NAJWYŻSZA IZBA KONTROLI
Delegatura w Katowicach

LKA.410.14.3.2024

Pan
dr Marian Błachut
Burmistrz
Czechowic-Dziedzic

Plac Jana Pawła II 1
43-502 Czechowice-Dziedzice

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 Czechowicach-Dziedzicach[1], Plac Jana Pawła II 1, 43-502 Czechowice-Dziedzice.

Kierownik jednostki kontrolowanej

Marian Błachut, Burmistrz Miasta i Gminy Czechowice-Dziedzice od 26 listopada 2006 r.[2]

(akta kontroli str. 3)

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 19 sierpnia 2024 r. (a także okresy wcześniejsze w zakresie uczestnictwa w programie Cyfrowa Gmina).

Podstawa prawna podjęcia kontroli

Art. 2 ust. 2 ustawy o NIK ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[3]

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli Delegatura w Katowicach

Kontrolerzy

1. Magdalena Śleziak, specjalista kontroli państwowej, upoważnienie do kontroli nr LKA/122/2024 z dnia 29 maja 2024 r.
2. Szymon Gruca, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LKA/177/2024 z dnia 6 sierpnia 2024 r.

(akta kontroli str.1-2)

[1] Dalej: Urząd.

[2] Dalej: Burmistrz.

[3] Dz. U. z 2022 r. poz. 623, dalej: ustawa o NIK.

II. Ocena ogólna[4] kontrolowanej działalności

OCENA OGÓLNA

W Urzędzie opracowano i wdrożono System Zarządzania Bezpieczeństwem Informacji[5] w rozumieniu § 19 ust. 1-3 rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności[6], minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[7]. Prawidłowo realizowano zadania dotyczące m.in.: opracowania dokumentacji w zakresie bezpieczeństwa przetwarzania danych osobowych i jej dostosowania do wymogów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[8].

W Polityce Bezpieczeństwa Informacji[9] Urzędu[10] i jej aktualizacji[11] zostały zidentyfikowane zbiory danych podlegające zabezpieczeniu, jednakże nie przypisano im odpowiedniego poziomu ochrony oraz nie określono do nich wag. Plan ochrony i zapewnienia ciągłości działania Urzędu[12] nie był kompletny, gdyż nie zawierał: procedur typologii sieci, systemowych serwerów wirtualnych oraz urządzeń brzegowych, jak i procedury czasu przywrócenia ciągłości działania, a także nie podlegał testowaniu i treningowi. W Urzędzie wyznaczono Zespół ds. bezpieczeństwa informacji. W okresie kontrolowanym Urząd dokonał przeglądu PBI. W Urzędzie wdrożono i wykorzystywano rozwiązania organizacyjne i techniczne, w tym m.in. w zakresie polityki haseł, jak i zabezpieczenia komputerów służbowych przed zainstalowaniem na nich nieautoryzowanego oprogramowania, komputery na stanowiskach pracy w miejscach obsługi obywateli zabezpieczone były przed wglądem osób nieuprawnionych, a pracownicy merytoryczni mieli dostęp do oprogramowania zgodnie z rejestrem prowadzonym przez Wydział Informatyki.

W okresie objętym kontrolą w Urzędzie podjęto działania w celu zapobiegania incydentom bezpieczeństwa informacji tj. przeprowadzono okresowe analizy ryzyka utraty integralności, poufności lub dostępności informacji, przeprowadzono też okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji. Urząd nie zidentyfikował kluczowych elementów infrastruktury i usług IT. W serwerowni, tj. pomieszczeniu podlegającemu szczególnej ochronie, znajdowały się materiały łatwopalne, tj. kartony i sprzęt komputerowy w kartonach, co zwiększało ryzyko utraty danych bądź przerwania ciągłości operacji na skutek pożaru.

---

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

[5] Dalej: SZBI.

[6] Dalej KRI.

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

[8] Dz.Urz.UE.L z 04.05.2016 Nr 119, str. 1, ze zm. Dalej: RODO.

[9] Dalej PBI.

[10] Wprowadzonej Zarządzeniem nr 120.24.2021 z dnia 29 marca 2021 r.

[11] Wprowadzonej Zarządzeniem nr 120.65.2023 z dnia 6 lipca 2023 r.

[12] Wprowadzony Zarządzeniem nr 120.32.2022 z dnia 5 kwietnia 2022 r.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[13] kontrolowanej działalności

OBSZAR

1. Organizacja bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych

1.1. Urząd w rozdziale VIII pn. *Rodzaje przetwarzanych informacji* w *Polityce Bezpieczeństwa Informacji Urzędu Miejskiego w Czechowicach-Dziedzicach wprowadzonej Zarządzeniem nr 120.24.2021 Kierownika Urzędu Miejskiego w Czechowicach-Dziedzicach z dnia 29 marca 2021 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji Urzędu Miejskiego w Czechowicach-Dziedzicach*[14], skrótowo wskazał, że *w Urzędzie poszczególne informacje są chronione na podstawie przepisów prawa*, a PBI obejmuje cztery grupy informacji tj.: dane osobowe; informacje publiczne; informacje finansowe i skarbowe; informacje stanowiące tajemnicę przedsiębiorstwa[15]. PBI zostało zaktualizowane w zakresie ww. rozdziału VIII (Zarządzeniem nr 120.65.2023 z dnia 6 lipca 2023 r.) i do ww. grupy informacji dodano[16]: informacje z ograniczoną dostępnością; informacje statystyczne; informacje strategiczne; oraz do każdej grupy informacji[17] wyszczególniono dokumentację. Do poszczególnych zidentyfikowanych grup informacji Urząd nie przypisał poziomu ochrony, oraz nie określił ich istotności (wagi), co opisano w *Sekcji stwierdzone nieprawidłowości*.

(akta kontroli str. 24-31)

1.2. Zgodnie z § 20 ust. 1 w związku z ust. 3 rozporządzenia KRI w Urzędzie został opracowany, ustanowiony i wdrożony SZBI.

(akta kontroli str. 24-209)

Na SZBI Urzędu składały się następujące dokumenty wewnętrzne:

a) Zarządzenie Kierownika Urzędu nr 120.56.2020 z dnia 26 listopada 2020 r. w sprawie ustanowienia SZBI w Urzędzie Miejskim w Czechowicach-Dziedzicach, zmienione trzykrotnie. W okresie objętym kontrolą ww. Zarządzenie jednokrotnie zmienione (zmiana wprowadzona Zarządzeniem nr 120.90.2023 z dnia 21 września 2023 r.) dotyczyła głównie składu osobowego Zespołu ds. Systemu Zarządzania Bezpieczeństwem Informacji.

(akta kontroli str. 205-209)

b) PBI opisana w pkt.1.1.

(akta kontroli str. 24-31)

c) Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych

[13] 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.

[14] Obowiązująca od 29 marca 2021 r. do nadal. Dalej: PBI.

[15] Ponadto w rozdziale tym podano, że PBI nie obejmuje informacji niejawnych w rozumieniu ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

[16] Grupa informacji pn. Informacje finansowe i skarbowe w PBI, w aktualizacji PBI została rozdzielona na: Informacje finansowe, Informacje skarbowe.

[17] Przykładowo do grupy informacji pn. Dane osobowe – wyszczególniono, że: wszystkie dokumenty zawierające dane osobowe zgłoszone do procesów RODO; do grupy informacji pn. informacje finansowe - wyszczególniono: sprawozdania finansowe, sprawozdania budżetowe, Budżet Gminy, Budżety poszczególnych komórek organizacyjnych, Plan finansowy; do grupy informacji statystycznych – wyszczególniono: Sprawozdania statystyczne do GUS, statystyka na potrzeby innych komórek Urzędu (IZD).

wprowadzona zarządzeniem nr 120.13.2021 Kierownika Urzędu Miejskiego w Czechowicach-Dziedzicach z dnia 26 lutego 2021 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych w Urzędzie Miejskim w Czechowicach-Dziedzicach oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Czechowicach-Dziedzicach (obowiązująca od 26.02.2021 do 13 lipca 2023 r.).

(akta kontroli str. 68-112)

- Została ona zastąpiona przez:

- Politykę Ochrony Danych Osobowych w Urzędzie Miejskim w Czechowicach-Dziedzicach wprowadzoną zarządzeniem nr 120.69.2023 Kierownika Urzędu Miejskiego w Czechowicach-Dziedzicach z dnia 13 lipca 2023 r.[18].

(akta kontroli str. 32-67)

- Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania informacji w Urzędzie Miejskim w Czechowicach-Dziedzicach wprowadzoną zarządzeniem nr 120.68.2023 Kierownika Urzędu Miejskiego w Czechowicach-Dziedzicach z dnia 13 lipca 2023 r.[19].

(akta kontroli str. 113-123)

d) Plan ochrony i zapewnienia ciągłości działania Urzędu Miejskiego w Czechowicach-Dziedzicach wprowadzony zarządzeniem nr 120.32.2022 Kierownika Urzędu Miejskiego w Czechowicach-Dziedzicach z dnia 5 kwietnia 2022 r.[20].

(akta kontroli str. 124-151)

e) Zasady postępowania z kluczami oraz zabezpieczenia budynków i pomieszczeń Urzędu Miejskiego w Czechowicach-Dziedzicach wprowadzone zarządzeniem nr 120.96.2021 Kierownika Urzędu Miejskiego w Czechowicach-Dziedzicach z dnia 10 listopada 2021 r.[21].

(akta kontroli str. 152-160)

f) Instrukcja zarządzania ryzykiem w bezpieczeństwie informacji w Urzędzie Miejskim w Czechowicach-Dziedzicach wprowadzona zarządzeniem nr 120.45.2021 Kierownika Urzędu Miejskiego w Czechowicach-Dziedzicach z dnia 8 czerwca 2021 r.[22].

(akta kontroli str. 161-166)

---

[18] w sprawie wprowadzenia Polityki Ochrony Danych Osobowych w Urzędzie Miejskim w Czechowicach-Dziedzicach obowiązująca od 13 lipca 2023 do nadal. Dokument ten regulował również kwestie związane ze zgłaszaniem incydentów bezpieczeństwa (§ 16). Dalej: Polityka Ochrony Danych Osobowych.

[19] w sprawie wprowadzenia Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania informacji w Urzędzie Miejskim w Czechowicach-Dziedzicach (obowiązuje od 13 lipca 2023 r. do nadal). Dalej: Instrukcja Zarządzania Systemem Informatycznym.

[20] w sprawie wprowadzenia planu ochrony i zapewnienia ciągłości działania Urzędu Miejskiego w Czechowicach-Dziedzicach. Obowiązuje od 5 kwietnia 2022 r. do nadal. Dalej: Plan ochrony i zapewnienia ciągłości działania.

[21] w sprawie zasad postępowania z kluczami oraz zabezpieczenia budynków i pomieszczeń Urzędu Miejskiego w Czechowicach-Dziedzicach (obowiązuje od 10 listopada 2021 r. do nadal). Dokument ten regulował również kwestie związane z fizycznym dostępem do pomieszczeń (w tym serwerowni).

[22] w sprawie wprowadzenia instrukcji zarządzania ryzykiem w bezpieczeństwie informacji w Urzędzie Miejskim w Czechowicach-Dziedzicach (obowiązuje od 8 czerwca 2021 r. do nadal). Dalej: Instrukcja zarządzania ryzykiem.

g) Polityka Cyberbezpieczeństwa w Urzędzie Miejskim w Czechowicach-Dziedzicach wprowadzona zarządzeniem nr 120.96A.2021 Kierownika Urzędu Miejskiego w Czechowicach-Dziedzicach z dnia 10 listopada 2021 r.[23].

(akta kontroli str.167-176)

h) Regulamin wykonywania pracy zdalnej wprowadzony zarządzeniem nr 120.66.2023 Kierownika Urzędu Miejskiego w Czechowicach-Dziedzicach z dnia 10 lipca 2023 r.[24].

(akta kontroli str. 177-204)

1.3. W Urzędzie opracowano Polityki Ochrony Danych Osobowych, które zawierały zasady obowiązujące przy przetwarzaniu danych osobowych oraz procedury i instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych, uwzględniające wymagania RODO.

(akta kontroli str. 32-112)

Burmistrz w wyjaśnieniach podał, że Urząd opracowane, zatwierdzone Polityki Ochrony Danych Osobowych każdorazowo zakomunikował pracownikom, pracownicy uczestniczyli w szkoleniach zorganizowanych przez IOD.

(akta kontroli str. 16)

1.4. W Urzędzie analiza ryzyka przeprowadzona była na podstawie Instrukcji zarządzania ryzykiem (Zarządzenia Nr 120.45.2021), analizą tą objęte były wszystkie wydziały, biura i samodzielne stanowiska pracy.

(akta kontroli str. 622-660)

I Z-ca Burmistrz w wyjaśnieniach podał, że *wszystkie komórki organizacyjne rokrocznie składały do Biura Audytu i Kontroli jednostkowe rejestry ryzyka. W większości przypadków, istotność ryzyka wykazywana przez wydziały, biura, samodzielne stanowiska pracy szacowana jest na poziomie akceptowalnym warunkowo, akceptowalnym lub pomijanym. Wysokie ryzyka wykazuje Wydział Informatyki jako wydział z najwyższym poziomem świadomości zagrożeń w środowisku informatycznym.*

(akta kontroli str. 617-620)

W rejestrze ryzyka Wydziału Informatyki na rok 2024 r. wykazano wysoki poziom ryzyka (istotność 12) w zakresie:

- zapewnienia personelu dla ryzyka naruszenia dostępności personelu (nieobecność pracownika, system zastępstw);
- zapewnienia odpowiedniego sprzętu (serwery zbiorczo) dla ryzyka zalania;

W roku poprzednim ww. Wydział wskazał w zakresie ryzyk te same ww. ryzyka, oraz dwa inne:

- zapewnienie odpowiedniego sprzętu serwery zbiorczo dla ryzyka utraty dostaw prądu;
- zapewnienie odpowiedniego sprzętu 750/4/2352/serwer dla ryzyka awaria, oraz ryzyka zdolności utrzymania systemu informatycznego.

(akta kontroli str. 621-655)

[23] w sprawie wprowadzenia Polityki Cyberbezpieczeństwa w Urzędzie Miejskim w Czechowicach-Dziedzicach (obowiązuje od 10 listopada 2021 r. do nadal). Dalej: Polityka Cyberbezpieczeństwa.

[24] w sprawie wprowadzenia Regulaminu wykonywania pracy zdalnej (obowiązuje od 10 lipca 2023 r. do nadal). Regulamin reguluje kwestie związane z pracą na odległość, oraz mobile przetwarzanie danych. Dalej: Regulamin pracy zdalnej.

Audytor wewnętrzny Urzędu opracowała *Zbiorczą informacja o zidentyfikowanych ryzykach w obszarze bezpieczeństwa informacji na 2023 r.* na podstawie jednostkowych rejestrów ryzyka złożonych przez 25 naczelników/kierowników bądź pracowników zatrudnionych na samodzielnych stanowiskach pracy. W ww. informacji przestawiono zestawienie ryzyk, których poziom jest krytyczny i nieakceptowalny w przedziale od 12-25 pkt. W ww. zestawieniu m.in. zidentyfikowano następujące ryzyka (o istotności 12):

- zapewnienie personelu w Wydziale Informatyki – rekomendowano wzmocnić kadrowo Wydział Informatyki o dodatkową osobę m.in. w związku tematem e-doręczeń, infrastruktury technicznej i bazodanowej;
- zmiana pomieszczenia serwerowni – relokacja części serwerów (ryzyko zalania) – akceptacja obecnego poziomu ryzyka – z powodu braku możliwości rozwiązania problemu – brak możliwości rozwiązania problemu akceptacja obecnego poziomu ryzyka;
- utrata dostaw prądu w zakresie zapewnienia odpowiedniego sprzętu – serwery zbiorczo – rekomendacja w IV kwartale 2023 r. ze środków pochodzących z ewentualnych oszczędności Wydziału Informatyki zakupić nowy jeden UPS;
- awaria serwera o 750/4/2352/serwer obsługującego dwa wydziały tj. Świadczeń Socjalnych i Wydział Spraw Obywatelskich – rekomendowano wdrożenia wieloletniego planu restrukturyzacji infrastruktury serwerowej z budżetem rocznym na poziomie 150 tys. zł.

Audytor wewnętrzny przygotowała również Zbiorczą informację o zidentyfikowanych ryzykach w obszarze bezpieczeństwa informacji na 2024 r. (dokument roboczy, przed zwołaniem Zespołu ds. Bezpieczeństwa Informacji i opracowania rekomendacji do zdiagnozowanych ryzyk). Na podstawie złożonych jednostkowych rejestrów w Zbiorczej informacji o zidentyfikowanych ryzykach w obszarze bezpieczeństwa informacji na 2024 rok wykazano m.in.: zalanie serwerowni (istotność 12); zapewnienie personelu w Wydziale Informatyki (istotność 12).

(akta kontroli str. 656-660, 769-772)

1.5. W Urzędzie został ustanowiony Plan ochrony i zapewnienia ciągłości działania (wprowadzony zarządzeniem nr 120.32.2022)[25]. Jednakże ww. Plan nie był kompletny, gdyż nie zawierał: procedur: typologii sieci, systemowych serwerów wirtualnych oraz urządzeń brzegowych, jak i procedury czasu przywrócenia ciągłości działania (co opisano w *Sekcji stwierdzone nieprawidłowości*).

Dokument ten został przekazany pracownikom do zapoznania się poprzez system Elektronicznego Obiegu Dokumentów[26]. W okresie objętym kontrolą ww. Plan nie był aktualizowany.

(akta kontroli str. 124-150, 368-375, 690-698)

W związku z powyższym, I Z-ca Burmistrza wyjaśnił, że: Plan ochrony i zapewnienia ciągłości działania (…) nie były aktualizowany, ponieważ z dokonanych przeglądów wynikało, że aktualizacja nie jest konieczna.

(akta kontroli str. 796-803)

[25] Z podziałem na rozdziały: *Rodzaj działalności jednostki (rozdział I); Charakterystykę obiektów (rozdział II); Analizę potencjalnych zagrożeń (rozdział III)* – w rozdziale tym wymieniono potencjalne zagrożenia z podziałem na: zdarzenia losowe zewnętrzne i wewnętrzne, oraz umyślne zdarzenia*; Ocenę aktualnego stanu ochrony jednostki i opis technicznych zabezpieczeń obiektu (rozdział IV)* – w rozdziale tym wymienione budynki i¨pomieszczenia oraz zastosowane w nich zabezpieczenia; *Skład, organizacja, zadania i zakres działania Służby Ochronnej (rozdział VI), Rekomendowane działania podejmowane w przypadku wystąpienia zagrożeń i zakłóceń (rozdział VII)*.

[26] Dalej: EZD.

1.6. W Urzędzie został opracowany Plan ochrony i zapewnienia ciągłości działania z dnia 5 kwietnia 2022 r. nie był on jednak kompletny co opisano w punkcie 1.5. niniejszego wystąpienia, natomiast zawierał on uregulowania w kwestii zasilania, które ujęte zostały w pkt 6 rozdziału VII pn. *Rekomendowane działania w przypadku zakłóceń lub braku zasilania elektrycznego.* W ww. Planie określono działania jakie należy podjąć w przypadku braku zasilania elektrycznego, a poszczególnym działaniom przypisano osoby lub Wydziały wyznaczone do realizacji działań naprawczych. Natomiast w pkt 9 ww. rozdziału w sposób ogólny opisano *Rekomendowane działania w przypadku awarii urządzeń teleinformatycznych* z podziałem na:

- *skutki: brak możliwości pracy w systemach komputerowych; możliwość utraty danych zawartych w systemach komputerowych.*
- *reakcja: przywrócenie sprawności urządzeń teleinformatycznych; w przypadku utraty danych próba przywrócenia danych z kopii archiwalnych*,

a poszczególnym działaniom przypisano osoby odpowiedzialne za wykonywanie tych działań, przykładowo działaniu pn.: *Opracowanie planu i harmonogramu przywrócenia działania urządzeń teleinformatycznych oraz odtworzenia utraconych danych* przypisano wykonanie: *Naczelnicy wydziałów, kierownicy biur, w których wystąpiła awaria w uzgodnieniu z Naczelnikiem WI, Naczelnikiem Wydziału Organizacyjnego i Kadr za zgodą Burmistrza.*

(akta kontroli str. 124-151)

Burmistrz w wyjaśnieniach podał, że Plan ochrony i zapewnienia ciągłości nie dokonuje podziału na sieć komputerową, macierze dyskowe czy urządzenia brzegowe.

(akta kontroli str. 368-375)

Urząd opracował Procedurę dotyczącą kopii zapasowych oraz Procedurę wykonywania przeglądów, konserwacji i napraw, które zawarł w obowiązującej Instrukcji Zarządzania Systemem Informatycznym, jak i w poprzedniej. W obu ww. Instrukcjach Procedura zarządzania kopiami zapasowymi była taka sama i określała, że kopie zapasowe baz danych przechowywane są w zamykanym sejfie, do którego dostęp posiada Naczelnik Wydziału Informatyki lub osoby przez niego upoważnione.

(akta kontroli str. 68-123)

W Urzędzie nie określono akceptowalnego czasu przywrócenia ciągłości działania systemów informatycznych Urzędu (co opisano w *Sekcji stwierdzone nieprawidłowości)*.

(akta kontroli str. 124-151, 946)

1.7. Burmistrz w wyjaśnieniach podał, że: *Plany zapewnienia ciągłości działania i plany odtworzeniowe nie podlegały w okresie kontroli testowaniu i treningowi. W ramach projektu Cyberbezpieczny Samorząd planowane jest podniesienie jakości procedur i realnych możliwości w zakresie ciągłości działania i planów odtwarzania poprzez: zakup serwera do testowania kopii i pełniącego funkcję nadmiarową, stworzenie procedur odtwarzania i procedur ich testowania.* Brak testowania Planu ochrony i zapewnienia ciągłości działania (przedstawiono szczegółowo w *Sekcji stwierdzone nieprawidłowości).*

(akta kontroli str. 371-375)

1.8. W okresie objętym kontrolą zaktualizowano: PBI (z dniem 6 lipca 2023 r.) oraz Politykę Ochrony Danych Osobowych (z dniem 13 lipca 2023 r.), Instrukcję Zarządzania Systemem Informatycznym (z dniem 13 lipca 2023 r.), jak

i wprowadzono zmiany do Zarządzenia ustanawiającego SZBI (z dniem 21 września 2023 r.).

(akta kontroli str. 30-67, 113-123, 205-209)

Aktualizacja dotycząca PBI została opisana w pkt.1.1., natomiast zmiany dotyczące Zarządzenia wprowadzającego SZBI opisano w pkt.1.2.

Zarządzeniem nr 120.69.2023 z dnia 13 lipca 2023 r., Burmistrz wprowadził do stosowania i przestrzegania kolejną Politykę Ochrony Danych Osobowych, do której wprowadzono następujące zmiany: uaktualniono zapisy dotyczące środków technicznych (§ 5) oraz środków organizacyjnych (§ 6); uwzględniono ochronę danych osobowych w fazie projektowania oraz domyślną ochronę danych (§ 4); w zapisach Polityki uwzględniono procedurę spełnienia obowiązku informacyjnego (§ 11); uaktualniono zapisy dotyczące audytu IOD (§ 20); uwzględniono ochronę danych osobowych w fazie projektowania oraz domyślna ochrona danych (art. 25 RODO).

(akta kontroli str. 32-67)

Zarządzeniem nr 120.68.2023 z dnia 13 lipca 2023 r. wprowadzono kolejną Instrukcję Zarządzania Systemem Informatycznym, w której w stosunku do poprzedniej uzupełniono zapisy tj. rozszerzono słownik definicji o PBI o „informacje" i „PBI", oraz usunięto definicje związane z Polityką ochrony danych osobowych (§ 2); wprowadzono Procedurę szkoleń (§ 4), oraz Procedurę utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania (§ 5); wydłużono okresu ważności hasła do 6 m-cy, z jednoczesnym zwiększeniem ilości znaków w haśle z 8 do 12 (§ 8); szyfrowanie danych przesyłanych mailem rozszerzono również na inne informacje nie tylko dane osobowe, ale również te w stosunku do których wymagane jest zachowanie poufności (§ 12); wprowadzono rejestr wydanych przenośnych nośników informacji (§ 13); rozszerzono konieczność szyfrowania sprzętu również na sprzęt zawierający informacje w stosunku do których wymagane jest zachowanie poufności (§ 14).

(akta kontroli str. 113-123)

Burmistrz w zakresie przeglądów podał, że: Urząd Miejski (…) poddał przeglądowi PBI. W dokumentacji SZBI nie wskazano zaplanowanych przeglądów. Wykonywane są one w odpowiedzi na zmieniające się otoczenie. W okresie objętym kontrolą dokonano aktualizacji: Polityki Bezpieczeństwa Informacji w wyniku przeglądu dokonanego na podstawie polecenia służbowego nr 120.0.1.2022 w sprawie dokonania w Urzędzie Miejskim w Czechowicach-Dziedzicach przeglądu informacji przetwarzanych, a nie będących danymi osobowymi. (…)

(akta kontroli str. 8-23)

Ponadto, Urząd dokonał przeglądów: Polityki Ochrony Danych Osobowych (z dniem 6 marca 2023 r.); Instrukcji Zarządzania Systemem Informatycznym (z dniem 15 lutego 2023 r.); Polityki Cyberbezpieczeństwa (z dniem 30 października 2023 r.) oraz Planu ochrony i zapewnienia ciągłości działania (z dniem 3 kwietnia 2023 r.).

(akta kontroli str. 230-233, 804, 806)

1.9. W Urzędzie:

- za bezpieczeństwo informacji odpowiadał: Zespół ds. bezpieczeństwa informacji (pięcioosobowy), w skład którego wchodzili: Sekretarz Miasta, Naczelnik Wydziału Informatyki, Z-ca Naczelnika Wydziału Informatyki, Naczelnik Wydziału Organizacyjnego i Kadr, oraz Kierownik Biura Audytu i Kontroli (audytor);

- za bezpieczeństwo fizyczne i środowiskowe odpowiadała: Naczelnik Wydziału Organizacyjnego i Kadr;
- za bezpieczeństwo ochrony danych osobowych: Inspektor Ochrony Danych[27], Z-ca IOD, oraz Administrator Systemów Informatycznych[28] oraz osoba odpowiedzialna za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa[29].

(akta kontroli str. 124-151, 205-209, 234-237)

1.10. W Urzędzie, zgodnie z art. 36a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, wyznaczono Administratora Bezpieczeństwa Informacji[30] (do 24 maja 2018 r., tj. do dnia wejścia w życie RODO) i zgodnie z art. 37 ust. 1 lit. a RODO w przypadku gdy przetwarzania dokonuje organ lub podmiot publiczny, stosownie do przepisu art. 8 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, administrator wyznaczył Inspektora Ochrony Danych (od 25 maja 2018 r.). Na stanowisko IOD wyznaczono osobę posiadającą odpowiednie przygotowanie i kwalifikacje zawodowe umożliwiające pełnienie tej funkcji oraz terminowo zgłoszono ten fakt Prezesowi Urzędu Ochrony Danych Osobowych.

W Zarządzeniu nr 120.29.2018 z 25 maja 2018 r. powołującym IOD, a także w Regulaminie Organizacyjnym Urzędu Miejskiego w Czechowicach-Dziedzicach wskazano, że IOD podlega bezpośrednio Burmistrzowi (administratorowi) celem zapewnienia niezależności jego działań, co było zgodne z art. 38 ust. 3 RODO. IOD posiadał odpowiednie kwalifikacje, pełnił wcześniej funkcję ABI, brał udział w szkoleniach dotyczących ochrony danych osobowych, ukończył studia podyplomowe.

(akta kontroli str. 234)

Do zadań IOD należało m.in.:

- informowanie administratora oraz pracowników Urzędu o obowiązkach spoczywających na nich wynikających z: RODO, ustawy o ochronie danych osobowych oraz Polityki Ochrony Danych Osobowych;
- monitorowanie przestrzegania RODO, ustawy o ochronie danych osobowych oraz Polityki Ochrony Danych Osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenie personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
- prowadzenie rejestru czynności przetwarzania;
- rejestru naruszeń ochrony danych osobowych;
- współpraca z organem nadzorczym;
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

(akta kontroli str. 245-248)

[27] Dalej: IOD.

[28] Dalej: ASI.

[29] Dalej: ksc.

[30] Dalej: ABI.

Burmistrz w wyjaśnieniach podał, że IOD oraz Z-ca IOD są również członkami Komisji ds. Ochrony Danych Osobowych Śląskiego Związku Gmin i Powiatów z siedzibą w Katowicach.

(akta kontroli str. 23)

W obu Politykach Ochrony Danych obowiązujących w okresie kontrolowanym osobami odpowiedzialnymi za zapewnienie bezpieczeństwa danych osobowych w Urzędzie byli: również naczelnicy wydziałów/ kierownicy biur/ pracownicy na samodzielnych stanowiskach, którzy dokonują doraźnej kontroli fizycznych zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe, mebli (szaf dokumentowych), w których przechowywane są dane osobowe oraz usytuowania monitorów ekranowych w zakresie zapewnienia poufności przetwarzanych danych osobowych.

(akta kontroli str. 32-112)

1.11. IOD oraz Z-ca IOD pełnili również funkcję Pełnomocnika i Zastępcy Pełnomocnika ds. Ochrony Informacji Niejawnych w Urzędzie. Powyższe rozwiązanie nie wpływało na prawidłowe umiejscowienie IOD w strukturze administratora danych (Burmistrza) i wykonywanie jego zadań w sposób niezależny. W zakresie zapewniania przestrzegania przepisów o ochronie danych osobowych, IOD i jego zastępca w strukturze organizacyjnej podlegali bezpośrednio tylko kierownikowi jednostki. W świetle art. 38 ust. 2 RODO administrator zapewnił IOD zasoby niezbędne do wykonywania zadań wskazanych w art. 39 RODO oraz zasoby niezbędne do utrzymania jego fachowej wiedzy.

(akta kontroli str. 11-23, 234-235)

1.12. Zgodnie z art. 21 ust. 1 i 3 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa[31] Burmistrz wyznaczył w Urzędzie pracownika, który był odpowiedzialny za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa (Zarządzeniem nr 120.9.2021 r. z dnia 22 lutego 2021 r.). Osobą tą był inspektor z Wydziału Zarządzania Kryzysowego, Ochrony Ludności i Spraw Obronnych. Zgodnie z art. 22 ust. 1 pkt 5 ustawy o ksc dane ww. osoby, numer telefonu oraz jej adres poczty elektronicznej zostały przekazane terminowo do NASK – Państwowego Instytutu Badawczego CSIRT NASK w Warszawie.

(akta kontroli str. 237, 260-264)

1.13. PBI, jak i jego aktualizacja nie określały jakie dokumenty powinny być sporządzone w ramach zapewnienia bezpieczeństwa informacji. PBI definiowała strukturę dokumentacji SZBI wprowadzając trójpoziomową dokumentację bezpieczeństwa

W obowiązującej dokumentacji SZBI w ramach II poziomu zostały opracowane następujące dokumenty: Polityka Ochrony Danych Osobowych, Instrukcja Zarządzania Systemem Informatycznym, Zasady postępowania z kluczami oraz zabezpieczenia budynków i pomieszczeń Urzędu, Instrukcja zarządzania ryzykiem w bezpieczeństwie informacji, Polityka Cyberbezpieczeństwa, Plan ochrony i zapewnienia ciągłości działania, Regulamin pracy zdalnej.

(akta kontroli str. 24-204)

1.14. Urząd zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI, utrzymywał aktualność inwentaryzacji i oprogramowania w dedykowanym oprogramowaniu zapewniającym

[31] Dz.U. z 2024 r., poz. 1077. Dalej: ustawa o ksc.

ich automatyczną aktualizację w zakresie rodzaju i konfiguracji sprzętu komputerowego a także instalowania/odinstalowania oprogramowania.

(akta kontroli str. 265-266, 962-988)

Inwentaryzacja pozostałego sprzętu Urzędu prowadzona była w arkuszu kalkulacyjnym Excel (serwery i routery).

(akta kontroli str. 267)

W wyniku oględzin[32] oprogramowania wykorzystywanego w Urzędzie do gromadzenia informacji w zakresie posiadanego sprzętu komputerowego stwierdzono, że oprogramowanie to umożliwia bieżący monitoring sprzętu IT oraz zawiera informacje o jego konfiguracji, natomiast poddany oględzinom wybrany serwer oraz router posiadał opis rodzaju i konfiguracji, co było zgodne z § 19 ust. 2 pkt 2 rozporządzenia KRI.

(akta kontroli str.819-848)

1.15. Urząd przystąpił do Programu „Cyberbezpieczny Samorząd – wzmocnienie poziomu cyberbezpieczeństwa w Urzędzie Miejskim i Ośrodku Pomocy społecznej w Czechowicach -Dziedzicach", a umowa o powierzenie grantu (nr RERC.02.02-CS.01-001/23 została podpisana z dniem 22 kwietnia 2024 r. przez Centrum Projektów Polska Cyfrowa[33]). Łączna wartość projektu ogółem wynosiła 934 065,00 zł (w tym dofinasowanie ze środków Unii Europejskiej: 849 999,26 zł, a wkład własny z 84 064,94 zł). Koniec realizacji Projektu został wyznaczony na 21 kwietnia 2026 r. (zgodnie z umową Grantobiorca zobowiązał się zrealizować Projekt w zakresie rzeczowym w okresie maksymalnie 24 miesiące od dnia wejścia w życie Umowy).

(akta kontroli str. 301-339)

W ramach realizacji Projektu w zakresie finansowym w ramach trzech obszarów zaplanowano wykonanie następujących zadań:

1) *Przeprowadzenie kompleksowego audytu zgodności z wymaganiami prawnymi oraz audytu bezpieczeństwa w Urzędzie i OPS* – wydatki ogółem 59 065 zł (w tym dofinansowanie 53 749,20 zł);
2) *Szkolenie dla kadry zarządzającej i pracowników IT (OPS i UM) oraz pracowników IT* – wydatki ogółem 79 999,20 zł (w tym dofinansowanie 72 799,34 zł);
3) *Pełnienie roli inżyniera projektu, zakup sprzętu i oprogramowanie* – wydatki ogółem 795 000 zł (w tym 723 450,72 zł), z czego: inżynier Projektu – wydatki ogółem 40 000 zł (w tym dofinansowanie 36 400,04 zł).

W ramach trzeciego obszaru w Projekcie przewidziano w:

- obszarze technicznym: zatrudnienie inżyniera Projektu; zakupy serwerów dla Urzędu oraz OPS (dla każdego oddzielnie 2);zakup pakietu oprogramowania Windows Server dla Urzędu oraz OPS, zakup pakietu oprogramowania dostępowego CAL (do serwera) dla Urzędu, oraz OPS; zakup urządzenia NAS dla Urzędu, zakup urządzenia typu UTM (dla Urzędu 2 sztuki i dla OPS 1 sztuka); zakup oprogramowania: antywirusowego oraz typu SAM-CMDB dla OPS; zakup urządzenia UPS, oraz przełącznika zarządzalnego dla OPS.

(akta kontroli str. 301-339)

[32] Badanie w zakresie inwentaryzacji sprzętu informatycznego przeprowadzono na podstawie doboru celowego: 10 komputerów stacjonarnych, dwóch laptopów, jednego routera, jednego serwera i jednej drukarki.

[33] Dalej: CPPC.

W ramach Programu przewidziano audyt bezpieczeństwa oraz wykonanie końcowej ankiety dojrzałości cyberbezpieczeństwa.

(akta kontroli str. 331- 339)

Urząd oraz Ośrodek Pomocy Społecznej terminowo przesłał do NASK – Państwowego Instytutu Badawczego Ankiety dojrzałości Ceberbezpieczeństwa, tj. w terminie do 30 dni od zawarcia umowy o powierzenie grantu. W ankiecie dotyczącej Urzędu m.in. wskazano, że planuje się: przeprowadzić szkolenie dla kadry zarządzającej w zakresie cyberbezpieczeństwa, wykonać inwentaryzację aktywów, dodać kluczowe aktywa do rejestru ryzyk, włączyć zagrożenia związane z cyberbezpieczeństwem w procesy zarządcze, utworzyć proces dot. identyfikowania i dokumentowania podatności; planowany zakup kontrolera domeny i sukcesywne wdrażanie Active Directory, zwiększyć bezpieczeństwo danych poprzez zakup urządzenia typu NAS do gromadzenia kopii zapasowych i zakup serwera do testowania kopii i pełniącego funkcję nadmiarową; stworzenie procedur oraz realnych możliwości odtwarzania poprzez zakup serwera nadwymiarowego.

(akta kontroli str. 297-300, 340-359)

Stwierdzone nieprawidłowości

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

1. Urząd do zidentyfikowanych grup informacji określonych w PBI, oraz w aktualizacji PBI nie przypisał odpowiedniego poziomu ochrony, zgodnego z ich wagą. Informacje te nie zostały sklasyfikowane z uwzględnieniem wymagań prawnych wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację, co było nierzetelne. Ponadto zgodnie z pkt A.8.1.1 i A.8.2.1 załącznika A normy PN-EN ISO/IEC 27001:2017, stanowiącymi że należy zidentyfikować informacje, aktywa związane z informacjami i środkami przetwarzania informacji oraz sporządzić i utrzymywać ewidencję tych aktywów; oraz klasyfikować z uwzględnieniem ww. wymagań.

(akta kontroli str. 24-31)

I Z-ca Burmistrza wyjaśnił, że „W PBI nie przypisano zbiorom danych wag, nie dokonano klasyfikacji z uwzględnieniem wymagań prawnych wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikacje ponieważ uznano, że wszystkie wymienione w PBI grupy informacji wraz z ich wyszczególnieniem, podlegają takiej samej ochronie w celu zapewnienia ich poufności, dostępności i integralności."

(akta kontroli str. 943-949)

W ocenie NIK, nieprzypisanie odpowiedniego poziomu ochrony, braku wag dla grup informacji podlegających zabezpieczeniu, oraz nie sklasyfikowanie ich według ww. wymagań jest działaniem nierzetelnym, gdyż zidentyfikowanie kluczowych zbiorów danych/grup informacji oraz przypisanie im wag umożliwia po sytuacji kryzysowej w pierwszej kolejności przywrócenie informacji najbardziej istotnych. Ważność informacji przetwarzanych w Urzędzie powinna być określona wagą. Waga powinna być określona na podstawie zespołu czynników wypływających na jej wartość. W celu jej wyznaczenia konieczne jest precyzyjne określenie tych czynników. Do zespołu czynników wagi m.in. zalicza się: zakres danych, istotność informacji dla działalności Urzędu, stopień złożoności procesu przetwarzania danych, liczbę uczestników, która przetwarza dane. Nie określenie poziomu ochrony dla grup informacji, brak wag może przyczynić się do utraty ważnych informacji.

2. Plan Ochrony i Zapewnienia Ciągłości Działania Urzędu (wprowadzony Zarządzeniem nr 120.32.2022 z dnia 5 kwietnia 2022 r.) nie był kompletny, gdyż

nie zawierał: procedur: typologii sieci, systemowych serwerów wirtualnych oraz urządzeń brzegowych, jak i procedury czasu przywrócenia ciągłości działania, co było nierzetelne.

(akta kontroli str. 124-151)

Z-ca Burmistrza wyjaśnił, że: *W Planie Ochrony i Zapewnienia Ciągłości Działania nie opracowano procedur: topologii sieci, systemowych serwerów wirtualnych, klastrów i macierzy dyskowych oraz urządzeń brzegowych ponieważ uznano, że nie jest konieczny tak szczegółowy podział. Dlatego w rozdziale VII, pkt 9 opracowanego Planu Ochrony i Zapewnienia Ciągłości Działania Urzędu Miejskiego w Czechowicach-Dziedzicach opisano rekomendowane działania w przypadku awarii urządzeń teleinformatycznych bez ich szczegółowego podziału.*

(akta kontroli str. 943-949)

Zdaniem NIK, brak ww. procedur może znacznie utrudnić przywracanie do funkcjonowania infrastruktury informatycznej w szczególności niezbędnych i istotnych dla działalności Urzędu systemów informatycznych po zdarzeniach losowych (takich jak pandemia, awaria, pożar, czy zalania). Procedury umożliwiają szybkie, skuteczne i precyzyjne przywrócenie ciągłości działania systemów informatycznych w jednostce, a strategia odtworzenia działań w zakresie ww. procedur, powinna być określona w utworzonych planach ciągłości/odtworzenia działania. Ponadto brak procedur naraża jednostkę na chaotyczne działania, które są obarczone prawdopodobieństwem błędów oraz niepowodzeniem, natomiast procedury minimalizują to ryzyko, ponieważ określają usystematyzowany, ściśle określony i sprawdzony sposób postępowania.

3. W Urzędzie nie określono akceptowalnego czasu przywrócenia ciągłości działania jego systemów informatycznych, co było działaniem nierzetelnym.

(akta kontroli str. 124-151, 946)

W wyjaśnieniach I Z-ca Burmistrza podał, że nie została opracowana procedura czasu przywrócenia ciągłości działania ponieważ uznano, że nie jest ona konieczna.

(akta kontroli str. 946)

Zdaniem NIK, nieokreślenie akceptowalnego czasu przywrócenia ciągłości działania w zakresie systemów informatycznych skutkuje niedostateczną wiedzą o czasie niezbędnym do ponownego uruchomienia poszczególnych systemów informatycznych istotnych do funkcjonowania Urzędu. Właściwe zarządzanie ciągłością działania jest kluczowe, gdyż umożliwia ono odtworzenie działalności po katastrofie lub innym incydencie.

4. W Urzędzie Plan ochrony i zapewnienia ciągłości działania z dnia 5 kwietnia 2022 r. nie polegał testowaniu i treningowi, co było nierzetelne. Jak wskazuje Norma ISO 22301 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.

(akta kontroli str. 124-151)

Z-ca Burmistrza podał, że *Plany zapewnienia ciągłości działania i plany odtworzeniowe nie podlegały w okresie kontroli testowaniu i treningowi z uwagi na brak środowiska teleinformatycznego na którym możliwe byłoby przeprowadzenie testów i treningów. W ramach projektu Cyberbezpieczny samorząd zostanie zakupiony serwer do testowania kopii zapasowych* (…).

(akta kontroli str. 796-803)

Zdaniem NIK, w przypadku ww. Planu istotne jest cykliczne jego testowanie w celu zidentyfikowania słabych punktów tego planu w trakcie ćwiczeń, aby w sytuacji wystąpienia incydentu ciągłości działania zadział on prawidłowo.

OCENA CZĄSTKOWA

W Urzędzie opracowano i wdrożono SZBI, jak i Polityki Ochrony Danych Osobowych dostosowano do wymogów RODO. W PBI i jej aktualizacji zidentyfikowano zbiory danych podlegające zabezpieczeniu, jednakże nie przypisano im odpowiedniego poziomu ochrony oraz nie określono do nich wag. Plan ochrony i zapewnienia ciągłości działania Urzędu nie był kompletny, nie podlegał on również w okresie objętym kontrolą testowaniu i treningowi. W Urzędzie wyznaczono Zespół ds. bezpieczeństwa informacji. W okresie kontrolowanym Urząd dokonał przeglądów: PBI, Instrukcji Zarządzania Systemem Informatycznym, Polityki cyberbezpieczeństwa, Planu ochrony i zapewnienia ciągłości. Urząd zaktualizował: PBI, Politykę Ochrony Danych Osobowych, Instrukcję Zarządzania Systemem Informatycznym, jak i wprowadził zmianę do Zarządzenia ustanawiającego SZBI. Urząd zgodnie z postanowieniami rozporządzenia KRI, utrzymał aktualność inwentaryzacji i oprogramowania.

OBSZAR

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

Opis stanu faktycznego

2.1. Urząd wdrożył Procedurę instalacji oprogramowania[34], która uniemożliwiała zainstalowanie nieautoryzowanego oprogramowania. Badanie[35] na przykładzie oprogramowania testowego wykazało, brak możliwości zainstalowania bez uprawnień Administratora Systemu Informatycznego dowolnego oprogramowania.
Ponadto w trakcie oględzin dziesięciu stanowisk komputerowych stwierdzono, ze były one zabezpieczone poprzez hasło o wysokiej złożoności, jak i ustalono, że dwa monitory znajdujące się w polu widzenia osób postronnych były zabezpieczone filtrem prywatyzującym (naklejonym w sposób trwały na monitor ekranowy), co uniemożliwiało wgląd do danych wyświetlanych na tych monitorach osobom postronnym. Powyższe działania były zgodne z § 19 ust. 2 pkt 4 rozporządzenia KRI.

(akta kontroli str. 448-480)

Zgodnie z §14 (Zasady użytkowania sprzętu przenośnego) obowiązującej Instrukcji Zarządzania Systemem Informatycznym, wynoszenie sprzętu przenośnego zawierającego dane osobowe poza obszar Urzędu w uzasadnionych przypadkach, było możliwe po uzyskaniu pisemnej zgody Burmistrza.

(akta kontroli str. 113-123)

Burmistrz w kwestii przetwarzania informacji na urządzeniach mobilnych podał, że: *Na wykorzystywanych w Urzędzie (…) tabletach i smartfonach nie są przetwarzane informacje służbowe. Sprzęt ten nie łączy się z systemami Urzędu, nie są wysyłane/odbierane dane Urzędu – nie ma zainstalowanej służbowej skrzynki pocztowej (email). W związku z powyższym nie są objęte monitorowaniem i nadzorem*

[34] Obowiązująca zawarta w Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania informacji w Urzędzie wprowadzonej Zarządzeniem nr 120.68.2023 z dnia 13 lipca 2023 r., poprzednia ujęta w poprzedniej Instrukcji Zarządzania Systemem Informatycznym wprowadzonym Zarządzeniem nr 120.13.2021 z 26 lutego 2021 r.

[35] Przeprowadzone na wybranych losowo dziesięciu komputerach służbowych wykazało (pięciu stacjonarnych i pięciu laptopach), że urządzenia te były odpowiednio zabezpieczone przed zainstalowaniem na nich nieautoryzowanego oprogramowania przez pracowników Urzędu.

w kontekście przetwarzania informacji. Burmistrz w wyjaśnieniach tych podał również, że dane zgromadzone na dyskach urzędowych komputerów przenośnych są szyfrowane.

(akta kontroli str. 378-379)

2.2. Analiza uprawnień do systemów informatycznych 15 pracowników merytorycznych Urzędu (w tym siedmiu na stanowiskach kierowniczych) wykazała, że uczestniczyli oni w procesie przetwarzania informacji w stopniu adekwatnym do realizowanych przez nich zadań, oraz, że mieli dostęp do oprogramowania zgodnie z prowadzonym w Urzędzie *Rejestrem przydzielonych uprawnień do zasobów* prowadzonym przez Wydział Informatyki[36], co było zgodne z § 19 ust. 2 pkt 4 rozporządzenia KRI.

(akta kontroli str. 527- 616)

2.3. W wyniku badania którym objęto 15 użytkowników (z 21 osób, które w okresie objętym kontrolą zakończyły pracę w Urzędzie), ustalono, że 14 pracowników miało cofnięte wszystkie zasoby przypisane do niego zgodnie z *Rejestrem przydzielonych uprawnień do zasobów*, a dla jednego, który miał przydzielone siedem zasobów, z czego jeden zasób, tj. konto email nie zostało usunięte. Natomiast uprawnienia dla ww. pracowników, w trzech przypadkach nie zostały cofnięte niezwłocznie, z czego dwóch przypadkach wnioski o cofnięcie uprawnień do zasobu zostały wystawione w szóstym dniu po ustaniu stosunku pracy (co opisano w *Sekcji stwierdzone nieprawidłowości)*.

(akta kontroli str. 914-942)

W kwestii nieusuniętego konta email Burmistrz wyjaśnił, że: *Konto o adresie sekretarz@um.czechowice-dziedzice.pl nie zostało usunięte, ponieważ jest przypisane do funkcji a nie do konkretnej osoby. W opisywanym przypadku podczas zmiany na stanowisku Sekretarza Miasta nie usuwano ww. adresu ale zmieniono hasło dostępu (23 lipca 2023 r.) i nowe hasło przekazano nowej osobie na tym stanowisku, uniemożliwiając jednocześnie korzystanie z adresu poprzedniej osobie.*

(akta kontroli str. 951-955)

2.4. W wyniku oględzin trzech systemów informatycznych[37] zarządzanych przez Urząd w zakresie 15 pracowników[38], stwierdzono, że zostały spełnione wymagania Polityki haseł, określonej w obowiązującej Instrukcji Zarządzania Systemem Informatycznym, służącym do przetwarzania informacji w Urzędzie. W zakresie objętych badaniem pracowników ustalono, że loginy były przypisane tylko do jednego użytkownika, co było zgodne z § 20 ust. 2 pkt. 7 lit c KRI.

(akta kontroli str. 527-616)

2.5. Na podstawie oględzin pięciu stanowisk pracy w miejscach obsługi obywateli[39] (tj. trzech stanowisk stacjonarnych w Biurze ds. Profilaktyki i Przeciwdziałania Uzależnieniom oraz dwóch w Wydziale Spraw Obywatelskich) stwierdzono, że usytuowanie monitorów, zapewniało, że dane wyświetlane na monitorach nie były

[36] Dalej: WI.

[37] Tj. FINN, LEX, Geoportal.

[38] Nie każdy użytkownik korzystał z trzech wymienionych systemów informatycznych łącznie tj.14 pracowników korzystało z LEX-a, 15 pracowników z FINN-a, a 4 pracowników korzystało Geoportal -u.

[39] Tj. trzech stanowisk stacjonarnych w Biurze ds. Profilaktyki i Przeciwdziałania Uzależnieniom oraz dwóch w Wydziale Spraw Obywatelskich.

widoczne dla osób nieuprawnionych (zabudowane stanowiska), co było zgodne z § 20 ust. 2 pkt 7 rozporządzenia KRI odnośnie zapewnienia ochrony przetwarzanych informacji.

(akta kontroli str. 448-480)

2.6. W Urzędzie w załączniku nr 10 *Regulaminu wykonywania pracy zdalnej*, określono zasady instalacji, inwentaryzacji, konserwacji, aktualizacji oprogramowania i serwisu powierzonego sprzętu oraz procedury wykonywania pracy zdalnej za pośrednictwem szyfrowanego połączenia VPN[40] gwarantującego bezpieczną pracę, w tym wskazano, że połączenie do sieci wewnętrznej Urzędu może nastąpić tylko za pośrednictwem szyfrowanego połączenia VPN, oraz tylko z urządzenia powierzonego pracownikowi przez pracodawcę. Natomiast zgodnie z Instrukcjami zarządzania systemem informatycznym[41] dostęp do sprzętu komputerowego określały zasady nadawania identyfikatorów (odrębny dla każdego użytkownika) oraz Polityka haseł (w obowiązującej instrukcji dwunastoznakowych, w poprzedniej instrukcji ośmioznakowych), jak i zasady użytkowania sprzętu przenośnego, określającego konieczność zabezpieczenia wynoszonych danych przez ich zaszyfrowanie, co było zgodne z § 19 ust. 2 pkt. 8 KRI. Pracownicy zostali zapoznani z ww. zasadami.

(akta kontroli str. 68-123, 177-204)

W Urzędzie ASI w okresie od 1 marca 2024 r. do 30 kwietnia 2024 r. przeprowadził kontrolę m.in. w zakresie stosowania procedur i zasad określonych w Instrukcji Zarządzania Systemem Informatycznym z 13 lipca 2023 r. dotyczących również pracy zdalnej – w wyniku niniejszej kontroli nie stwierdzono żadnych przypadków naruszeń procedur i zasad wynikających z ww. zarządzenia.

(akta kontroli str. 289-291)

2.7. W ww. Instrukcjach opisanych w powyższym punkcie wynoszenie sprzętu poza Urząd możliwe było tylko po uzyskaniu zgody Burmistrza[42], z kolei w zakresie zabezpieczenia od strony technicznej Burmistrz w wyjaśnieniach podał, że: *każdy laptop ma zdefiniowanych użytkowników posiadających unikalny login i hasło, dostęp do systemu BIOS jest możliwy po wpisaniu hasła, zablokowana jest możliwość uruchomienia systemu z zewnętrznego nośnika oraz wszystkie dane są szyfrowane.* Ponadto podał, że dane zgromadzone na dyskach urzędowych komputerów przenośnych są szyfrowane z wykorzystaniem odpowiedniego mechanizmu. Powyższe działania były zgodne z § 19 ust. 2 pkt 9 i 11 rozporządzenia KRI.

(akta kontroli str. 68-123, 378-379)

2.8. W głównej serwerowni Urzędu zastosowano rozwiązania umożliwiające zabezpieczenie informacji przed nieuprawnionym ujawnieniem, modyfikacją, usunięciem lub zniszczeniem. Zapewniono ochronę fizyczną pomieszczenia serwerowni. W trakcie oględzin pomieszczenia serwerowni stwierdzono jednak, że znajdowały się tam materiały łatwopalne (co opisano w *Sekcji stwierdzone nieprawidłowości*).

(akta kontroli st. 699- 742)

2.9. Analiza czterech umów serwisowych[43] zawartych przez Gminę Czechowice-Dziedzice z podmiotami zewnętrznymi wykazała, że zamieszczono w nich

[40] Wirtualna prywatna sieć.

[41] Zarządzenia nr: 120.68.2023 z dnia 13 lipca 2023 r., oraz nr 120.13.2023 z dnia 26 lutego 2021 r.

[42] We wcześniejszej za

[43] W tym dwóch wraz z umowami powierzenia.

postanowienia gwarantujące odpowiedni poziom poufności i bezpieczeństwa informacji, co było zgodne z § 20 ust. 2 pkt 10 rozporządzenia KRI.

(akta kontroli str. 378-379, 380-414)

2.10. W Urzędzie została opracowana i wdrożona procedura opisująca przekazywanie do naprawy sprzętu komputerowego podmiotom zewnętrznym. W *Procedurze wykonywania przeglądów, konserwacji i napraw*, określono, że w przypadku przekazywania sprzętu IT do naprawy podmiotom zewnętrznym, przed jego przekazaniem należy pozbawić go nośników zawierających informacje lub jeśli jest to niemożliwe usunąć te informacje z nośnika uniemożliwiając ich odczytanie. W sytuacji gdy nie ma możliwości usunięcia z nośnika, dopuszcza się możliwość wykonania naprawy sprzętu komputerowego w obecności pracownika Urzędu[44]. Zapisy określone ww. procedurze spełniały wymogi zawarte w § 19 ust. 2 pkt. 7c i 9 rozporządzenia KRI stanowiącym o zapewnieniu środków uniemożliwiających nieautoryzowany dostęp oraz zabezpieczeniu informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnieniu, modyfikacji, usunięciu lub zniszczeniu.

(akta kontroli str. 68-112, 113-123,487)

2.11. W ramach Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania informacji w Urzędzie, przyjęto tożsamą *Procedurę zarządzania kopiami zapasowymi,* która regulowała m.in. tworzenie kopii zapasowych, określała jak ma być prowadzony Rejestr wykonanych kopii zapasowych i co ma zawierać, oraz miejsce i okres przechowywania kopii. Kopie zapasowe baz danych przechowywane były w zamkniętym sejfie, do którego dostęp miały upoważnione osoby.

(akta kontroli str. 68-123)

2.12. W jednostce kontrolowanej kopie zapasowe były tworzone na podstawie ww. *Instrukcji.* Analiza zapisów rejestru wykonanych kopii zapasowych wykazała, że w okresie od 1 stycznia 2023 r. do 8 sierpnia 2024 r. wykonano 49 kopii zapasowych, w tym w 13 przypadkach (26,5%) przekroczono maksymalny termin 14 dni na wykonanie kopii, co stanowiło naruszenie *pkt. 5 § 19 Procedury zarządzania kopiami zapasowymi obowiązującej ww. Instrukcji*[45] *(„Kopie zapasowe wykonuje się nie rzadziej niż co czternaście dni").* W powyższych 13 przypadkach kopie wykonano po upływie od 15 do 49 dni (co opisano w *Sekcji stwierdzone nieprawidłowości*).

W toku oględzin Główny specjalista w Wydziale Informatyki przeprowadził próbne odzyskanie bazy danych z kopii zapasowej zapisanej na dysku zewnętrznym zdeponowanym w sejfie, w pomieszczeniu innym niż miejsce wytworzenia danych. Odzyskany plik bazy danych otworzył się prawidłowo.

(akta kontroli str. 810-818)

2.13. W wyniku oględzin ustalono, że w jednostce kontrolowanej użytkowano 13 serwerów fizycznych. Główny specjalista w Wydziale Informatyki przedstawił stan zajętości dysków twardych 3 serwerów:

- serwer systemu 1, zajęte 72,8%,
- serwer systemu 2, zajęte 83,1%,
- serwer systemu 3, zajęte 55,9%.

(akta kontroli str. 807-809)

W kwestii monitorowania pojemności nośników pamięci I Z-ca Burmistrza wyjaśnił, że: „*Pojemność nośników pamięci systemów Urzędu podlega monitorowaniu. Monitorowanie to odbywa się podczas wgrywania poprawek*

[44] W poprzedniej Instrukcji w procedurze był zapis „w obecności osoby upoważnionej przez ADO".

[45] W poprzedniej Instrukcji również to samo uregulowanie w kwestii wykonywania kopii zapasowych nie rzadziej niż co 14 dni, lecz procedura określona była w § 17

i aktualizacji w systemach. Proces ten nie jest jednak sformalizowany i nie jest sporządzana dokumentacja z monitorowania."

(akta kontroli str. 943-949)

2.14. W Urzędzie nie zostały zidentyfikowane kluczowe elementy infrastruktury i usługi IT w celu zapewnienia ciągłości działania Urzędu oraz nie określono ich zabezpieczenia pod kątem wpływu czynników zewnętrznych (co opisano w *Sekcji stwierdzone nieprawidłowości*).

(akta kontroli str. 124-151)

Stwierdzone nieprawidłowości

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

1. Dwóm byłym pracownikom[46], nie cofnięto niezwłocznie dostępów do zasobów informatycznych Urzędu, co było niezgodne z § 19 ust. 2 pkt 5 rozporządzenia KRI stanowiącym, *że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań: bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.* I tak:

- wnioski o cofnięcie uprawnień pracownikowi Wydziału Świadczeń Społecznych do dwóch zasobów informatycznych[47] wystawione zostały przez Naczelnika Wydziału Świadczeń Społecznych pięć dni po dacie zakończenia zatrudnienia, tj. 6 maja 2024 r.,
- w zakresie programu Familia pracownik został wyrejestrowany siedem dni po ustaniu zatrudnienia (w statusie wyrejestrowane wyświetlało datę 8 maja 2024 r., a w statusie zablokowane brak daty),
- do komputera o nr inw. XI/35/571 na wniosku o cofnięcie do zasobu widniała data 6 maja 2024 r., tj. pięć dni po ustaniu zatrudnienia,

(akta kontroli str. 850-852, 855-856, 914-915, 941-942)

- osobie pełniącej funkcję Sekretarza cofnięto dostęp do iPKO Biznes[48] 4 sierpnia 2023 r., tj. sześć dni po ustaniu zatrudnienia, na wniosku o cofnięcie uprawnień w zakresie cofnięto dostęp widnieje ta sama data, wniosek został wystawiony w ostatnim dniu pracy, tj. 28 lipca 2023 r.

(akta kontroli str. 860-867, 914- 915)

Burmistrz wyjaśnił, że: *Wyżej wymienione wnioski zostały złożone i cofnięte po terminie z uwagi na niedopatrzenie czasowe ze strony osób składających wniosek. W przypadku wniosków dot. (…)* pracownika Wydziału Świadczeń Społecznych[49] *nie zostały one złożone w terminie zwolnienia (30.04.2024 r.) ale zostały złożone w pierwszym dniu obecności naczelnika Wydziału świadczeń Społecznych tj. 06.05.2024 r.* (…) *W przypadku aplikacji IPKO-Biznes cofnięcie nastąpiło w 5 dniu roboczym po wymaganym terminie. Planowane jest przypomnienie zasad zawartych w Instrukcji zarządzania systemem informatycznym, w tym w szczególności dot. cofania uprawnień do zasobu.*

(akta kontroli str. 951-955)

[46] Z 15 byłych pracowników objętych badaniem.

[47] Familia oraz komputer o nr inw. XI/35/571.

[48] iPKO biznes to serwis bankowości internetowej dla klientów firmowych i korporacyjnych PKO Banku Polskiego z dostępem przez aplikację mobilną.

[49] Przypis kontrolera NIK.

2. W trakcie oględzin pomieszczenia podlegającego szczególnej ochronie, tj. serwerowni stwierdzono, że znajdowały się tam materiały łatwopalne, co było niezgodne z § 19 ust. 2 pkt 9 rozporządzenia KRI.

(akta kontroli st. 699- 742)

I Z-ca Burmistrza w wyjaśnieniach podał, że *Sytuacja taka miała charakter krótkotrwały. W pomieszczeniu serwerowni zdeponowano świeżo dostarczony sprzęt, który jest instalowany na docelowych stanowiskach*.

(akta kontroli str. 796-803)

Zdaniem NIK, w ramach zapewnienia bezpieczeństwa, w tym ochrony przeciwpożarowej, w serwerowni nie powinny (nawet krótkotrwale) znajdować się materiały łatwopalne, gdyż zwiększa to ryzyko pożaru co może prowadzić do: utraty danych, przerwania działania ważnych operacji, oraz znacznych strat finansowych.

3. Na podstawie rejestru prowadzonego przez WI, ustalono, że w okresie od 1 stycznia 2023 r. do 8 sierpnia 2024 r. w 13 z 49 wykonanych kopii zapasowych (tj. 26,5%) przekroczono maksymalny termin 14 dni na ich wykonanie, co stanowiło naruszenie *pkt. 5 § 19 Procedury zarządzania kopiami zapasowymi ujętej w obowiązującej ww. Instrukcji*[50] *(„Kopie zapasowe wykonuje się nie rzadziej niż co czternaście dni").* W powyższych 13 przypadkach kopie wykonano po upływie od 15 do 49 dni.

(akta kontroli str. 810-818)

Burmistrz wyjaśnił, że „z wyjaśnień otrzymanych od pracownika odpowiedzialnego za wykonywanie kopii zapasowych wynika, że kopie zapasowe były wykonywane w terminie, natomiast fakt wykonania kopii nie został odnotowany w rejestrze, co przyczyniło się do pojawienia przekroczenia terminu. Niestety z uwagi na fakt cyklicznego nadpisywania starych kopii nowymi kopiami nie ma możliwości udokumentowania tego faktu. Przypomniano pracownikowi o konieczności przestrzegania procedur w zakresie nie tylko sporządzania kopii ale także o właściwym dokumentowaniu tego faktu."

(akta kontroli str. 950)

4. W Urzędzie, w ramach zapewnienia ciągłości działania, nie zidentyfikowano kluczowych elementów infrastruktury i usług IT oraz zabezpieczenia ich pod kątem wpływu czynników zewnętrznych, co było nierzetelne.

(akta kontroli str. 124-151)

I Z-ca Burmistrza wyjaśnił, że: „*nie zostały zidentyfikowane kluczowe elementy infrastruktury i usługi IT, oraz ich zabezpieczenie pod kątem wpływu czynników zewnętrznych ponieważ uznano, że nie jest konieczny taki podział na etapie tworzenia dokumentów głównych SZBI.(…)".*

(akta kontroli str. 943-949)

NIK wskazuje, że zarządzanie ciągłością działania ma na celu zapewnienie, że infrastruktura i usługi IT będą mogły być odtworzone do wcześniej zdefiniowanych poziomów. Dlatego też - zdaniem NIK - istotne jest zidentyfikowanie kluczowych dla pracy Urzędu elementów infrastruktury informatycznej, jak i usług informatycznych. Bez zdefiniowania tych kwestii szybkie i skuteczne przywrócenie infrastruktury i usług IT w sytuacji wystąpienia zakłócenia ciągłości działania może być znacznie utrudnione.

[50] W poprzedniej Instrukcji również to samo uregulowanie w kwestii wykonywania kopii zapasowych nie rzadziej niż co 14 dni, lecz procedura określona była w§ 17

OCENA CZĄSTKOWA

W Urzędzie podejmowano działania w zakresie zapewnienia bezpieczeństwa informacji m.in. poprzez zabezpieczenie komputerów przed możliwością instalowania dowolnego oprogramowania przez użytkowników, ustawienie monitorów w sposób zapewniających ochronę dany na nich przetwarzanych, nadawanie uprawnień pracownikom adekwatnie do realizowanych przez nich zadań oraz stosowanie w umowach serwisowych zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

Stwierdzone w tym obszarze nieprawidłowości dotyczyły m.in. niezidentyfikowania kluczowych elementów infrastruktury i usług IT oraz ich zabezpieczenia pod kątem wpływu czynników zewnętrznych oraz składowania w pomieszczeniu podlegającemu szczególnej ochronie, tj. serwerowni, materiałów łatwopalnych.

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

3.1. W Urzędzie opracowano i wdrożono *Instrukcję zarządzania ryzykiem*, w której w § 9 określono, że naczelnicy, kierownicy i pracownicy zatrudnieni na samodzielnych stanowiskach zobowiązani byli dokumentować prowadzoną analizę ryzyka poprzez tworzenie rejestrów ryzyka. Rejestry te należało przekazywać do Biura Audytu i Kontroli w terminie do końca lutego każdego roku.

(akta kontroli str. 161-166)

Zgodnie z § 10 powyższej instrukcji, o sposobie postępowania w odniesieniu do zidentyfikowanego ryzyka (istotność ryzyka), którego poziom jest akceptowalny warunkowo, akceptowalny lub pomijany, decyzję podejmuje naczelnik, kierownik i samodzielne stanowisko pracy, natomiast którego poziom jest krytyczny, nieakceptowalny decyzję podejmuje wyłącznie Burmistrz.

W stosunku do każdego zidentyfikowanego w podległej komórce organizacyjnej Urzędu ryzyka naczelnik, kierownik i samodzielne stanowisko pracy zobowiązani byli planować i wdrażać odpowiednie mechanizmy kontrolne/działania minimalizujące.
Naczelnicy, kierownicy i samodzielne stanowiska pracy mieli obowiązek dokonywania okresowych przeglądów i monitorowania poziomu ryzyka w celu uzyskania informacji czy:

- ryzyko nadal występuje,
- pojawiło się nowe ryzyko,
- prawdopodobieństwo i wpływ ryzyka zmieniło się,
- stosowane mechanizmy kontrolne/minimalizujące są efektywne.

Burmistrz w wyjaśnieniach podał, że przeglądy, o którym mowa wyżej, wykonywane były corocznie – przy składaniu nowego rejestru ryzyka.

W okresie objętym kontrolą audytor wewnętrzny przygotowała, na podstawie jednostkowych rejestrów ryzyka; przekazanych przez naczelników/kierowników i samodzielne stanowiska pracy, Zbiorczą informację o zidentyfikowanych ryzykach w obszarze bezpieczeństwa informacji na 2023 r. oraz roboczą informację na rok 2024 r. (obie opisane w obszarze pierwszym pkt 1.4.).

Burmistrz w wyjaśnieniach podał, że: *20 czerwca 2023 r. na posiedzeniu Zespołu ds. bezpieczeństwa informacji audytor wewnętrzny zaprezentował wyniki analizy ryzyka w bezpieczeństwie informacji; na ich podstawie Zespół sformułował rekomendacje do przedstawienia Burmistrzowi. Rekomendacje zostały przyjęte.* (…) *Pismem z dnia 18 lipca 2023 r. właściwe komórki zostały poinformowane o konieczności realizacji rekomendacji.* W uzupełnieniu wyjaśnień Burmistrz m.in. podał, że z rekomendacji

sformułowanych na 2023 r. zrealizowano: szkolenie dla członków GKRPA[51]; zakupiono UPS; w IV kwartale 2023 r. dokonano zakupu nowego serwera. Natomiast w zakresie wzmocnienia kadrowo WI podał, że: z uwagi na bardzo ograniczone możliwości lokalowe, nie tylko Wydziału Informatyki ale i całego Urzędu Miejskiego ewentualna decyzja o realizacji tej rekomendacji została odłożona w czasie.

(akta kontroli str. 661-669, 989)

3.2. Urząd zgodnie z art. 22 ustawy o ksc określił zarządzanie incydentem w § 7 *Polityki Cyberbezpieczeństwa* (z dnia 10 listopada 2021 r.) pn. *Zasady postępowania z incydentami,* w których określono, że *każda osoba, która zidentyfikowała zdarzenie cyberbezpieczeństwa lub wystąpienie słabości systemu zgłasza to osobie odpowiedzialnej za utrzymywanie kontaktów z podmiotami ksc. (…)Osoba odpowiedzialna za kontakt z podmiotami ksc po ocenie, że zgłoszenie jest incydentem ma m.in. wskazać osobę odpowiedzialną za podjęcie natychmiastowych działań, uruchomić działania w celu natychmiastowego zatrzymania dokumentu, dokonać analizy wspólnie z osobami wskazanymi przez Burmistrza (…), wykorzystać ten incydent jako podstawę weryfikacji oraz doskonalenia systemu bezpieczeństwa.*

(akta kontroli str. 167-176)

Stosownie do postanowień określonych w art. 33 RODO, w Urzędzie w *Procedurze postępowania w przypadku wystąpienia naruszenia ochrony danych osobowych*[52] określono sposób postępowania w przypadku naruszenia ochrony danych osobowych, oraz w *Procedurze monitorowania zagrożeń i zdarzeń*[53], w której określono, że każda osoba w przypadku podejrzenia wystąpienia zagrożenia danych osobowych lub wystąpienia zdarzenia bezpieczeństwa danych osobowych, zobowiązana jest do poinformowania o tym fakcie bezpośredniego przełożonego, który następnie wystąpienie zagrożenie/zdarzenia bezpieczeństwa danych osobowych zgłasza odpowiednio: Naczelnikowi Wydziału Organizacyjnego i Kadr (w zakresie bezpieczeństwa fizycznego i środowiskowego), Naczelnikowi WI (w zakresie bezpieczeństwa informatycznego), oraz IOD (w pozostałych obszarach)

(akta kontroli str. 32-67, 68-112)

Zgodnie z § 20 ust. 2 pkt 13 rozporządzenia KRI, zgłaszanie podejrzenia wystąpienia zagrożenia bezpieczeństwa/zdarzenia bezpieczeństw: zostało uregulowane w rozdziale VII (Rekomendowane działania podejmowane w przypadku wystąpienia zagrożeń i zakłóceń) Planu Ochrony i Zapewnienia Ciągłości Działania, w którym określono, że każda osoba w przypadku podejrzenia wystąpienia zagrożenia bezpieczeństwa zobowiązana jest do poinformowania o tym fakcie bezpośredniego przełożonego, który następnie wystąpienie zagrożenia zgłasza odpowiednio:

- w zakresie bezpieczeństwa fizycznego i środowiskowego Naczelnikowi Wydziału Organizacyjnego i Kadr;
- w zakresie bezpieczeństwa teleinformatycznego Naczelnikowi WI;
- w zakresie cyberbezpieczeństwa lub słabości systemu osobie odpowiedzialnej za utrzymanie kontaktu z podmiotami ksc;
- w obszarach ochrony danych osobowych nie wymienionych powyżej – IOD;
- w obszarach dotyczących ochrony informacji niejawnych – Pełnomocnikowi ds. Ochrony Informacji Niejawnych.

[51] Gminnej Komisji Rozwiązywania Problemów Alkoholowych.

[52] Procedura określona w obowiązującej Polityce Ochrony Danych Osobowych w § 19, w poprzedniej w § 17.

[53] Procedura określona w obowiązującej Polityce Ochrony Danych Osobowych w § 18, w poprzedniej w § 16.

Ww. rozdziale uregulowane były rekomendowane działania np. w przypadku pożaru pomieszczeń; zakłóceń lub braku zasilania elektrycznego oraz awarii urządzeń teleinformatycznych.

(akta kontroli str. 124-150)

Zarządzanie incydentem w Urzędzie zostało ujęte w trzech ww. dokumentach. W audycie Bezpieczeństwa informacji – Incydenty, Audytor wewnętrzny dokonała Porównania stanu oczekiwanego wg normy PN-EN ISO/IEC 27002:2023-01 do stanu faktycznego, w którym wykazała:

- w zakresie *Odpowiedzialność i procedury* (w kolumnie stan oczekiwany), podała, że ustalenie procedur zapewniających szybką, skuteczną i zorganizowaną reakcję na incydenty, może stanowić punkt odniesienia do stworzenia w Urzędzie jednej spójnej, a zarazem prostej do stosowania procedury dotyczącej incydentów bezpieczeństwa informacji; w kolumnie porównania pn. *stan faktyczny* podała, że ujęte w audycie zarządzenia, częściowo dotykają tematu incydentu, zgłaszania i reagowania,
- w zakresie *Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji* (w kolumnie stan oczekiwany) wskazała, że zapewnienie kanału do zgłoszeń, zapewniających możliwe jak najszybsze zgłoszenie incydentu – w kolumnie *stanu faktycznego* wskazała, że w Urzędzie nie obowiązuje jeden kanał do zgłaszania incydentów, z reguły przywoływani są Naczelnicy kluczowych Wydziałów czyli OR i WI oraz IOD, w zakresie stan oczekiwany podała, że zapewnienie kanału do zgłoszeń, zapewniających jak najszybsze zgłoszenie incydentu.

(akta kontroli str. 764-766)

Osoby podejmujące decyzję w sprawie zdarzeń związanych z bezpieczeństwem informacji, jak i naczelnicy poszczególnych przyjmujący zgłoszenia o podejrzeniu wystąpienia zagrożenia bezpieczeństwa (wymienieni w Planie ochrony i ciągłości działania) nie zostali przeszkoleni w zakresie identyfikacji incydentów.
W związku z powyższym I Z-ca Burmistrza w wyjaśnieniach podał, że: *Przyczyną braku przeszkolenia naczelników poszczególnych wydziałów w zakresie identyfikacji incydentów, w tym szczególnie naczelników wymienionych w Planie ochrony i ciągłości działania, jest fakt, że zaznajomienie się z dokumentacją w ww. zakresie uznano za wystarczające. Naczelnicy uczestniczyli w szkoleniu ogólnym z PBI.*

(akta kontroli str. 498-501, 943-949)

3.3. W okresie od 1 stycznia 2023 r. do 20 czerwca 2024 r. łącznie w czterech wewnętrznych szkoleniach uczestniczyło 493 pracowników (zatrudnionych pracowników merytorycznych z dostępem do systemów informatycznych 172 osoby na dzień 20 czerwca 2024 r.), z czego:
1. „Ochrona danych osobowych w Urzędzie - Anonimizacja danych" (aplikacja FINN) w roku 2023 r. uczestniczyło online 156 pracowników;
2. „Ochrona danych osobowych w Urzędzie - Szkolenie PODO - zmiany 2023" (aplikacja FINN) w 2023 r. uczestniczyło online 155 pracowników;
3. „Ochrona danych osobowych w Urzędzie - Retencja danych osobowych w BIP" (aplikacja FINN), szkolenie w trakcie kontroli na ww. dzień online przeszkolono 33 pracowników;
4. Omówienie struktury dokumentacji stanowiącej SZBI z elementami zarządzania ryzykiem", szkolenie stacjonarne w dniach 22-23 listopada 2023 r., przeszkolono 149 pracowników.

(akta kontroli str. 499-506)

Urząd skierował dwóch pracowników na studia podyplomowe, w tym audytora wewnętrznego na „Audyt Bezpieczeństwa Systemów Informatycznych”[54] oraz głównego specjalistę w Wydziale Informatyki na „Zarządzanie Cyberbezpieczeństwem”[55] (rozpoczęcie od października 2024 r.).

(akta kontroli str. 498)

3.4. Zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI (w którym mowa o zapewnieniu okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok), w Urzędzie został przeprowadzony w okresie od 9 października 2023 r. do 29 grudnia 2023 r. audyt wewnętrzny w temacie Bezpieczeństwo informacji – Incydenty, w wyniku którego wydano następujące rekomendacje:

- Wprowadzić w Urzędzie jeden prosty schemat zgłaszania powiadomień o zdarzeniach mających znamiona incydentu w bezpieczeństwie informacji – dla wszystkich obszarów, tj. bezpieczeństwo fizyczne, ochrona danych osobowych, cyberbezpieczeństwo i systemy informatyczne – Politykę incydentu jako dokument z II poziomu dokumentacji stanowiącej SZBI.
- Dokonać aktualizacji – we wskazanych w audycie uwagach audytora – Polityki Ochrony Danych.
- Dokonać aktualizacji – we wskazanych w audycie uwagach audytora – Polityki Cyberbezpieczeństwa.
- W związku z rosnącą rolą zagrożeń związanych z cyberbezpieczeństwem oraz zadań dla pełnomocnika ds. cyberbezpieczeństwa, rozważyć wyłączenie funkcji pełnomocnika ze struktur Wydziału Zarządzania Kryzysowego i (przykładowo), poszerzenie Wydziału Informatyki o osobę pełniącą ww. funkcję.
- Rozszerzyć zakres zadań zespołu ds. bezpieczeństwa informacji o cykliczną analizę zdarzeń z zakresu incydentów w bezpieczeństwie informacji i obowiązkiem raportowania Burmistrzowi (analogicznie usunąć zapis o czynności o podobnym charakterze z Polityki Ochrony Danych).

W audycie wskazano, że sposób i harmonogram wykonania rekomendacji oraz wskazania osób odpowiedzialnych za wykonanie rekomendacji, ma dokonać się na posiedzeniu Zespołu ds. bezpieczeństwa informacji.

(akta kontroli str. 744-768)

W kwestii wdrożenia rekomendacji, I Z-ca Burmistrza podał, że *Rekomendacje z audytu zostaną omówione na najbliższym posiedzeniu Zespołu ds. bezpieczeństwa informacji i tam opracowany zostanie harmonogram oraz wskazane zostaną osoby odpowiedzialne za wykonanie każdej z rekomendacji.*

(akta kontroli str. 796-803)

Stwierdzone nieprawidłowości

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

OCENA CZĄSTKOWA

W Urzędzie w okresie objętym kontrolą, podjęto działania w celu zapobiegania incydentom bezpieczeństwa informacji, tj. przeprowadzono okresowe analizy ryzyka utraty integralności, poufności lub dostępności informacji, zorganizowano szkolenia pracowników. W jednostce przeprowadzono okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji.

[54] Zakończenie czerwiec 2024 r.

[55] Rozpoczęcie od października 2024 r.

IV. Uwaga i wnioski

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

Uwaga

zwraca uwagę na konieczność niezwłocznego odbierania byłym pracownikom Urzędu uprawnień do systemów informatycznych,

oraz wnosi o:

Wnioski

1. Sklasyfikowanie zidentyfikowanych grup informacji z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację; przypisanie informacjom odpowiedniego poziomu ochrony oraz wag.
2. Uzupełnienie polityk Planu zapewnienia ciągłości działania o niezbędne procedury.
3. Określenie akceptowalnego czasu przywrócenia ciągłości działania czasu niezbędnego do otworzenia procesów po awarii.
4. Zapewnienie poddawania testowaniu i treningowi Planu zapewnienia ciągłości działania.
5. Niezwłoczne usunięcie z serwerowni materiałów łatwopalnych.
6. Zapewnienie terminowego wykonywania kopii zapasowych i rzetelnego prowadzenia rejestrów w tym zakresie.
7. Zidentyfikowanie kluczowych elementów infrastruktury i usług IT oraz ich zabezpieczenia pod kątem wpływu czynników zewnętrznych.

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.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

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

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

Katowice, dnia 19 września 2024 r.

Kontrolerzy
Magdalena Śleziak
specjalista kontroli państwowej

……..…….

Najwyższa Izba Kontroli
Delegatura w Katowicach