 27 czerwca 2024 r. oględzin dziesięciu komputerów, w tym siedmiu stacjonarnych i trzech laptopów, ustalono, że na kontach ich użytkowników nie było możliwe zainstalowania oprogramowania testowego aplikacji Adobe Reader gdyż system wyświetlał monit o podniesienie uprawnień do poziomu administratora.

(akta kontroli str.603 – 606)

Powyższe było zgodne z § 19 ust. 2 pkt 7 lit. c rozporządzenia Krajowych Ramach Interoperacyjności[21].

Jak wyjaśniła Naczelnik Wydziału Organizacyjnego, *w Urzędzie nie wykorzystuje się tabletów, jedynie telefony komórkowe, które zostały przekazane w użytkowanie 12 wyznaczonym naczelnikom i pracownikom wydziałów. Pracownicy korzystający ze służbowych telefonów komórkowych mają zablokowany dostęp do instalacji nowego oprogramowania poprzez blokadę sklepu z aplikacjami (np. Sklepu Play) oraz usługi instalacji (pliki .apk). Wyżej wymieniona metoda realizowana jest za pośrednictwem* aplikacji *AppLock zabezpieczonej kodem PIN*.

(akta kontroli str. 607)

2.2. Analiza zakresów czynności oraz nadanych uprawnień[22] pracownikom Urzędu, wykonujących zadania w systemach informatycznych, wykazała, że we wszystkich przypadkach posiadali oni uprawnienia przyznane w oparciu o funkcjonującą w Urzędzie procedurę PS06[23] i PS07[24], otrzymane uprawnienia dotyczyły dostępu do LEXa, poczty służbowej, domeny sieciowej, systemu obiegu dokumentów. Natomiast dostęp do innych systemów np. *BOMARK* – środki trwałe, księgowość budżetowa, fakturowanie, *RATUSZ* – Pas drogowy, Odpady komunalne, wynikał z zadań realizowanych wskazanych w zakresach obowiązków. W przypadku pracownika Urzędu, który został przeniesiony służbowo z Wydziału Gospodarki Lokalami do Wydziału Księgowości i Budżetu, odebrano uprawnienia do pracy m.in. w systemie; Lokalowy Zasób Gminy, Rejestr umów o odpracowanie zadłużenia, windykacja umorzeń, system zarządzania nieruchomościami, równocześnie nadano dostęp do m.in.; systemu *BOMARK* – księgowość budżetowa, fakturowanie.
Wnioski o nadanie dostępu do systemów Naczelnikom Wydziałów informatycznych sporządził Burmistrz, a w przypadku innych pracowników wnioski zostały sporządzone przez Naczelników Wydziałów. Wydane uprawnienia były zarejestrowane w rejestrach upoważnień i prowadzonych przez IOD oraz Kierownika Biura Informatyki i ASI, co było zgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI.

(akta kontroli str. 608 – 716)

[21] Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz. U. 2024r. poz. 773, dalej: *Krajowe Ramy Interoperacyjności.*

[22] Dla 15 pracowników Urzędu, w tym dziewięciu Naczelników Wydziałów, jednego Kierownika komórki oraz pięciu pozostałych pracowników Urzędu, w tym jednego, który w czasie objętym kontrolą został przeniesiony z jednego do drugiego Wydziału.

[23] Nadawanie uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemie informatycznym.

[24] Nadawanie uprawnień do przetwarzania danych osobowych i rejestrowanie tych uprawnień w systemie informatycznym.

2.3. W okresie objętym kontrolą, z 12 pracownikami Urzędu rozwiązano umowę o pracę. W wyniku przeprowadzonych oględzin systemu IT ustalono, że we wszystkich tych przypadkach, stosownie do § 19 ust. 2 pkt 5 rozporządzenia Krajowych Ramach Interoperacyjności, konta tych pracowników zostały niezwłocznie zablokowane.

(akta kontroli str. 717, 718)

Jak wyjaśnił Burmistrz, *w przypadku 12 pracowników, z którymi rozwiązano umowę o pracę w okresie objętym kontrolą, rozwiązanie umowy o pracę powoduje utratę dostępu do przetwarzania danych i natychmiastowe wyłączenie kont użytkownika z systemów. Odbywa się to podczas podpisywania karty obiegowej danego pracownika. W czasie tego procesu pracownik zdaje kartę chipową dającą dostęp do systemów, a pracownik Biura Informatyki dodatkowo blokuje możliwość korzystania z danego konta.*

(akta kontroli str. 835)

2.4. Wg procedury PS08 – Stosowane metody uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem hasło umożliwiające dostęp do systemów informatycznych powinno składać się z, co najmniej ośmiu znaków i zawierać miało małe litery i wielkie litery oraz cyfry lub znaki specjalne. Miało być zmieniane nie rzadziej niż co 30 dni.

(akta kontroli str. 151)

Przeprowadzone oględziny[25] trzech używanych w Urzędzie systemów informatycznych: Komax 2.0. – system kadrowo-płacowy, eM@ndat – system dla Straży Miejskiej oraz Ratusz – system do zarządzania jednostkami administracji samorządowej potwierdziły, iż zastosowane hasła spełniały wymogi ww. procedury PS08.

(akta kontroli str. 720 – 721)

Analiza 36 loginów trzech poddanych oględzinom systemów[26], wykazała, że w dziewięciu przypadkach login wykorzystywał nazwisko i poprzez to wskazywał bezpośrednio użytkownika a w pozostałych 27 przypadkach identyfikatory były tworzone według zasady; symbol komórki i kolejny przypisany numer. We wszystkich powyższych systemach loginy były unikalne.

(akta kontroli str. 722 – 723)

2.5. Przeprowadzone[27] oględziny czterech stanowisk pracy na których realizowano zadania związane z wydawaniem dowodów osobistych z wykorzystaniem aplikacji „Źródło" wykazały, że monitory usytuowane były w sposób uniemożliwiający wgląd do danych przez osoby nieuprawnione. Powyższe spełniało wymogi § 19 ust. 2 pkt 7 rozporządzenia Krajowych Ramach Interoperacyjności.

(akta kontroli str. 724)

2.6. Urząd stosownie do § 20 ust. 2 pkt 8 rozporządzenia KRI, opracował poniższe procedury gwarantujące bezpieczną pracę zdalną, w szczególności przy przetwarzaniu mobilnym:

- procedura PS 17 – Ochrona danych podczas pracy zdalnej na sprzęcie służbowym,
- procedura PS 18 – Procedura korzystania ze służbowej poczty elektronicznej,
- procedura PS 19 - Procedura postępowania z urządzeniami mobilnymi.

[25] W dniu 27 czerwca 2024 r.
[26] Ratusz – 27 kont użytkowników, KOMAX – 7 i @Mandat – 2 konta użytkowników.
[27] W dniu 6 czerwca 2024 r.

W ramach tych procedur opisano zasady korzystania ze sprzętu informatycznego minimalizujące ryzyka kradzieży informacji, w tym urządzeń mobilnych. Np. osoba korzystająca z urządzeń wykorzystywanych do realizacji pracy zdalnej nie mogła podejmować pracy w miejscach publicznych, jak: kawiarnie, restauracje, galerie handlowe, zakazano udostępniania urządzeń innym osobom, np. domownikom, do pracy pracownik powinien wykorzystywać wyłącznie służbowe programy i systemy udostępnione przez pracodawcę. Zabroniono używania poczty elektronicznej do prowadzenia korespondencji prywatnej lub pracy charytatywnej niepowiązanej z działalnością pracodawcy. Ograniczono instalację oprogramowania oraz wprowadzono kontrolę dostępu w postaci konta użytkownika i administratora w przypadku mobilnej stacji roboczej lub aplikacji ograniczającej dostęp na smartfonie.

(akta kontroli str. 199 – 215)

Wszyscy pracownicy Urzędu zostali z zapoznani z ww. procedurami i zobowiązani do ich stosowania.

2.7. Jak wyjaśnił Kierownik Biura Informatyki Urzędu, *w Urzędzie stosuje się rozwiązania związane z ochroną danych zgromadzonych na laptopach poprzez zastosowanie mechanizmów Actiwe Directory (AD), które wymuszają przy uruchomieniu przez danego użytkownika sprzętu uwierzytelnienie za pomocą loginu i hasła, a w przypadku dysków twardych stosuje się oprogramowanie szyfrujące dyski twarde*.

(akta kontroli str. 836)

2.8. W wyniku przeprowadzonych oględzin serwerowni[28] ustalono m.in., że serwerownia była wyodrębnionym pomieszczeniem umiejscowionym w budynku Urzędu, wejście do serwerowni było zabezpieczone wzmocnionymi drzwiami wyposażonymi w zamki oraz w system kontroli dostępu. Pomieszczenie nie było oznaczone w sposób umożliwiający identyfikację jego przeznaczenia. W pomieszczeniu serwerowni zainstalowano system alarmowy oraz jego manipulator. Wejście i wyjście z serwerowni było możliwe przy użyciu indywidualnych kart elektronicznych, a ich ewidencję prowadzono elektronicznie. Serwerownia wyposażona była w system klimatyzacji. W dniu oględzin w pomieszczeniu nie odnotowano obecności materiałów łatwopalnych, w szczególności dokumentów, segregatorów, teczek. Sprzęt informatyczny był podłączony do dedykowanej sieci elektrycznej, która była wydzielona i posiadała własne zabezpieczenia, a rozdzielnica elektryczna zasilania obwodów była zabezpieczona przed dostępem osób trzecich. Serwerownia posiadała zasilanie awaryjne – UPS.

(akta kontroli str. 725 – 729)

Jak wyjaśnił Kierownik Biura Informatyki, *w serwerowni zainstalowane jest urządzenie serwer środowiska, którego zadaniem jest monitorowanie temperatury oraz wilgotności w pomieszczeniu, w przypadku wzrostu temperatury i przekroczeniu zadanej wartości krytycznej administratorzy otrzymują wiadomość sms oraz informację w postaci maila, że została przekroczona temperatura krytyczna. System alarmowy zainstalowany w serwerowni uruchamiany jest codziennie przed zakończeniem pracy Urzędu oraz wyłączany po rozpoczęciu pracy. Rejestr pracowników upoważnionych do przebywania w serwerowni nie jest prowadzony, gdyż dostęp do niej mają wszyscy pracownicy Biura Informatyki. W pomieszczeniu serwerowni nikt nie przebywa na stałe, a personel sprzątający wykonuje czynności porządkowe wyłącznie w obecności pracownika Biura Informatyki. Urząd dysponuje*

[28] W dniu 27 czerwca 2024 r.

przenośnym urządzeniem klimatyzacyjnym, które stanowi urządzenie rezerwowe na wypadek awarii systemu klimatyzacji w pomieszczeniu serwerowni.

(akta kontroli str.730)

2.9. Analiza czterech zawartych umów[29] z podmiotami zewnętrznymi wykazała, m.in., że w analizowanych umowach stosownie do § 20 ust. 2 pkt 10 rozporządzenia KRI zawarto zapisy mówiące o zobowiązaniu wykonawcy do zachowania tajemnicy informacji do jakich może mieć dostęp w związku z realizowaniem umowy.
I tak np. w umowa BI.1330.15.2024 zawierała m.in. zapis, który zobowiązywał operatora do „*zachowania, tak w okresie obowiązywania umowy, jak również po jej zakończeniu, tajemnicy, co do wszystkich danych pozyskanych przy wykonywaniu umowy, a także innych informacji mogących mieć charakter poufny*".

(akta kontroli str. 731 – 776)

2.10. W Urzędzie została opracowana i wdrożona procedura PS11 - dotycząca sposobu, miejsca i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych, w której zawarto informacje o przekazywaniu i niszczeniu nośników informacji.
Wg ww. procedury, nośniki danych (w tym również kopie zapasowe i archiwalne) winny być przechowywane w wydzielonym pomieszczeniu i/lub szafie/sejfie w sposób zabezpieczający je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem, a warunki środowiskowe przechowywania nośników powinny być zgodne z wytycznymi producentów nośników.

(akta kontroli str. 168 - 170)

W sprawie postępowania ze sprzętem IT w sytuacji ich przekazania do serwisu, Kierownik Biura Informatyki wyjaśnił, że *Urząd (…) nie przekazuje sprzętu IT zawierającego informacje poza swoją siedzibę. Sprzęt jest użytkowany w jednostce do „śmierci technologicznej" i nie jest zbywany lub przekazywany do ponownego użycia. Po zezłomowaniu sprzętu oprogramowanie systemowe jest usuwane wraz z niszczeniem nośnika danych a licencjonowane programy jeśli nadają się do dalszego wykorzystania instalowane są na nowym sprzęcie.*

(akta kontroli str. 837)

Burmistrz dodatkowo wyjaśnił ,że *pracownicy Biura Informatyki postępują zgodnie z Procedurą PS11 Polityki Systemu Zrządzania Bezpieczeństwem Informacji UM, która to wymaga aby z urządzeń i/lub nośników danych zawierających dane osobowe przed przekazaniem do naprawy dane te usunąć w sposób trwały uniemożliwiający późniejsze odczytanie/odtworzenie. W przypadku przekazania nośników danych w celu ich odzyskania wymagane jest zobowiązanie firmy zewnętrznej do zachowania tajemnicy poprzez umieszczenie w umowie klauzuli poufności oraz zawarcie umowy powierzenia przetwarzania danych osobowych w sytuacji gdy ma to zastosowanie.*

(akta kontroli str. 835)

2.11. W Urzędzie zostały ustalone procedury dotyczące tworzenia i przechowywania kopii zapasowych:

[29] Umowa nr BI.1330.007.2024 na sprawowanie nadzoru technicznego nad autorskimi programami komputerowymi do obsługi dodatków mieszkaniowych, do dodatków energetycznych, umowa nr BI.1330.012.204 na wykonanie usługi w zakresie serwisu i nadzoru autorskiego nad prawidłowością funkcjonowania oprogramowania Ratusz-zintegrowanego systemu zarządzania Gminą, umowa nr BI.1330.06.2024 na nadzór autorski nad eksploatacją oprogramowania „Księgowość budżetowa" i „Środki Trwałe", umowa nr BI.1330.15.2024 na udostępnienie licencji oraz utrzymanie systemu FINN e-Zamówienia Publiczne.

- Procedura PS 10 – tworzenie kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania, w której wskazano, m.in., że kopie baz danych oraz aplikacji bazodanowych zlokalizowanych na serwerach wykonywane są, w cyklu dziennym (w godzinach nocnych) za pomocą aplikacji archiwizujących dane do postaci tzw. kopii pełnych, w cyklach dwugodzinnych za pomocą aplikacji archiwizujących dane do postaci tzw. kopii przyrostowej, która na koniec dnia jest tworzona jako kopia pełna. Kopie zapasowe wykonywane są na macierzach dyskowych oraz na nośnikach zewnętrznych (macierz dyskowa, taśmy magnetyczne, płyty CD, DVD),

- Procedura PS11 - sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych, wg procedury okres przechowywania kopii zapasowych ustalono na minimum 5 dni roboczych, które należało zniszczyć niezwłocznie po ustaniu ich użyteczności. Ponadto wskazano, iż zdezaktualizowane i uszkodzone kopie należy mechanicznie niszczyć w sposób uniemożliwiający ich ponowne użycie. Za bezpieczeństwo przechowywania kopii zapasowych z serwerów odpowiedzialnym był ASI, a za bezpieczeństwo przechowywanych kopii zapasowych na nośnikach zewnętrznych tworzonych przez użytkowników odpowiadały osoby, które stworzyły kopie zapasową.

(akta kontroli str. 160 – 174)

2.12. W Urzędzie zasady tworzenia, przechowywania i testowania kopii zapasowych regulowała Procedura PS10 i PS11.

W wyniku przeprowadzonych[30] oględzin ustalono, że kopie zapasowe były wykonywane w ramach dziennego zadania kopii podstawowej oraz tygodniowego zadania kopii z kopii[31]. Kopie w cyklu tygodniowym były rejestrowane na liście kontrolnej poprawności zapisu stanowiącej załącznik Z2 do procedury PS10.

W trakcie oględzin przeprowadzono próbne odzyskiwanie danych z kopii zapasowej[32], odzyskany plik otworzył się prawidłowo.

Kopie wykonywano na macierzach dyskowych, które przechowywano w oddzielnym pomieszczeniu w metalowej szafie.

Do tworzenia i testowania kopii używano ww. oprogramowania Veeam Backup, testowanie kopii było wykonywane automatycznie i było zapisywane w rejestrze kopii zapasowych.

(akta kontroli str. 777 – 784)

Nie tworzono kopi zapasowych na taśmach magnetycznych, płytach CD i DVD, co szerzej opisano w sekcji *Stwierdzone nieprawidłowości.*

2.13. Do monitorowania zajętości dysków serwerów w Urzędzie wykorzystywano aplikację vSphere Client, w której ustalono parametry progów ostrzegawczych:
- 75 % zajętości, informacja o przekroczeniu poziomu ostrzegawczego,
- 85% zajętości, informacja o przekroczeniu poziomu krytycznego.

(akta kontroli str. 786)

W trakcie oględzin trzech serwerów fizycznych, na których uruchomione były maszyny wirtualne ustalono, że zajętość dysków wyniosła od 52% do 58%.

(akta kontroli str. 785)

[30] W dniu 27 czerwca 2024 r.
[31] Stosownie do Procedury PS 10.
[32] Z 27 kwietnia 2024 r.

2.14. Jak wyjaśnił Burmistrz, *kluczowe elementy infrastruktury IT zostały wymienione w scenariuszach postępowania w przypadku awarii i obejmują serwery i elementy aktywne sieci; UTM, switche. Awaryjność łącza internetowego została rozwiązana poprzez zastosowanie dwóch niezależnych przyłączy należących do różnych dostawców Internetu. Elementy kluczowe są zlokalizowane w serwerowni, do której dostęp mają tylko uprawnione osoby – pracownicy Biura Informatyki. Jest ona zabezpieczona atestowanymi zamkami, wyposażona w sygnalizację włamań i pożaru (serwer środowiska), klimatyzację oraz zasilacze awaryjne dla kluczowych elementów infrastruktury.*
Natomiast odnośnie czasu wymaganego do przywrócenia systemów oraz procesów do działania Burmistrz wyjaśnił, że *takie czynności są podejmowane niezwłocznie po stwierdzeniu awarii systemu informatycznego.*

(akta kontroli str. 835)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki, w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:

Kopie zapasowe danych i oprogramowania tworzono jedynie na macierzach dyskowych, pomimo że - zgodnie z obowiązującą procedurą PS 10, pkt 4 lit D - należało dodatkowo tworzyć również kopie zapasowe na taśmach magnetycznych bądź płytach CD lub DVD.

(akta kontroli str. 163 i 781)

Jak wyjaśnił Kierownik Biura Informatyki, *w wyniku modernizacji w czerwcu 2023 r. infrastruktury technicznej w ramach projektu „Cyfrowa Gmina", odstąpiłem od sporządzania kopii zapasowych na nośnikach zewnętrznych jak taśmy magnetyczne i płyty CD/DVD, co w konsekwencji spowodowało również odstąpienie od ich przechowywania w wydzielonym pomieszczeniu i/lub szafie/sejfie. Obecnie kopie tworzy się tylko na macierzach dyskowych, które są przechowywane w oddzielnym pomieszczeniu – wydzielonej serwerowni. W wyniku zmiany sposobu sporządzania kopii zapasowej, nie dokonano aktualizacji procedur dotyczących tworzenia kopii zapasowych oraz sposobu i miejsca ich przechowywania, gdyż rozpoczęła się procedura związana z aktualizacją całego Systemu Zarządzania Bezpieczeństwem Informacji i Ochrony Danych Osobowych w związku z przystąpieniem do rządowego programu „Cyberbezpieczny Samorząd".*

(akta kontroli str. 836)

Według NIK, Kierownik Biura Informatyki nie jest uprawniony do zmiany zasad dotyczących tworzenia kopii zapasowych, wynikających z procedur przyjętych zarządzeniem Burmistrza.

OCENA CZĄSTKOWA

W ocenie NIK, Urząd podejmował działania mające na celu zapewnienie warunków dla prawidłowej organizacji bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych. Przy tworzeniu kopii zapasowych zbiorów danych ograniczono się do jedynie macierzy dyskowych, pomimo że obowiązujące procedury wymagały wykorzystania w tym zakresie również taśm magnetycznych, płyt CD, DVD.

OBSZAR

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

3.1. Urząd na przełomie listopada i grudnia 2023 r., stosownie do § 20 ust. 2 pkt 3 rozporządzenia KRI, dokonał analizy ryzyka utraty integralności, poufności lub dostępności informacji za 2023 r.

Jak opisano w pkt. 1.4. niniejszego wystąpienia zidentyfikowano ryzyko związane z potrzebą zachowania ciągłości działania systemów informatycznych, które mogło stanowić zagrożenie zachowania integralności, poufności i dostępności. W celu zminimalizowania ww. ryzyka zaplanowano zakup agregatu zasilającego oraz dostosowanie instalacji zasilającej budynek Urzędu. Ww. plan został zatwierdzony przez Burmistrza.

(akta kontroli str. 280 – 333)

Jednym z zadań zaplanowanych w ramach Programu „Cyberbezpieczny Samorząd", do którego przystąpiono z dniem 24 czerwca 2024 r., miała być dostawa i montaż agregatu prądotwórczego dla budynku Urzędu.

(akta kontroli str. 570)

3.2. Urząd zapewnił możliwość bezzwłocznego zgłaszania incydentów w zakresie bezpieczeństwa informacji, danych osobowych przez pracowników i incydentów cyberbezpieczeństwa poprzez opracowanie i wdrożenie procedury PS05[33], z którą zapoznano wszystkich pracowników Urzędu.

(akta kontroli str. 130 – 134)

W okresie od 29 maja 2023 r. do 12 czerwca 2024 r. odnotowano łącznie 97 zgłoszeń-incydentów[34], np. zgłoszono blokadę konta użytkowania w systemie informatycznym, zagubienie listu przez operatora pocztowego.

(akta kontroli str. 788 – 794)

Jak wyjaśnił Pełnomocnik ds. bezpieczeństwa informacji, *brak danych o wcześniejszych zgłoszeniach incydentów wynikał, ze zmiany oprogramowania, w których rejestrowano zdarzenia. Na dzień dzisiejszy Urząd nie posiada już aktualnej licencji do użytku wcześniejszego oprogramowania (do rejestracji incydentów) i nie ma możliwości odczytu tych danych. W przypadku zaistnienia incydentów podejmowane działania zaradcze polegały m.in., na przypomnieniu wszystkim pracownikom określonych procedur wskazanych w Polityce SZBI, a w przypadku awarii sprzętu i oprogramowania dokonywana była ich naprawa*.

(akta kontroli str. 838)

3.3. W okresie objętym kontrolą w Urzędzie przeprowadzono 21 szkoleń indywidualnych dla nowo zatrudnianych pracowników w zakresie ochrony danych osobowych i systemu zarządzania bezpieczeństwem informacji Urzędu.
Wysłano również 12 informacji przypominających lub wyjaśniających kwestie związane z bezpieczeństwem informacji do wszystkich pracowników Urzędu.

(akta kontroli str. 795 – 822)

Ponadto w tym samym czasie zorganizowano i przeprowadzono dwa szkolenia w formie webinarów w zakresie „Retencja danych osobowych w BIP", w którym wzięło udział 13 pracowników Urzędu[35] oraz „Przetwarzanie danych osobowych

[33] Zarządzanie incydentami, niezgodnościami oraz działania korygujące, dokument opisywał działania jakie należy podejmować w przypadku incydentów bądź niezgodności wynikłych w trakcie przetwarzania danych oraz dokumentowanie działań korygujących.

[34] Zgłoszenia dotyczyły w 28% (27) problemów z zalogowaniem się użytkownika do systemu za pośrednictwem hasła, w 1% (1) problemów z zalogowaniem się użytkownika do systemu za pośrednictwem karty uwierzytelniającej, w 2% (2) zagubieniem listu przez operatora pocztowego, w 53% (51) awarii oprogramowania oraz w 16% (16) były to zgłoszenia testowe lub nieodzwierciedlające stanu faktycznego.

[35] Szkolenie przeprowadzono w dniu 4 kwietnia 2024 r. ilość przeszkolonych stanowiła 11,5% wszystkich pracowników Urzędu (113 zatrudnionych).

w BIP JST – jak zapewnić zgodność z RODO?", w których wzięło udział sześciu pracowników Urzędu[36] oraz siedmiu przedstawicieli jednostek podległych Gminie. Ponadto, 65 pracowników Urzędu uczestniczyło w szkoleniu przeprowadzonym przez firmę zewnętrzną, tematem szkolenia był „Bezpieczny pracownik", szkolenie obejmowało m.in. cyberbezpieczeństwo oraz metody ochrony przed atakami komputerowymi i socjotechnicznymi[37].

(akta kontroli str. 823 – 833)

Jak wyjaśnił Pełnomocnik ds. bezpieczeństwa informacji*, posiadany budżet na dany rok na szkolenia w zakresie bezpieczeństwa informacji pozwala na zorganizowanie tylko jednego takiego szkolenia, które co roku planuję*.

(akta kontroli str. 838)

3.4. W Urzędzie we wrześniu 2023 r. stosownie do § 20 ust. 2 pkt 14 rozporządzenia KRI przeprowadzono okresowy audyt wewnętrzny z zakresu bezpieczeństwa informacji. W wyniku przeprowadzonego audytu sformułowano zalecenia poaudytowe.

(akta kontroli str. 432 – 433)

Audytor Urzędu po przeprowadzonej kontroli sprawdzającej, w dniu 16 kwietnia 2024 r., stwierdził wykonanie wszystkich rekomendacji.

(akta kontroli str.446 – 449)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki, w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

OCENA CZĄSTKOWA

NIK ocenia pozytywnie działania Urzędu dotyczące: prowadzenia okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji, przeprowadzenia audytu wewnętrznego z zakresu informacji oraz zapewnienie szkoleń osób zaangażowanych w proces przetwarzania informacji.

Wniosek

IV. Wniosek

W związku ze stwierdzoną nieprawidłowością, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, wnosi o podjęcie działań mających na celu w pełni realizowanie procedury tworzenia kopii zapasowych na nośnikach zewnętrznych lub dostosowanie tej procedury do aktualnych potrzeb Urzędu w tym zakresie.

V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

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

[36] Szkolenie przeprowadzono w dniu 23 maja 2024 r. ilość przeszkolonych stanowiła 5,3% wszystkich pracowników Urzędu (113 zatrudnionych).

[37] Szkolenie przeprowadzono w dniu 14 grudnia 2023 r. ilość przeszkolonych stanowiła 59,1% wszystkich pracowników Urzędu (110 zatrudnionych).

Obowiązek poinformowania NIK o sposobie wykonania wniosku

Zgodnie z art. 62 ustawy o NIK, należy poinformować Najwyższą Izbę Kontroli, w terminie 21 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykonania wniosku pokontrolnego 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.

Katowice, dnia 20 września 2024 r.

Kontroler
Jerzy Piasecki
Gł. specjalista kontroli państwowej

.....

Najwyższa Izba Kontroli
Delegatura w Katowicach