NAJWYŻSZA IZBA KONTROLI
Delegatura w Katowicach

LKA.410.14.4.2024

Pan
Daniel Beger
Prezydent
Miasta Świętochłowice
ul. Katowicka 54
41-600 Świętochłowice

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 Świętochłowicach[1] ul. Katowicka 54, 41-600 Świętochłowice.
Kierownik jednostki kontrolowanej	Daniel Beger, Prezydent Miasta Świętochłowice[2] od 22 listopada 2018 r. do dnia zakończenia czynności kontrolnych w jednostce.
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 w 2024 r.[3] (także okresy wcześniejsze w zakresie uczestnictwa w programie Cyfrowa Gmina/Cyfrowy Powiat).
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[4]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Katowicach
Kontrolerzy	1. Kinga Kołodziejczyk starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LKA/120/2024 z 22 maja 2024 r. 2. Szymon Gruca główny specjalista kontroli państwowej, upoważnienie do kontroli nr LKA/121/2024 z 22 maja 2024 r.

(akta kontroli str.1-4)

[1] Dalej: „Urząd".

[2] Dalej: „Prezydent Miasta".

[3] tj. do dnia 19 lipca 2024 r.

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

II. Ocena ogólna[5] kontrolowanej działalności

OCENA OGÓLNA

W okresie objętym kontrolą Urząd podejmował działania mające na celu zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych.

Podejmowane działania polegały m.in. na:

- opracowaniu Polityki Bezpieczeństwa Urzędu Miasta dotyczącej bezpieczeństwa danych osobowych, a także zawierającej elementy związane z zasobami informatycznymi Urzędu i ich zabezpieczeniem;
- przeprowadzaniu analiz ryzyka w zakresie zapewnienia ciągłości działania;
- przeprowadzaniu corocznych audytów z zakresu bezpieczeństwa informacji;
- opracowaniu procedur i instrukcji stanowiących dokumenty wykonawcze do Polityki bezpieczeństwa;
- opracowaniu regulaminu pracy wykonywanej w formie zdalnej.

W Urzędzie nie wdrożono jednak Systemu Zarządzania Bezpieczeństwem Informacji[6], a nieprawidłowe działanie jednostki kontrolowanej dotyczyło nieprzypisania zbiorom danych kategorii ochrony, nieopracowania polityki ciągłości działania oraz planów ciągłości działania i planów odtworzeniowych. Z uwagi na nieopracowanie ww. planów nie wyznaczono również osób odpowiedzialnych za ciągłość działania systemów informatycznych Urzędu, a tym samym żadnemu z pracowników nie przypisano obowiązków z powyższego zakresu.

Na Inspektora Ochrony Danych Osobowych[7] prawidłowo powołano osobę posiadającą niezbędne kwalifikacje do wykonywania tejże funkcji. IOD zagwarantowano niezależność, przy czym zarówno analiza ryzyka, jak i audyt bezpieczeństwa były przeprowadzane corocznie przez tę samą osobę – IOD, co naruszało zasadę niezależności i obiektywizmu audytu. Terminowo zostały wyznaczone i zgłoszone osoby odpowiedzialne za utrzymanie kontaktów z podmiotami Krajowego Systemu Cyberbezpieczeństwa.

Urząd posiadał pełną informację o posiadanych zasobach informatycznych oraz o zbiorach przetwarzanych danych podlegających zabezpieczeniu i ochronie.

Pracownicy uzyskiwali adekwatne do realizowanych zadań dostępy do rejestrów, baz danych, systemów dziedzinowych, a konta pracowników, którzy zakończyli pracę były zamykane w momencie powzięcia przez pracowników Wydziału Informatyki informacji o odejściu pracownika. Pracownicy Urzędu zostali przeszkoleni z zakresu cyberbezpieczeństwa i zapoznani z zasadami zapewnienia bezpieczeństwa informacji. W Urzędzie zapewniono ciągłość działania systemów informatycznych pomimo nieopracowania polityk i planów zachowania ciągłości działania oraz planów odtworzeniowych.

Służbowy sprzęt IT został zabezpieczony przed dostępem osób nieuprawnionych oraz zainstalowaniem nieautoryzowanego oprogramowania. Jedynie na służbowych telefonach komórkowych użytkownicy mogli instalować oprogramowanie z zewnątrz. Kopie zapasowe były tworzone i testowane na bieżąco, a sposób ich utworzenia umożliwiał odzyskanie zapisanych danych. Stwierdzono natomiast niewłaściwe zabezpieczenie serwerowni.

---

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

[6] Dalej:"SZBI".

[7] Dalej: „IOD" lub „IODO".

Urząd korzystał ze środków Programów rządowych „Cyfrowa Gmina" i „Cyberbezpieczny Samorząd", które pozwoliły na realizację zadań z zakresu zapewnienia bezpieczeństwa informacji i ciągłości działania.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[8] kontrolowanej działalności

OBSZAR

1.Organizacja bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych

Opis stanu faktycznego

1.1. W Urzędzie identyfikowano i aktualizowano zbiory danych w ramach funkcjonującej Polityki Bezpieczeństwa Informacji. Dane przetwarzane przez Urząd oraz sposób ich przetwarzania zostały opisane w załącznikach do Polityki Bezpieczeństwa Informacji:

- Załącznik nr 2 – Rejestr czynności przetwarzania;
- Załącznik nr 3 – Rejestr kategorii czynności przetwarzania;
- Załącznik nr 5 – Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
- Załącznik nr 6 – Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
- Załącznik nr 7 – Sposób przepływu danych pomiędzy poszczególnymi systemami.

Dane podlegające zabezpieczeniu znajdowały się w 42 zbiorach.
Sposób ochrony informacji został opisany w Polityce Bezpieczeństwa Informacji oraz oparty na przepisach prawa dotyczących dostępu do informacji ustawowo chronionych. Jednakże ww. zbiorom danych nie przypisano wag, ani kategorii ochrony, co zostało opisane w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 15-26,113-254)

1.2. W Urzędzie nie wdrożono SZBI, w rozumieniu § 19 ust. 1 rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności[9] minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów informatycznych[10], co zostało opisane w sekcji *Stwierdzone nieprawidłowości*.

Obowiązująca w Urzędzie Polityka Bezpieczeństwa Urzędu[11] dotyczyła bezpieczeństwa danych osobowych, zawierała jednak elementy dotyczące zasobów informatycznych Urzędu oraz ich zabezpieczenia. Prezydent w Zarządzeniu wprowadzającym Politykę bezpieczeństwa zobowiązał wszystkich pracowników do przestrzegania postanowień zawartych w ww. dokumencie oraz załącznikach

[8] 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.

[9] Dz.U. z 2024 r. poz. 773, do maja 2024 r. obowiązywały przepisy rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247). Dalej„ rozporządzenie KRI"

[10]. W okresie objętym kontrolą był to przepis § 20 ust. 1-3 rozporządzenia KRI z 12 kwietnia 2012 r

[11] Polityka Bezpieczeństwa Urzędu została wprowadzona Zarządzeniem Prezydenta Miasta Nr 430/2020 z dnia 15 czerwca 2020 r. Zmienione Zarządzeniem Prezydenta Miasta Nr 684/2020 z dnia 14 października 2020 r. Dalej: „Polityka bezpieczeństwa".

do niego. Nadzór nad przestrzeganiem postanowień Polityki bezpieczeństwa został powierzony Inspektorowi Ochrony Danych[12] oraz Naczelnikowi Wydziału Informatyki.

(akta kontroli str. 104-110,119,1206-1207)

1.3. W Urzędzie sporządzono dokumentację w zakresie ochrony danych osobowych uwzgledniającą wymogi 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)[13]. W Polityce bezpieczeństwa zostały opisane:

- prawa osób wynikające z RODO[14],
- zasady przetwarzania danych[15],
- miejsca/obszary/zbiory/rejestry przetwarzania danych osobowych,
- przetwarzanie danych osobowych,
- wydawanie upoważnień do przetwarzania danych osobowych.

Ponadto, dokumentacja w zakresie ochrony danych osobowych stanowiła załącznik do Polityki bezpieczeństwa[16].

Polityka bezpieczeństwa została wprowadzona Zarządzeniami Prezydenta, w których wszyscy pracownicy Urzędu zostali zobligowani do jej przestrzegania. W Zarządzeniach zostały również wskazane osoby odpowiedzialne za nadzór nad przestrzeganiem jej postanowień – co zostało opisane w punkcie drugim wystąpienia pokontrolnego.

(akta kontroli str. 104-110,260-288)

[12] Dalej: „IOD".

[13] Dalej: „RODO".

[14] Prawo: dostępu do danych, do poprawienia danych, do ograniczenia przetwarzania danych, do sprzeciwu, do bycia zapomnianym (do usunięcia danych), do przenoszenia danych.

[15] Zasada: zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu, minimalizacji danych, prawidłowości, ograniczenia przechowywania, integralności i poufności, rozliczalności.

[16] Załącznik nr 1 – Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, Załącznik nr 2 – Rejestr czynności przetwarzania, Załącznik nr 3 – Rejestr kategorii czynności przetwarzania, Załącznik nr 4 - Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, Załącznik nr 5 - Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, Załącznik nr 6 - Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, Załącznik nr 7 - Sposób przepływu danych pomiędzy poszczególnymi systemami, Załącznik nr 8 – Umowa powierzenia przetwarzania danych osobowych, Załączniki nr 10-12 – Zgoda na przetwarzanie danych osobowych, Załączniki nr 13-14 – Zgoda na upublicznienie wizerunku, Załączniki nr 20-22 oraz 24-28 klauzule informacyjne, Załącznik nr 23 – Klauzula poufności, Załącznik nr 29 i 29a – Upoważnienie do przetwarzania danych, Załącznik nr 30 – Rejestr osób upoważnionych do przetwarzania danych osobowych, Załącznik nr 31 - Wykaz kont osób i systemów przetwarzających dane osobowe, Załącznik nr 32 - Zgłoszenie naruszenia ochrony danych osobowych do organu nadzorczego, Załącznik nr 33 - Rejestr incydentów naruszenia ochrony danych, Załączniki nr 34 – 35 – Wykaz udostępnień danych osobowych, Załącznik nr 36 – Wniosek o udostępnienie danych osobowych, Załącznik nr 37 - Wykaz podmiotów, z którymi zawarto umowy powierzenia przetwarzania danych, Załącznik nr 38 - Określenie środków technicznych i organizacyjnych zalecanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, Załącznik nr 39 - Procedura postępowania w zakresie sporządzania Rejestru Czynności Przetwarzania Danych i Rejestru Kategorii Czynności Przetwarzania Danych, Załącznik nr 40 - Procedura postępowania w CV składanymi przez kandydatów do pracy, Załącznik nr 41 - Procedura postępowania w przypadku naruszenia ochrony danych osobowych, Załącznik nr 42 - Procedura postępowania w zakresie zawierania umów powierzenia przetwarzania danych, Załącznik nr 43 – Procedura retencji danych osobowych, Załącznik nr 44 - Określenie przebiegu procesu przygotowania, przechowywania i prowadzenia rejestru upoważnień do przetwarzania danych osobowych, Załącznik nr 45 – Polityka czystego biurka.

1.4.Analiza ryzyka była przeprowadzana w ramach kontroli zarządczej oraz raz do roku przez Inspektora Ochrony Danych Osobowych[17] w zakresie wybranych zbiorów, w tym obszarów IT w ramach funkcjonującej Polityki bezpieczeństwa.

(akta kontroli str. 15-26,80-103,809-840)

1.5.W Urzędzie nie ustanowiono polityki ciągłości działania, co zostało opisane w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 15-26,65-72,104-112)

1.6.W Urzędzie nie opracowano i nie wdrożono Planu zapewnienia ciągłości działania oraz planów odtworzeniowych, co zostało opisane w sekcji *Stwierdzone nieprawidłowości*.

W odniesieniu do czasu przywracania poszczególnych systemów oraz procesów do działania Prezydent wyjaśnił, że *Urząd przywraca działanie systemu doraźnie w ramach potrzeb. Nie prowadzi się dokumentacji w tym zakresie. W ramach Programu „Cyberbezpieczny Samorząd" planowane jest wprowadzenie aktualizacji dokumentacji dla zapewnienia zgodności z normą ISO 27001 wraz z planem ciągłości działania oraz obowiązkiem wykonywania testów odtworzenia kopii zapasowych.*

(akta kontroli str. 10-26)

1.7. Z uwagi na to, że w Urzędzie nie zostały przyjęte plany zapewnienia ciągłości działania ani plany odtworzeniowe nie mogły one podlegać testowaniu bądź treningowi.

Jednakże w Instrukcji Zarządzania Systemem Informatycznym[18] został opisany sposób testowania i odzyskiwania kopii zapasowych. Jak wyjaśnił Prezydent: obecnie implementacja ww. instrukcji polega na wykorzystaniu rozwiązań technicznych środowiska Veeam Backup&Replication.

System zachowania ciągłości działania opierał się na testowaniu skuteczności i poprawności wykonywanych kopii bezpieczeństwa poprzez okresowe sprawdzanie stanu najnowszych punktów przywracania w łańcuchu kopii zapasowych. Mechanizm uruchamiany był w ostatnią niedzielę miesiąca o określonej godzinie. Kolejny element stanowiło narzędzie pozwalające weryfikować odzyskiwanie kopii zapasowych danych przechowywanych w maszynach wirtualnych. Dzięki temu narzędziu można było uruchomić maszynę wirtualną bezpośrednio z kopii zapasowej w laboratorium wirtualnym[19]. Narzędzie było wykorzystywane doraźnie w ramach potrzeb, bez automatycznego harmonogramu.

(akta kontroli str. 15-26,65-72)

1.8.Polityka bezpieczeństwa od momentu wprowadzenia w 2020 r. do czasu rozpoczęcia kontroli w 2024 r. była aktualizowana sześć razy – trzy razy w 2020 r.[20], dwa razy w 2023 r.[21]. i raz w 2024 r.[22]. Zmiany te dotyczyły:

w 2020 r.

- aktualizacji Rejestru Czynności Przetwarzania, do którego dodano czynności przetwarzania zidentyfikowane w toku bieżących działań prowadzonych w zakresie ochrony danych osobowych;

[17] Dalej: „IODO" lub „IOD".

[18] Dział 11 pkt 5 i 6.

[19] Dedykowane środowisko izolowane od pozostałej infrastruktury.

[20] Zarządzeniami Prezydenta Miasta: Nr 566/2020 z dnia 11 sierpnia 2020 r., Nr 684/2020 i 685/2020 z dnia 14 października 2020 r.

[21] Zarządzeniami Prezydenta Miasta Nr 50/2023 z dnia 6 lutego 2023 r., Nr 199/2023 z dnia 19 kwietnia 2023 r.

[22] Zarządzeniem Prezydenta Miasta nr 110/2024 z dnia 11 marca 2024 r.

- wprowadzenia wzoru upoważnienia do przetwarzania danych osobowych w związku z wykonywaniem pracy przy przetwarzaniu danych osobowych dotyczących Zakładowego Funduszu Świadczeń Socjalnych;
- aktualizacji upoważnienia do przetwarzania danych osobowych, w którym wprowadzono odwołanie do Regulaminu Organizacyjnego Urzędu;
- wprowadzenia wzoru upoważnienia do przetwarzania danych osobowych zgromadzonych w Systemie Rejestrów Państwowych wraz z wnioskiem o nadanie/odebranie uprawnień do ich przetwarzania.

w 2023 r.

- wprowadzenia wzoru upoważnienia do przetwarzania danych osobowych w związku z prowadzeniem działań przez Gminną Komisję Rozwiązywania Problemów Alkoholowych wraz z klauzulą informacyjną;
- wprowadzenia Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

w 2024 r.

- wprowadzenia wzoru upoważnienia do przetwarzania danych osobowych dotyczących realizacji zadań przez komisje lekarskie orzekające o stopniu zdolności do służby wojskowej osób stawiających się do kwalifikacji, wraz z wzorem Rejestru osób upoważnionych do przetwarzania danych osobowych – System Rejestrów Państwowych.

(akta kontroli str.104-112,260-288)

1.9.W Urzędzie nie wyznaczono pracowników odpowiedzialnych za bezpieczeństwo informacji oraz zapewnienie ciągłości działania, co zostało opisane w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 668-669)

1.10.W okresie objętym kontrolą Urząd zawierał umowy zlecenia[23] z podmiotem zewnętrznym na wykonywanie usługi polegającej na pełnieniu funkcji IOD. Zleceniobiorca posiadał odpowiednie kwalifikacje zawodowe do pełnienia tej funkcji – został wpisany na listę biegłych sądowych z zakresu ochrony danych osobowych, uczestniczył w szkoleniach m.in. z zakresu ogólnego rozporządzenia RODO, przygotowania do kontroli przeprowadzanej przez Prezesa Urzędu Ochrony Danych Osobowych[24], ochrony danych osobowych w samorządzie terytorialnym po zmianach sektorowych, ochrony danych osobowych pracowników i kandydatów do pracy, efektywnego zarządzania ryzykiem, udostępniania danych osobowych w sektorze publicznym, RODO w ochronie zdrowia, audytu zgodności z RODO, rejestrowania czynności przetwarzania według RODO, ochrony danych osobowych sygnalistów, technicznych i organizacyjnych środków bezpieczeństwa danych osobowych. Zleceniobiorca ukończył również kurs Inspektora Ochrony Danych Osobowych według rozporządzenia RODO.

(akta kontroli str.289-312)

1.11. IOD wykonywał swoje obowiązki w sposób niezależny, a w jego działalności nie występował konflikt interesów, było to zgodne z art. 38 ust. 3 oraz art. 38 ust. 6 RODO. Zawarta umowa na usługi IOD nie rodziła żadnych skutków w zakresie uprawnień pracowniczych wynikających ze stosunku pracy, 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

[23] Umowa nr OR/75/2022 zawarta w dniu 28 grudnia 2022 r. Zgodnie z zawartą umową Zleceniobiorca wykonywał usługę w okresie od 1 stycznia do 31 grudnia 2023 r. Umowa nr CRU/942/2023 zawarta w dniu 29 grudnia 2023 r. Umowę zawarto na okres od 1 stycznia do 31 grudnia 2024 r.

[24] Dalej: „UODO".

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.289-300)

1.12.Dwaj pracownicy Wydziału Informatyki zostali wyznaczeni do utrzymywania kontaktów z podmiotami Krajowego Systemu Cyberbezpieczeństwa[25]. W zgłoszeniu osób kontaktowych do CSIRT NASK z dnia 3 marca 2021 r. zawarto wymagane dane: imię i nazwisko, numer telefonu oraz adres poczty elektronicznej. Zgłoszenia dokonano w terminie 14 dni od dnia wyznaczenia przez Prezydenta[26], co było zgodne z art. 22 ust. 1 pkt 5 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa[27].

Ww. osoby zostały zgłoszone do kontaktów w zakresie zadań publicznych zależnych od systemów informacyjnych realizowanych zarówno przez jednostki organizacyjne Urzędu, jak i przez jednostki podległe Prezydentowi Miasta lub przez Urząd nadzorowane.

(akta kontroli str. 313-318)

19 kwietnia 2023 r. Zarządzeniem Prezydenta Miasta w sprawie aktualizacji Polityki bezpieczeństwa[28] została wprowadzona Instrukcja zarządzania systemem teleinformatycznym służącym do przetwarzania danych osobowych w Urzędzie, która stanowiła załącznik nr 1 do Polityki bezpieczeństwa. W ww. dokumencie zostały opisane m.in.: zabezpieczenia infrastruktury informatycznej i telekomunikacyjnej, zabezpieczenia programów i baz przetwarzających dane osobowe, procedura dostępu podmiotów zewnętrznych, procedura korzystania z Internetu, procedura korzystania z poczty elektronicznej, procedura nadawania uprawnień do przetwarzania danych osobowych, metody i środki uwierzytelnienia, procedura rozpoczęcia, zawieszenia i zakończenia pracy, procedura tworzenia kopii zapasowych, sposób, miejsce i okres przechowywania oraz korzystania z elektronicznych nośników informacji i wydruków, procedura zabezpieczenia systemu informatycznego, w tym przed wirusami komputerowymi, zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych, procedura wykonywania przeglądów i konserwacji.

(akta kontroli str. 270-285)

1.13.W Urzędzie zostały sporządzone następujące procedury, instrukcje i polityki wewnętrzne stanowiące dokumenty wykonawcze wymagane przez Politykę bezpieczeństwa:

- Procedura tworzenia kopii zapasowych;
- Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;

[25] Dalej: „CSIRT NASK."

[26] Pełnomocnik Rządu do spraw Cyberbezpieczeństwa, pismem z dnia 17 lutego 2021 r. zwrócił się o dokonywanie zgłoszeń osób do kontaktów z CSIRT NASK w przypadku cyberataków. Na podstawie ww. pisma Prezydent, w dniu 3 marca 2021 r. zgłosił do kontaktów dwóch pracowników Wydziału Informatyki.

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

[28] Zarządzenie Nr 199/2023 z dnia 19 kwietnia 2023 r.

- Polityka plików Cookies;
- Procedura dotycząca sporządzania rejestru czynności przetwarzania;
- Procedura postepowania z CV składanymi przez kandydatów do pracy;
- Procedura postępowania w przypadku naruszenia ochrony danych osobowych;
- Procedura postępowania w zakresie zawierania umów powierzenia przetwarzania danych osobowych;
- Procedura retencji danych osobowych;
- Procedura udzielania upoważnienia do przetwarzania danych osobowych;
- Polityka czystego biurka.

(akta kontroli str.65-72,111,255-259, 270-285,1107-1121)

1.14.Posiadanie przez Urząd Informacji o zasobach informatycznych, ich rodzaju i konfiguracji zostało zweryfikowane na podstawie przeprowadzonych oględzin oprogramowania służącego do inwentaryzacji sprzętu informatycznego i danych z niego pozyskanych dla próby[29] złożonej z 10 komputerów stacjonarnych, dwóch laptopów, jednej drukarki, jednego serwera i jednego routera brzegowego.
Podczas oględzin stwierdzono, że:

w Urzędzie do inwentaryzacji zasobów IT stosowany był specjalistyczny program do kompleksowego zarządzania infrastrukturą IT, który umożliwiał:

a) Zarządzanie zasobami informatycznymi Urzędu, poprzez:
- inwentaryzację komputerów i sprzętu;
- zarządzanie oprogramowaniem;
- automatyzację zarządzania IT - zdalne skrypty;
- automatyczne powiadomienia i alerty.

b) Zapewnienie monitoringu i bezpieczeństwa, poprzez:
- analizę wykorzystania komputerów i programów;
- zarzadzanie nośnikami wymiennymi;
- monitorowanie wydruków i drukarek;
- blokowanie stron WWW i kontrolę Internetu;
- centralny syslog (konsola do przeglądania logów Windows z komputerów).

c) Pracę zdalną oraz usługi Helpdesku, poprzez:
- obsługę zgłoszeń serwisowych – helpdesk;
- zarządzanie incydentami zgłaszanymi przez użytkowników;
- zdalne zarządzanie i pomoc;
- zdalne przejęcie pulpitu użytkownika.

Inwentaryzacja i zarządzanie zasobami IT było prowadzone poprzez system *uplook Zasoby*, który umożliwiał zdalną, automatyczną inwentaryzację zasobów oraz natychmiastowe ich wyszukiwanie po zadanych parametrach.

Karty informacyjne z systemu *uplook Zasoby* zawierały następujące informacje o sprzęcie:

- informacje ogólne takie jak np.: nazwa, typ, status, numer inwentarzowy, kod księgowy, numer seryjny, lokalizacja, dział, główny użytkownik, osoba odpowiedzialna;

[29] Próba sprzętu IT została dobrana w sposób losowy przez kontrolera na podstawie wydruku z ewidencji.

- informacje księgowe takie jak np.: numer faktury, kod księgowy, dostawca, cena netto, vat, cena brutto, data zakupu, data nabycia, gwarancja, umowa serwisowa;
- informacje sprzętowe takie jak np.: model, procesor, liczba rdzeni procesora, RAM, rozmiar dysku, karta graficzna, rozdzielczość monitora, nazwa DNS, adresy IP, adres MAC, system operacyjny;
- informacje dodatkowe takie jak np.: główny użytkownik, producent;
- licencje: nazwa, wydawca, typ, wersja, opis;
- incydenty: Id, aktualizacja, status, priorytet, zgłaszający, rozwiązujący, rozwiązanie, dostęp, temat;
- użytkownicy.

Informacja o rodzaju i konfiguracji sprzętu zapewniająca ciągłość jego działania i możliwość odtworzenia po ewentualnej katastrofie lub zdarzeniu losowym była gromadzona w oprogramowaniu zarządzania zmianą[30]. Raporty o konfiguracji sprzętu były przesyłane mailowo. Dodatkowo ww. narzędzie dawało możliwość masowej zmiany konfiguracji sprzętu poprzez skrypty wysyłane na wiele urządzeń.

(akta kontroli str. 676-726)

1.15.Urząd przystąpił do Rządowego Programu „Cyberbezpieczny Samorząd". Umowa o powierzenie grantu[31] została podpisana w dniu 21 marca 2024 r. Zgodnie z postanowieniami umowy, Miasto jest zobowiązane do zrealizowania Projektu w zakresie rzeczowym w okresie maksymalnie 24 miesięcy od dnia jej wejścia w życie, ale nie dłużej niż do 30 czerwca 2026 r[32]. Całkowita wartość Projektu wynosi 850 tys. zł, pierwsza transza w wysokości 250 tys. zł została przekazana na rachunek bankowy Urzędu w dniu 29 kwietnia 2024 r. W ramach Projektu mają zostać zrealizowane następujące zadania:

- organizacyjne:
    a) zakup normy z serii ISO/IEC 27000 oraz normy ISO 22301 – działanie obejmuje Urząd Miejski, Powiatowy Urząd Pracy[33] oraz Ośrodek Pomocy Społecznej[34] w Świętochłowicach,
    b) wdrożenie SZBI[35] wraz z dokumentacją i szkoleniami zgodnie z wymogami ww. normy, uwzględniając również wdrożenie zarządzania ciągłością działania w oparciu o obowiązujące wymagania norm ISO/IEC 22301 oraz wymagania prawne – działanie obejmuje Urząd Miejski,
    c) przeprowadzenie audytów SZBI zgodnie z wymogami normy PN-EN ISO/IEC 27001:2023 oraz przeprowadzenie audytu związanego z rozliczeniem Projektu - działanie obejmuje Urząd Miejski, PUP oraz OPS w Świętochłowicach,
    d) przeprowadzenie audytu SZBI – działanie obejmuje Urząd Miejski. Urząd w celu opracowania koncepcji Projektu korzystał z usług doradczych, które miały na celu określenie najlepszych rozwiązań w zakresie podniesienia poziomu cyberbezpieczeństwa.

[30] Jest to bezobsługowe narzędzie, które robi kopię konfiguracji (po SSH) wszystkich urządzeń sieciowych (routery, switche, access pointy) sprawdzając w tym samym czasie zmiany konfiguracji.

[31] Umowa nr FERC.02.02-CS.01-001/23/0042/FERC.02.02-CS-001/23/2024.

[32] Ramy czasowe realizacji Projektu to 21 marca 2024 r. – 20 marca 2026 r.

[33] Dalej: „PUP".

[34] Dalej: „OPS".

[35] W Urzędzie nie funkcjonuje SZBI. Urząd posiada Politykę bezpieczeństwa, która nie uwzględnia wymagań określonych według normy PN-EN ISO/IEC 27001:2023 oraz jej poprzednich wersjach.

- kompetencyjne:
    e) autoryzowane szkolenie pracowników IT w zakresie:
- serwerowych systemów operacyjnych (celu podwyższenia kompetencji obsługi i zarządzania systemem serwerowym Windows Serwer);
- rozwiązań i zarządzania cyberbezpieczeństwem systemów w infrastrukturze IT, tj.: instalacją, konfiguracją oraz zarządzaniem rozwiązań EST funkcjonujących w Urzędzie;
- zarządzania systemami XDR;
- zarządzania infrastrukturą sieciową. Szkolenie umożliwi identyfikację podatności i zagrożeń w funkcjonowaniu sieci komputerowych oraz zarządzania nimi;
- zarządzania bezpieczeństwem IT - odbędą szkolenia i warsztaty dotyczące: wprowadzenia do zagadnień bezpieczeństwa IT, wybranych elementów bezpieczeństwa, SZBI – rozwiązań zabezpieczających systemy i infrastrukturę IT;
    f) szkolenie kierownictwa i pracowników na temat cyberzagrożeń i bezpieczeństwa informacji.
- techniczne:
    a) rozbudowanie przestrzeni dyskowej umożliwiającej wykonywanie i testowanie kopii zapasowych systemów IT oraz przechowywanie logów systemów, zakup macierzy dyskowej, która zapewni odpowiednie zasoby dla tych rozwiązań;
    b) Urząd nie posiada rozwiązania w zakresie zapobiegania niechcianym zdarzeniom w infrastrukturze, które zapewnią ochronę stacji roboczych, systemów serwerowych, pełne szyfrowanie dysków, sandboxing w chmurze oraz rozwiązanie Extended Detection & Response[36], dlatego planuje zakup i wdrożenie rozwiązania w tym zakresie;
    c) zakup i wdrożenie rozwiązania w zakresie kontroli dostępu do sieci;
    d) uzyskanie wsparcia ekspertów w zakresie zarządzania bezpieczeństwem informacji i cyberbezpieczeństwem;
    e) zapewnienie ciągłości wsparcia funkcjonowania rozwiązania do inwentaryzacji zarządzania zasobami informatycznymi, monitorowania zasobów oraz zarzadzania i monitorowania użytkowników[37];
    f) zapewnienie ciągłości wsparcia rozwiązania do administrowania sieci, monitorowania i zarządzania infrastrukturą IT[38];
    g) zapewnienie ciągłości funkcjonowania systemu do zarzadzania aktualizacjami oraz nadzorowania oprogramowania systemowego[39];
    h) przeprowadzenie skanowania podatności i zagrożeń infrastruktury IT oraz aplikacji web (stron internetowych jednostki) dotyczących cyberbezpieczeństwa przez podmiot zewnętrzny.

Przed przystąpieniem do Programu w Urzędzie został przeprowadzony audyt funkcjonowania SZBI, dokonano również analizy stanu cyberbezpieczeństwa

[36] Dalej: „XDR".

[37] Wsparcie serwisowe tego rozwiązania było zapewnione do 27 lutego 2024 r.

[38] Wsparcie serwisowe tego rozwiązania było zapewnione do 18 maja 2024 r.

[39] Wsparcie serwisowe tego rozwiązania było zapewnione do 27 stycznia 2024 r.

podczas opracowywania Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego i jednostkach podległych.

(akta kontroli str. 319-505)

W latach 2021-2023 Miasto uczestniczyło w Projekcie „Cyfrowa Gmina". Za kwotę 1 473,24 tys. zł brutto zakupiono: 20 komputerów, 20 monitorów, 10 laptopów, 30 pakietów biurowych, serwer wirtualizacyjny, system do komunikacji online oraz wideokonferencji, oprogramowanie Windows Server 2022 datacenter (dwa serwery i 400 licencji dostępowych), router brzegowy UTM Fortigate 200 F wraz z analizerem logów, dwa przełączniki 10G, trzy przełączniki 48p, przełącznik 24p, oprogramowanie do backupu Veeam Backup & Replication, oprogramowanie do e-usług. Ponadto z ww. środków rozbudowano i doposażono pozostałe serwery, rozbudowano i doposażono macierz dyskową, przeprowadzono szkolenia dla 300 urzędników z zakresu cyberbezpieczeństwa.

(akta kontroli str. 506-563)

Stwierdzone nieprawidłowości

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

1. Sklasyfikowanym zbiorom danych, które były przetwarzane w Urzędzie nie przypisano wag, ani odpowiedniego poziomu ochrony co było nierzetelne i niezgodne z pkt. A.8.1.1 i A.8.2.1 załącznika A normy PN-EN ISO/IEC 27001:2017, zgodnie z którą należy zidentyfikować informacje, aktywa związane z informacjami i środkami przetwarzania informacji oraz sporządzić i utrzymywać ewidencję tych aktywów; informacje powinny być klasyfikowane z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację.

Prezydent wyjaśnił, że *w ramach Projektu Cyberbezpieczny Samorząd opracowana zostanie dokumentacja SZBI, w ramach której zbiorom informacji zostaną przydzielone wagi oraz zostanie im przypisany odpowiedni poziom ochrony, jak również dokonana zostanie klasyfikacja zbiorów danych/informacji z uwzględnieniem wymagań prawnych wartości, krytyczności i wrażliwości. Umowa na opracowanie ww. dokumentacji została podpisana 25 czerwca 2024 r.*

(akta kontroli str. 15-26,113-254,1174-1175,1181)

2. W Urzędzie nie wdrożono SZBI, co stanowiło naruszenie § 19 ust. 1 rozporządzenia KRI, który stanowił, że podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność, w związku z ust. 3 tego rozporządzenia, który stanowił, że wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym: 1) PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń; 2) PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem.

Prezydent wyjaśnił, że *formalnie w Urzędzie nie wprowadzono SZBI natomiast wdrożono wiele elementów systemu. Ponadto 25 czerwca 2024 r. została podpisana umowa na opracowanie dokumentacji SZBI w ramach Programu „Cyberbezpieczny*

samorząd". Zarządzeniem Prezydenta[40] powołano grupę roboczą do opracowania dokumentacji SZBI. Termin wykonania i wprowadzenia ww. dokumentacji został określony na dzień 1 września 2024 r.

(akta kontroli str. 104-110,119,1206-1207)

NIK wskazuje, że przywołane w wyjaśnieniach „elementy systemu" nie tworzą spójnego, usystematyzowanego systemu, co nie pozwala na zrealizowanie wymogów określonych w § 19 ust. 1 ww. rozporządzenia.

3. W Urzędzie nie ustanowiono polityki ciągłości działania, określającej założenia, zakres oraz podstawowe zasady zarządzania ciągłością działania i w rezultacie: nie opracowano Planu zapewnienia ciągłości działania ani planów odtworzeniowych i nie określono akceptowalnego czasu na przywrócenie ciągłości działania systemów informatycznych; nie testowano i nie poddano treningowi Polityki ciągłości działania; nie wyznaczono również pracowników odpowiedzialnych za bezpieczeństwo informacji oraz zapewnienie ciągłości działania. Niepodjęcie działań ww. zakresie należy uznać jako nierzetelność.

(akta kontroli str. 10-26, 65-72,104-112)

Z wyjaśnień Prezydenta wynika, że *zachowanie ciągłości działania Urzędu polega na zaimplementowaniu rozwiązań technicznych takich jak: nadmiarowość/redundancja urządzeń stanowiących krytyczną infrastrukturę (serwery, router brzegowy, przełączniki sieciowe) oraz wielopoziomowego systemu tworzenia kopii zapasowych opartego na uznanym rozwiązaniu pn. Veeam Backup&Replication.* Prezydent wyjaśnił również, że *poza Polityką Bezpieczeństwa w Urzędzie nie wprowadzono innych polityk w tym zakresie. Planowane jest opracowanie dokumentacji dotyczącej ciągłości działania w oparciu o normę ISO 22301 – wymagania dla systemu zarządzania ciągłością działania w ramach Projektu „Cyberbezpieczny Samorząd".*

(akta kontroli str. 10-26, 65-72,104-112)

Odnośnie niewyznaczenia pracowników odpowiedzialnych za bezpieczeństwo informacji Naczelnik Wydziału Organizacyjnego wyjaśniła, że *z uwagi na brak wprowadzenia procedur zapewnienia ciągłości działania, nie wyznaczono pracowników odpowiedzialnych za bezpieczeństwo informacji.*

(akta kontroli str. 668-669)

NIK wskazuje, że celem Polityki ciągłości działania jest określenie założeń, zakresu oraz podstawowych zasad zarządzania ciągłością działania oraz zdefiniowanie, w jaki sposób Urząd zapewni, że spełnione będą wszystkie warunki umożliwiające odtworzenie działalności po katastrofie lub innym incydencie zakłócającym działanie. Celem zarządzania ciągłością działania jest identyfikacja potencjalnych zagrożeń dla urzędu, określenie wpływu, jaki zagrożenia te mogą wywrzeć na działalności jednostki oraz zapewnienie odpowiedniego przygotowania urzędu na sytuacje awaryjne, dające możliwość efektywnego reagowania na sytuacje awaryjne i zapewnienie dalszego ciągłego działania Urzędu. Dokument ten stanowi podstawę opracowania Planu zapewnienia ciągłości działania oraz planów odtworzeniowych.

Stosownie do ustalonej normy określonej w załączniku A PN-ISO/IEC 27001:2017, pkt A.17.1.1. pkt A.17.1.2 i pkt 17.1.3., przy planowaniu ciągłości bezpieczeństwa informacji Urząd powinien określić wymagania dotyczące bezpieczeństwa informacji i ciągłości zarządzania bezpieczeństwem informacji w niekorzystnych sytuacjach np. w czasie kryzysu lub katastrofy, przy wdrażaniu ciągłości bezpieczeństwa Urząd

[40] Zarządzenie Nr 274/2024 z dnia 8 lipca 2024 r. w sprawie wyznaczenia członków grupy roboczej do opracowania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Świętochłowicach.

powinien ustanowić, udokumentować, wdrożyć i utrzymywać procesy, procedury i zabezpieczenia dla zapewnienia w niekorzystnej sytuacji wymaganego poziomu ciągłości bezpieczeństwa informacji oraz przy weryfikowaniu, przeglądzie i ocenie ciągłości bezpieczeństwa informacji Urząd powinien weryfikować ustanowione i wdrożone zabezpieczenia ciągłości bezpieczeństwa informacji w regularnych odstępach czasu celem zapewnienia ich aktualności i skuteczności w niekorzystnych sytuacjach.

OCENA CZĄSTKOWA

Zbiorom danych przetwarzanych w Urzędzie, podlegających zabezpieczeniu nie przypisano odpowiedniego poziomu ochrony, w tym nie uwzględniono określonych w Polskiej Normie wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację. W Urzędzie nie wdrożono SZBI, nie podjęto również działań regulacyjnych dotyczących zapewnienia ciągłości działania.

W jednostce wprowadzono natomiast Politykę Bezpieczeństwa Informacji, która była na bieżąco aktualizowana. Powołano IOD posiadającego odpowiednie kwalifikacje do pełnienia tej funkcji oraz sporządzono dokumentację w zakresie ochrony danych osobowych. Ponadto władze Miasta wystąpiły o środki z programów „Cyfrowa Gmina" i „Cyberbezpieczny Samorząd" na poprawę Cyberbezpieczeństwa.

OBSZAR

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

Opis stanu faktycznego

2.1.Brak możliwości zainstalowania nieautoryzowanego oprogramowania został zweryfikowany na podstawie oględzin 10 komputerów[41], na których podjęto próbę instalacji nieautoryzowanego oprogramowania[42], po uprzednim ustaleniu faktycznie zalogowanego użytkownika danego komputera.

Oględziny wykazały, że do przeprowadzenia operacji instalacji oprogramowania wymagane było posiadanie uprawnień administratora lokalnego.

W wyniku oględzin ustalono, że na wszystkich badanych komputerach niemożliwe było zainstalowanie oprogramowania testowego - na kontach użytkowników, system wyświetlił monit o podniesienie uprawnień do poziomu administratora. Było to zgodne z § 20 ust. 2 pkt 2 rozporządzenia KRI.

(akta kontroli str. 919-920)

W jednostce kontrolowanej zdecydowana większość pracowników użytkowała komputery stacjonarne. Urząd posiadał również służbowe tablety, jednak jak wynika z wyjaśnień Prezydenta, *dostęp do tabletów zakupionych przez Wydział Informatyki stanowiących element systemu głosowania podczas sesji Rady Miejskiej został zabezpieczony kodem PIN. Służbowe telefony komórkowe nie zostały zabezpieczone przed instalacją oprogramowania przez użytkownika, jednakże wykorzystanie sprzętu służbowego zostało uregulowane w Polityce bezpieczeństwa.*

Odnośnie do braku zabezpieczenia służbowych telefonów komórkowych przed instalacją oprogramowania przez użytkownika Prezydent wyjaśnił, że *planowane jest przygotowanie i wdrożenie procedury określającej postępowanie z tabletami i telefonami służbowymi przed przekazaniem ich pracownikom. W procedurze*

[41] 8 komputerów stacjonarnych i 2 laptopów. Komputery poddane oględzinom zostały wytypowane w sposób losowy przez kontrolera przeprowadzającego oględziny.

[42] Plik testowy – aplikacji Adobe Reader.

zostanie ujęty proces konfiguracji ww. sprzętu w zakresie zabezpieczenia oprogramowaniem monitorującym.

(akta kontroli str. 10-14,1184-1185)

2.2.Nadawanie, modyfikowanie i odbieranie uprawnień/dostępów do systemów, rejestrów, baz danych został zweryfikowany na podstawie oględzin dostępów posiadanych przez 15 pracowników wykonujących zadania w systemach informatycznych.

Oględziny posiadanych przez 15[43] pracowników Urzędu uprawnień wykazały, że pracownicy posiadali uprawnienia zgodne z realizowanymi czynnościami zapisanymi w zakresach obowiązków a osoby, które zmieniły stanowisko pracy w Urzędzie i przeszły do innej komórki organizacyjnej nie posiadały dostępu do systemów informatycznych używanych do realizacji zadań w poprzedniej komórce organizacyjnej.

Nadawanie, modyfikowanie, odbieranie uprawnień do systemów, baz danych było realizowane w oparciu o:

- Politykę Bezpieczeństwa – punkt 21.1 Kontrola dostępu do systemu informatycznego.
- Załącznik nr 1 do Polityki Bezpieczeństwa – Instrukcja Zarządzania Systemem Informatycznym.
  a) Rozdział 8. Procedura nadawania uprawnień do przetwarzania danych osobowych.
  b) Rozdział 4 Zabezpieczenia programów i baz przetwarzających dane osobowe.

Wydział Informatyki opracował system wniosków elektronicznych oraz wdrożył dedykowany system help-desk. Jeżeli ww. system był stosowany przez kierowników komórek organizacyjnych, Wydział Informatyki posiadał pełną historię posiadanych przez pracownika uprawnień wraz ze wszystkimi modyfikacjami. W przypadku realizowania przez przełożonych wniosków o nadanie uprawnień pracownikom w inny sposób aniżeli poprzez wniosek elektroniczny (np. za pośrednictwem poczty elektronicznej), Wydział Informatyki posiadał jedynie informacje o aktualnych dostępach danego pracownika.

Każdy wniosek o nadanie / odebranie / modyfikację uprawnień był weryfikowany. Jednakże w części merytorycznej, czyli w obszarze dostępu i uprawnień do systemów dziedzinowych, to bezpośredni przełożony decydował o poziomie uprawnień.

Badanie próby wykazało, że uprawnienia pracowników nie były zawyżane.

(akta kontroli str. 1135-1155)

2.3.Blokowanie dostępu do systemów informatycznych byłym pracownikom zostało zweryfikowane na podstawie oględzin 15[44] kont byłych pracowników.

Oględziny wykazały, że konta pracowników, którzy zakończyli pracę w Urzędzie były zamykane. Jednakże usługa katalogowa Microsoft Active Directory nie przechowywała informacji o wyłączeniu konta. Po wyłączeniu konta atrybut „whenchanged" był aktualizowany o bieżącą datę i godzinę, jednak nie było gwarancji, że obiekt nie został zmieniony od czasu jego wyłączenia. W przypadku dokonania modyfikacji konta nie było informacji o tym kto jej dokonał.

[43] 11 Naczelników Wydziałów, Skarbnik Miasta, 3 pracowników, którzy zmienili komórkę organizacyjną.

[44] Próba została wytypowana w sposób losowy z wykazu pracowników, którzy zakończyli pracę w Urzędzie.

Zamknięcie konta było określane w systemie jako CHECKED lub NOT CHECKED. Jednakże system nie informował o dacie zablokowania konta, a jedynie o ostatniej modyfikacji.
Pomimo tego, że w Urzędzie istnieje System tworzenia / blokowania kont oraz nadawania / odbierania uprawnień w oparciu o rozwiązanie polegające na dokonywaniu zgłoszeń poprzez dedykowane formularze elektroniczne dostępne dla pracowników z poziomu przeglądarki internetowej – zgłoszeń nie dokonano w dziewięciu na 15 przebadanych kont (tj.60%), w pozostałych sześciu przypadkach (40% badanej próby) wnioski o zamknięcie konta wpłynęły do Wydziału Informatyki w terminie od jednego do pięciu dni po zakończeniu pracy przez pracownika.

(akta kontroli str. 1188-1192)

2.4.Oględziny trzech[45] systemów informatycznych Urzędu pod kątem wymagań dla haseł dostępu wykazały, że dla poszczególnych systemów zostały ustalone wymogi w zakresie tworzenia oraz zmiany haseł dotyczące ich długości (osiem, dziesięć znaków), zawierania dużych liter, cyfr i znaków specjalnych. Określony został również 30 dniowy termin ważności hasła. W badanych systemach Urząd stosował wszystkie udostępnione opcje wymagań dotyczące haseł. We wszystkich badanych systemach loginy można było przypisać do konkretnego użytkownika, jednakże w ww. systemach poza kontami użytkowników istniały również konta techniczne – producenta programu i administratora.
Jak wyjaśnił Prezydent działania poszczególnych użytkowników korzystających z tego samego loginu są rozliczane *z poziomu administratora systemu oraz dostępu do sieci badając, który użytkownik zalogował się do domeny Active Directory, a następnie nawiązał połączenie do danego serwera (adres IP +port).*

(akta kontroli str. 1156-1160,1185)

2.5.Ustaleń dotyczących zachowania poufności danych wyświetlanych na monitorach komputerowych w miejscach obsługi obywateli dokonano na podstawie oględzin trzech stanowisk pracy w Wydziale Spraw Obywatelskich, na których były realizowane zadania z wykorzystaniem aplikacji „Źródło". Oględziny wykazały, że monitory usytuowane były w sposób uniemożliwiający wgląd do danych przez osoby nieuprawnione, tym samym zostały spełnione wymogi § 20 ust. 2 pkt 7 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 informatycznych.

Jeden z monitorów był odwrócony w stronę osób odbierających dowody osobiste, jednakże jak wyjaśnił Naczelnik Wydziału, *na tym komputerze pracownicy nie mają dostępu do aplikacji „źródło"*. Pracownicy Wydziału korzystali na nim z elektronicznej poczty służbowej, edytora tekstu, arkusza kalkulacyjnego etc. Monitor ustawiony był w odległości około trzech metrów od osób realizujących sprawy związane z otrzymaniem lub wymianą dowodu osobistego.

Przyczyną usytuowania monitora w stronę osób realizujących sprawy w Urzędzie są warunki lokalowe i trudności w przeorganizowaniu stanowisk pracy.

(akta kontroli str. 670-675)

2.6.Regulamin pracy zdalnej został wprowadzony Zarządzeniem Prezydenta w kwietniu 2023 r.[46] pomimo tego, że praca zdalna w Urzędzie była możliwa od listopada 2020 r.[47] W ww. regulaminie opisano zasady korzystania ze sprzętu

[45] Dysponent, Taxi+, RESTO.

[46] Zarządzenie Prezydenta Miasta Nr 190/2023 z dnia 12 kwietnia 2023 r. w sprawie wprowadzenia Regulaminu pracy zdalnej w Urzędzie Miejskim w Świętochłowicach. Regulamin wszedł w życie 23 kwietnia 2023 r.

[47] Pracę zdalną wprowadzono Zarządzeniem Prezydenta Miasta Nr 867/2020 z dnia 3 listopada 2020 r. w sprawie wykonywania pracy zdalnej w Urzędzie Miejskim w Świętochłowicach.

informatycznego minimalizujące ryzyka kradzieży informacji. Treść Regulaminu została podana do wiadomości pracowników poprzez jego udostępnienie w wewnętrznej sieci Intranet, wysłanie komunikatu do pracowników pocztą elektroniczną oraz wywieszenie dokumentu na tablicy informacyjnej. Było to zgodne z § 20 ust. 2 pkt 8 rozporządzenia KRI.

(akta kontroli str. 596-638)

2.7.Prezydent wyjaśnił, że *Wydział Informatyki zabezpiecza komputery w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym, poprzez szyfrowanie oraz wykorzystanie usługi katalogowej Active Directory w celu autoryzacji dostępu do danych*.

(akta kontroli str. 10-14).

2.8.Oględziny zabezpieczeń fizycznych zastosowanych w serwerowni wykazały, że serwerownia nie była właściwie zabezpieczona, co zostało opisane w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 921-931,1182-1183,1213)

2.9.Na podstawie badania treści czterech umów zawartych pomiędzy Gminą Świętochłowice a podmiotami zewnętrznymi na: 1. serwis i nadzór nad funkcjonowaniem oprogramowania RATUSZ, 2. Konserwację i nadzór eksploatacyjny nad programem „eMandat:, 3. Serwis i nadzór autorski nad prawidłowością funkcjonowania oprogramowania[48], 4. Świadczenia usług utrzymania oraz rozwoju oprogramowania stwierdzono, że w umowach zostały zawarte zapisy mówiące o zobowiązaniu wykonawcy do zachowania tajemnicy informacji do jakich może mieć dostęp w związku z ich realizowaniem, co było zgodne z § 20 ust. 2 pkt 10 rozporządzenia KRI.

(akta kontroli str. 639-667)

2.10.Z wyjaśnień Prezydenta wynika, że *nośniki zawierające dane (dyski) zostają zawsze w Urzędzie. Zbycie/likwidacja sprzętu komputerowego również odbywa się po demontażu nośników (dysków), które następnie są komisyjnie niszczone. W latach 2023-2024 nie miało miejsca wydanie sprzętu zewnętrznemu serwisowi.*

(akta kontroli str. 15-26,52-64)

2.11.Procedura tworzenia kopii zapasowych przewidywała budowanie sekwencji ich tworzenia kopii na czterech poziomach. Dostęp do kopii zapasowych posiadał Administrator Systemu Informatycznego.

(akta kontroli str. 15-26,65-72)

2.12.W jednostce kontrolowanej zasady tworzenia, przechowywania i testowania kopii zapasowych regulowała Procedura tworzenia kopii zapasowych stanowiąca pkt 11 Polityki Bezpieczeństwa.

W wyniku oględzin ustalono, że kopie zapasowe były tworzone w następujący sposób:

1. zakres zasobów objętych tworzeniem kopii obejmował wszystkie używane maszyny wirtualne jednostki kontrolowanej oraz obecne w nich systemy IT;

2. kopie wykonywane były na czterech poziomach zgodnie z przyjętym harmonogramem dla każdego poziomu, poza godzinami pracy jednostki kontrolowanej:

[48] Oprogramowanie: Adres – rejestr numeracji nieruchomości, Bank osnów – bank poziomych i wysokościowych osnów geodezyjnych, Dokument- kartoteka opisowo graficzna obiektów EWMAPY, Drogi – ewidencja dróg oraz obiektów mostowych, Ewmapa – system grafiki komputerowej, Ewopis – system ewidencji gruntów, budynków i lokali z kartoteką podatkową, Mienie – ewidencja mienia gminy, powiatu lub Skarbu Państwa, Ośrodek – system ewidencji i zarządzania dokumentami w ośrodkach dokumentacji geodezyjnej i kartograficznej, Rejcen – rejestr cen i wartości nieruchomości, Winplan – plan zagospodarowania przestrzennego, Znaki – system rejestracji oznakowania dróg.

Testowanie kopii było wykonywane ręcznie, po wykonaniu testów administrator systemu otrzymywał pocztą elektroniczną raport z wynikiem testu. Według wyjaśnień Naczelnika Wydziału Informatyki, *wiadomość taka po potwierdzeniu poprawnego wyniku testów była usuwana.*

Aktualizacje i zmiany konfiguracyjne w używanych systemach były wprowadzane przez pracowników Wydziału Informatyki poza godzinami pracy jednostki kontrolowanej, po wykonaniu kopii zapasowych.

Test odzyskania z kopii pliku wskazanego przez kontrolera wykazał poprawność kopii oraz potwierdził możliwość odtworzenia zapisanych informacji.

(akta kontroli str. 1166-1173)

2.13.W Urzędzie nie opracowano procedur dotyczących monitorowania pojemności nośników pamięci. Natomiast pojemność nośników pamięci systemów Urzędu była monitorowana. Przeprowadzone oględziny zajętości nośników pamięci systemów informatycznych Urzędu wykazały, że zajętych było 32,25% klastra dysków SSD i 40,28% klastra dysków SAS.
Z powodu zbliżającego się terminu zakończenia wsparcia technicznego użytkowanej macierzy, Urząd był w procesie realizacji postępowania o udzielenie zamówienia publicznego na zakup nowego systemu macierzowego, który miał zostać sfinansowany w ramach projektu „Cyberbezpieczny Samorząd".
W trakcie oględzin stwierdzono zajętość pamięci niektórych maszyn wirtualnych na poziomie powyżej 80 %. Taki poziom zajętości nośników pamięci nie był uznawany za krytyczny, gdyż alerty poziomu zajętości nośników pamięci zostały ustawione na 90%.
Jak wyjaśnił Prezydent *alerty w ramach używanych systemów zostały ustawione w oparciu o progi skonfigurowane przez producentów oprogramowania (progi domyślne/dobre praktyki).*

(akta kontroli str. 932-935,1186)

2.14.W Urzędzie została opracowana dokumentacja dotycząca ochrony danych osobowych składająca się z Polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym.
Jak wyjaśnił Prezydent: *Urząd posiada rozwiązania w zakresie monitorowania funkcjonowania systemów IT oraz zabezpieczenia w zakresie ochrony antywirusowej. W ramach programu Cyberbezpieczny Samorząd zostanie podniesiony poziom ochrony infrastruktury IT oraz zostanie wdrożony SZBI wraz z procedurami dotyczącymi ciągłości działania.*
Odnośnie do czasu przywracania poszczególnych systemów oraz procesów do działania Prezydent wyjaśnił, że *Urząd przywraca działanie systemu doraźnie w ramach potrzeb. Nie prowadzi się dokumentacji w tym zakresie. W ramach Programu Cyberbezpieczny Samorząd planowane jest wprowadzenie aktualizacji dokumentacji dla zapewnienia zgodności z normą ISO 27001 wraz z planem ciągłości działania oraz obowiązkiem wykonywania testów odtworzenia kopii.*

(akta kontroli str. 10-14)

Ponadto, Prezydent wyjaśnił, że *kluczowe elementy infrastruktury IT, jak również stanowiska komputerowe w Wydziale IT zostały zabezpieczone przed utratą zasilania poprzez zastosowanie urządzenia UPS. Problem awaryjności łącza internetowego został rozwiązany poprzez zastosowanie dwóch niezależnych przyłączy należących do różnych operatorów internetowych. Ponadto router brzegowy posiada tryb failover, który w sposób zautomatyzowany wykrywa przerwy i balansuje ruchem sieciowym pomiędzy dostępnymi łączami internetowymi.*

Zabezpieczenie fizyczne serwerowni przed kradzieżą czy włamaniem opierają się na monitoringu wizyjnym, systemie alarmowym, a budynek został objęty ochroną realizowaną przez firmę zewnętrzną. Wdrożono również system ograniczenia

dostępu poprzez rejestrowanie obiegu kluczy. Do pomieszczenia serwerowni mają dostęp jedynie pracownicy Wydziału Informatyki.

(akta kontroli str. 15-26)

Stwierdzona nieprawidłowość

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

Pomieszczenie serwerowni nie zostało właściwie zabezpieczone z uwagi na m.in.:

- wyraźne jego oznaczenie z zewnątrz – co umożliwiało identyfikację przeznaczenia pomieszczenia przez osoby postronne;
- zainstalowany w pomieszczeniu serwerowni system ochrony przeciwpożarowej, który nie został przetestowany pod kątem sprawności oraz
- brak ewidencji wyjść i czasu przebywania pracowników w pomieszczeniu.

Prezydent wyjaśnił, że *system przeciwpożarowy zainstalowany w serwerowni jest przestarzały wobec powyższego prowadzone są rozmowy i konsultacje dotyczące wyboru nowego systemu przeciwpożarowego i jego zastosowania w pomieszczeniu serwerowni. Ustalanie tożsamości osób przebywających w serwerowni odbywa się na podstawie monitoringu wizyjnego. W ramach budżetu na rok 2024 planowana jest wymiana/ modernizacja systemu kontroli dostępu do serwerowni oraz warunków środowiskowych w niej panujących. Ponadto w dniu 1 lipca 2024 r. zostało usunięte zewnętrzne oznaczenie serwerowni (etykieta na drzwiach).*

(akta kontroli str. 921-931,1182-118,1213)

OCENA CZĄSTKOWA

Wdrożone i wykorzystywane w Urzędzie rozwiązania organizacyjne i techniczne zapewniały bezpieczeństwo informacji oraz ciągłość działania systemów informatycznych Urzędu m.in. poprzez uniemożliwienie zainstalowania nieuprawnionego oprogramowania na komputerach pracowników, prawidłowe nadawanie, modyfikowanie oraz odbieranie uprawnień użytkownikom. W Urzędzie opracowano regulacje dotyczące ochrony danych osobowych, nadawania haseł dostępu, tworzenia, testowania i przechowywania kopii zapasowych. Ponadto, zapewniona została ochrona danych wyświetlanych na monitorach pracowników przed dostępem osób trzecich. Sprzęt komputerowy oraz nośniki danych były prawidłowo zabezpieczane przed dostępem osób nieuprawnionych oraz instalacją zewnętrznego oprogramowania przez użytkownika. Pojemność nośników pamięci była na bieżąco monitorowana. W umowach zawieranych z podmiotami zewnętrznymi zawarto zapisy mówiące o zobowiązaniu do zachowania tajemnicy informacji. Stwierdzona nieprawidłowość dotyczyła niewłaściwego zabezpieczenia pomieszczenia serwerowni.

OBSZAR

3.Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

3.1.Sposób zarządzania ryzykiem bezpieczeństwa informacji wynikał z załącznika nr 9 do Polityki bezpieczeństwa dotyczącego analizy ryzyka, jak również z Zarządzenia Prezydenta[49] w sprawie kontroli zarządczej w Urzędzie Miejskim w Świętochłowicach oraz jednostkach organizacyjnych Miasta.
W latach 2023-2024 w Urzędzie została przeprowadzona analiza ryzyka.
Po przeprowadzonej w Urzędzie analizie ryzyka sformułowane zostały zalecenia dotyczące:

- opracowania i wdrożenia procedur zabezpieczających dane wykorzystywane przez pracowników, którzy przemieszczają się

[49] Zarządzenie Nr 665/2020 z dnia 1 października 2020 r.

z dokumentacją pomiędzy obiektami Urzędu znajdującymi się w różnych lokalizacjach;
- dopuszczenia do użycia wyłącznie zakwalifikowanych nośników zewnętrznych (pendrive, dysk zewnętrzny, karta pamięci etc.);
- konieczności podejmowania cyklicznych działań kontrolnych dotyczących poziomu ryzyka.

W ramach realizacji zaleceń zakupiono zamykane teczki zapewniające bezpieczne przenoszenie dokumentacji pomiędzy obiektami Urzędu, trwają prace nad przygotowaniem projektu zarządzenia Prezydenta w sprawie wprowadzenia zasad postępowania z pamięciami zewnętrznymi, raz w roku IOD przeprowadza ocenę ryzyka w zakresie RODO, przeprowadzana jest również analiza ryzyka w zakresie kontroli zarządczej.

(akta kontroli str. 80-103,1183)

3.2.Procedury dotyczące zgłaszania incydentów naruszania bezpieczeństwa informacji, incydentów dotyczących danych osobowych i / lub incydentów cyberbezpieczeństwa stanowiły część Polityki bezpieczeństwa[50]. W ramach ww. procedury pracownicy byli zobligowani do zgłaszania incydentów przełożonemu lub IOD poprzez wysłanie wiadomości na dedykowane adresy mailowe. Pracownicy mogli dokonywać zgłoszeń w zakresie naruszenia bezpieczeństwa informacji, poprzez formularz udostępniony w wewnętrznej sieci Urzędu – Intranet.
Ponadto, dwóch pracowników Urzędu zostało wyznaczonych do kontaktu z CSIRT NASK w przypadku cyberataków.

(akta kontroli str. 104-112,313-318,731-739)

Prezydent wyjaśnił, że *w okresie objętym kontrolą nie zostały stwierdzone incydenty, ani naruszenia w zakresie ochrony danych osobowych. W ramach Programu Cyberbezpieczny Samorząd zostanie opracowana dokumentacja oraz wdrożony SZBI wraz z procedurami dotyczącymi reagowania na incydenty z zakresu naruszenia bezpieczeństwa informacji.*

(akta kontroli str. 10-14)

3.3.W 2022 r. w ramach programu „Cyfrowa Gmina" zostało przeprowadzone szkolenie stacjonarne z obszaru cyberbezpieczeństwa[51] dla 300 urzędników.

W latach 2023-2024 Urząd zakupił dwa pakiety szkoleń w modelu e-learning o tematyce „Bezpieczny Pracownik w Cyberprzestrzeni tzw. Security Awareness"

[50] Opisane w dziale 21.4 Zarządzanie incydentami i naruszeniami i stanowiące załącznik nr 41 – Procedura postępowania w przypadku naruszenia ochrony danych osobowych.

[51] Szkolenie dotyczyło następujących zagadnień: czym jest cyberbezpeiczeństwo?, Główne założenia i wymagania prawne cyberbezpieczństwa w pracy urzędnika, elementy składowe wdrożenia wymagań ustawy o krajowym systemie cyberbezpieczeństwa, System Zarządzania Bezpieczeństwem Informacji (SZBI), proces wdrażania SZBI, polityka bezpieczeństwa informacji w organizacji, definicja incydentu bezpieczeństwa i zasady postepowania z incydentem, rodzaje incydentów, przyczyny incydentów bezpieczeństwa, skutki incydentów bezpieczeństwa, ataki sieciowe i komputerowe, bezpieczeństwo fizyczne i środowiskowe, zabezpieczenie informatycznych nośników danych, zdalny dostęp do zasobów jednostki, korzystanie z urządzeń prywatnych przez pracowników oraz związane z tym potencjalne zagrożenia, zasady korzystania ze służbowego sprzętu do celów prywatnych, przechowywanie danych w chmurze i korzystanie z zewnętrznych dostawców usług informatycznych, narzędzia do pracy w chmurze, prawidłowe korzystanie z oprogramowania antywirusowego, zasady aktualizacji programów i aplikacji, szyfrowanie komunikacji, dokumentów i poczty elektronicznej, polityka haseł, zarządzanie dostępem i tożsamością,

część pierwsza obejmowała 13[52] lekcji, część druga 10[53] lekcji. Obydwie części szkolenia zakończone były testem sprawdzającym wiedzę.

Zakupione przez Urząd licencje szkoleniowe miały charakter wieczysty. Pracownicy mogli wielokrotnie skorzystać poszczególnych modułów szkoleniowych.

W szkoleniach wzięło udział odpowiednio – w części pierwszej 67% pracowników, w części drugiej 59% pracowników.

Ponadto, IOD co roku przeprowadza szkolenia pracowników w zakresie ochrony informacji. W okresie objętym kontrolą IOD przeprowadził pięć szkoleń: cztery[54] w 2023 r. i jedno[55] w 2024 r.

(akta kontroli str. 15-26,73-79,740-808)

3.4.Audyt wewnętrzny z zakresu bezpieczeństwa informacji był w Urzędzie corocznie przeprowadzany[56] przez IOD, przy czym analizy ryzyka oraz audyt wewnętrzny z zakresu bezpieczeństwa wykonywane były przez tę sama osobę (IOD), co zostało opisane w sekcji *Stwierdzone nieprawidłowości.*
W 2023 r. w Raporcie z weryfikacji stosowania Polityki bezpieczeństwa oraz procedur ochrony danych osobowych w zakresie zgodności z RODO[57] zawartych zostało 13 rekomendacji.

W 2024 r. Raport z weryfikacji Polityki bezpieczeństwa zawierał 11 rekomendacji,

Po każdym audycie Naczelnicy Wydziałów/ Kierownicy komórek organizacyjnych oraz pracownicy zajmujący wyodrębnione ze struktury stanowiska w Urzędzie byli obligowani do stosowania zawartych w Raporcie rekomendacji.

Ww. pracownicy informowali Wydział Organizacyjny o stosowaniu rekomendacji, bądź o problemach w ich stosowaniu wynikających np. z braku zamykanych szaf na dokumenty, czy też zepsutych zamkach w szafach na dokumenty.

Jak wyjaśnił Prezydent *były dokonywane liczne wymiany zamków w meblach biurowych, a także w ramach posiadanych środków finansowych dokonano zakupu nowych mebli biurowych, dla wydziałów zgłaszających takie zapotrzebowanie.*

(akta kontroli str.809-840,1181,1210-1212)

Stwierdzona nieprawidłowość

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

Zarówno analiza ryzyka, jak i audyt bezpieczeństwa były przeprowadzane corocznie przez tę samą osobę – IOD, co naruszało zasadę niezależności i obiektywizmu audytu.
Prezydent wyjaśnił m.in., że *przeprowadzanie tych czynności przez IOD daje możliwość ustalenia priorytetów i skoncentrowania się na aspektach pociągających za sobą większe ryzyko. Takie podejście również ułatwia doradzanie administratorowi danych, na które operacje przetwarzania należy przeznaczyć więcej czasu i zasobów*

[52] Moduł 1 – Wprowadzenie do bezpieczeństwa informacji, Moduł 2 – Czym jest Phishing?, Moduł 3 – Internet, Moduł 4 – Portale, Moduł 5 – Poczta, Moduł 6 – Hasła, Moduł 7 – Socjotechnika, Moduł 8 – Mobile, Moduł 9 – Prawo, Moduł 10- Bezpieczeństwo, Moduł 11- Ransomware, Moduł 12 – Zabezpieczenia, Moduł 13 – Vishing.

[53] Moduł 14 – Cyberprzestępcy, Moduł 15 – Menadżer haseł, Moduł 16 – Mul finansowy, Moduł 17 – Bezprzewodowe życie, Moduł 18 – Praca zdalna, Moduł 19 – Phishing 2.0, Moduł 20 – Jak cyberprzestępcy kradną dane przez telefon, Moduł 21 – Fake News, Moduł 22 – Ciągłość działania, Moduł 23 – Cloud.

[54] Ochrona i przetwarzanie danych osobowych – projekt „Wsparcie dla uczniów z Ukrainy – Świętochłowice – Miasto na prawach powiatu" dwie edycje – zrealizowane 16 stycznia 2023 r. i 4 grudnia 2023 r., Ochrona i przetwarzanie danych osobowych – zrealizowane 5 czerwca 2023 r., Ochrona i przetwarzanie danych osobowych – projekt „O zdrowie dbamy, bo ergonomię mamy" – zrealizowane 27 marca 2023 r.

[55] Ochrona i przetwarzanie danych osobowych – projekt „Kreujemy zawodową przyszłość w Świętochłowicach" – zrealizowane 8 kwietnia 2024 r.

[56] W 2023 r. – od 2 stycznia do 20 lutego 2023 r., w 2024 r. – od 8 stycznia do 26 lutego.

[57] Dalej: „Raport z weryfikacji Polityki bezpieczeństwa.", lub „Raport."

i które obszary powinny zostać poddane ewentualnym zmianom oraz jakie szkolenia należy przeprowadzić dla pracowników lub kierowników odpowiedzialnych za przetwarzanie danych.

(akta kontroli str.809-840,1181,1210-1212)

NIK nie podziela argumentacji Prezydenta m.in. z uwagi na to, że IOD odpowiada za identyfikację ryzyk i ustanowienie w tym zakresie stosownych zabezpieczeń a audytor wewnętrzny za ocenę skuteczności wdrożonych zabezpieczeń, tym samym funkcje te nie powinny być łączone, gdyż ich połączenie stwarza ryzyko braku obiektywizmu oraz niezależności audytu.

OCENA CZĄSTKOWA

W Urzędzie były podejmowane działania w celu zapobiegania incydentom w zakresie bezpieczeństwa informacji w szczególności poprzez coroczne przeprowadzanie analizy ryzyka i wewnętrznych audytów z zakresu bezpieczeństwa informacji. Ponadto zostały opracowane procedury dotyczące zgłaszania incydentów naruszania bezpieczeństwa informacji, incydentów dotyczących danych osobowych i/lub incydentów cyberbezpieczeństwa, a pracownicy na bieżąco uczestniczyli w szkoleniach z zakresu cyberbezpieczeństwa. Stwierdzona nieprawidłowość dotyczyła dopuszczenia do przeprowadzania przez IOD zarówno analizy ryzyka, jak i wewnętrznego audytu bezpieczeństwa informacji.

IV. Wnioski

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

Wnioski

1. Sklasyfikowanie przetwarzanych informacji z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację i przypisanie informacjom odpowiedniego poziomu ochrony.
2. Opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji o którym mowa w § 19 ust. 1 w związku z ust. 3 rozporządzenia KRI, uwzględniającego zalecenia normy PN-ISO/IEC 27001 i norm z nią związanych (PN-ISO/IEC 27002, PN-ISO/IEC 27005, PN-ISO/IEC 24762).
3. Ustanowienie Polityki ciągłości działania i w związku z tym opracowanie i wdrożenie Planu zapewnienia ciągłości działania oraz planów odtworzeniowych, zapewnienie ich testowania i treningu oraz wyznaczenie pracowników odpowiedzialnych za bezpieczeństwo informacji oraz zapewnienie ciągłości działania i przypisanie im czynności w tym zakresie.
4. Zapewnienie prowadzenia audytów w zakresie bezpieczeństwa informacji przez różne osoby aby zapewnić ich niezależność i obiektywizm.
5. Zapewnienie właściwego zabezpieczenia serwerowni.

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 wykonania wniosków

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

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

Katowice, dnia 20 września 2024 r.

Kontroler
Kinga Kołodziejczyk
St. inspektor kontroli państwowej

Najwyższa Izba Kontroli
Delegatura w Katowicach

.....