NAJWYŻSZA IZBA KONTROLI
Delegatura w Bydgoszczy

LBY.410.12.6.2024

Mateusz Stachowiak
Burmistrz Kcyni
Urząd Miejski w Kcyni
ul. Rynek 23
89-240 Kcynia

WYSTĄPIENIE POKONTROLNE

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

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

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miejski w Kcyni[1].
Kierownik jednostki kontrolowanej	Mateusz Stachowiak – Burmistrz Kcyni[2].
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]
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[4]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Bydgoszczy
Kontroler	Leszek Murat, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LBY/87/2024 z 22 maja 2024 r.

(akta kontroli str. 1-2, 10-27)

II. Ocena ogólna[5] kontrolowanej działalności

OCENA OGÓLNA

Urząd podjął działania dla zapewnienia bezpieczeństwa informacji, w tym opracowano Politykę Bezpieczeństwa Informacji oraz powołano niezależnego Inspektora Ochrony Danych. Niemniej nie przeprowadzano w okresie objętym kontrolą testów sprawdzających odtworzenie systemu, aplikacji, bazy danych lub dokumentów z kopii, a także nie utrzymywano aktualności inwentaryzacji sprzętu służącego do przetwarzania informacji. Ponadto nie ustanowiono polityk ciągłości działania i nie opracowano planów zapewnienia ciągłości działania oraz planów odtworzeniowych.

W Urzędzie podejmowano działania w zakresie zapewnienia bezpieczeństwa informacji m.in. poprzez nadawanie uprawnień pracownikom adekwatnie do realizowanych przez nich zadań. Wprowadzono również procedury dotyczące przekazywania sprzętu komputerowego podmiotom zewnętrznym oraz zasady pracy zdalnej. Jednakże nie zapewniono odpowiednich warunków przechowywania kopii zapasowych danych oraz nie zabezpieczono informacji w sposób uniemożliwiający nieuprawnionemu ujawnienie, modyfikację, usunięcie lub zniszczenie. Nie przeprowadzano także testowego sprawdzenia odtworzenia systemu, aplikacji, bazy

[1] Dalej: „Urząd".
[2] Od 7 maja 2024 r. (dalej: „Burmistrz"). Wcześniej Burmistrzem był: Marek Szaruga (od 20 listopada 2018 r. do 19 sierpnia 2023 r.), Rafał Heftowicz (od 20 sierpnia 2023 r. do 3 października 2023 r. na podstawie upoważnień), Wojciech Niemczyk (od 4 października 2023 r. do 24 stycznia 2024 r. – wyznaczony przez Prezesa Rady Ministrów), Rafał Heftowicz (od 25 stycznia 2024 r. do 6 maja 2024 r. – wyznaczony przez Prezesa Rady Ministrów).
[3] Czynności kontrolne w jednostce zakończono 26 lipca 2024 r.
[4] Dz. U. z 2022 r. poz. 623, dalej: „ustawa o NIK".
[5] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

danych lub dokumentów z kopii. Ponadto spośród 10 pracowników Urzędu posiadających uprawnienia użytkownika, których stosunek pracy ustał, konta trzech nie zostały zablokowane.

W Urzędzie podjęto działania w celu zapobiegania incydentom bezpieczeństwa informacji, tj. zorganizowano szkolenia pracowników oraz dokonano analizy zagrożeń i ryzyka przy przetwarzaniu danych osobowych, w tym poufności, integralności i rozliczalności systemów informatycznych. Nie przeprowadzono natomiast audytu wewnętrznego z zakresu bezpieczeństwa informacji. Ponadto nie prowadzono rejestru incydentów zgodnie z przyjętą procedurą i nie dołożono wystarczającej staranności w realizacji działań naprawczych.

III. Opis ustalonego stanu faktycznego

OBSZAR

1. Organizacja bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych

Opis stanu faktycznego

1. Urząd zidentyfikował zbiory danych podlegających zabezpieczeniu (ochronie), do których włączono 63 kategorie zadań odnoszących się m.in. do: ewidencjonowania ludności, pobierania podatków i opłat lokalnych, przeprowadzania inwestycji komunalnych, udzielania zamówień publicznych, opieki i transportu dzieci i młodzieży, ewidencjonowania gruntów i budynków, rekrutacji pracowników, dokonywania spisu ludności i spisu rolnego. Urząd określił poziom ochrony danych poprzez wymagane do stosowania środki bezpieczeństwa.

(akta kontroli str. 5, 28-42)

2. Od 4 marca 2022 r. Urząd posiadał Politykę Bezpieczeństwa Informacji (dalej: „PBI", „Polityka Bezpieczeństwa"), przyjętą zarządzeniem Burmistrza[6]. Polityka Bezpieczeństwa nie została zakomunikowana trzem spośród 40 pracowników Urzędu, co zostało opisane w sekcji „stwierdzone nieprawidłowości". Właścicielem odpowiadającym za opracowanie, wdrożenie i utrzymanie PBI był Burmistrz, zaś procesy te koordynował Sekretarz Gminy.

System Zarządzania Bezpieczeństwem Informacji składał się z: a) Polityki Bezpieczeństwa i Ochrony Danych Osobowych[7], b) Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, c) Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych, d) Rejestru incydentów związanych z bezpieczeństwem informacji, e) Rejestru przeglądów PBI, f) Instrukcji BHP na stanowisku pracy z komputerem i drukarką, g) Ewidencji urządzeń wynoszonych poza siedzibę Urzędu.

(akta kontroli str. 5, 43-121, 653)

Polityka Bezpieczeństwa Informacji nie wskazywała wprost pracownika Urzędu odpowiadającego za jej ocenę, przegląd i modyfikację. Burmistrz wyjaśnił m.in., że z PBI (rozdziału XIII) wynika, że podmiotami, które dokonują oceny jest ASI i inne osoby zaangażowane w budowę i eksploatację systemu bezpieczeństwa.

[6] Zarządzenie nr P.4.2022 Burmistrza Kcyni z dnia 4 marca 2022 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Kcyni, dalej: „zarządzenie w sprawie PBI".

[7] Przyjęta zarządzeniem nr P.3.2022 Burmistrza Kcyni z dnia 4 marca 2022 r., dalej także „PBODO".

NIK zauważa, że w PBI wskazano, że dokumentacja powinna być przeglądana i weryfikowana okresowo, nie rzadziej niż raz w roku (rozdział XIII pkt 5), zaś zmiany w dokumentach może proponować ASI i inne osoby zaangażowane w budowę i eksploatację systemu bezpieczeństwa (rozdział XIII pkt 6), bez wskazania wprost, kto dokonuje przeglądu i weryfikacji.

(akta kontroli str. 43-104, 279)

3. W celu wykonania obowiązku określonego w art. 24 i 25 rozporządzenia RODO[8] w Urzędzie przyjęto Politykę Bezpieczeństwa i Ochrony Danych Osobowych, a także Instrukcję postępowania w przypadku naruszenia ochrony danych[9]. W aktach tych uregulowano m.in.: przetwarzanie danych osobowych na urządzeniach mobilnych, pseudonimizację i szyfrowanie danych, obsługę monitoringu wizyjnego, świadczenie pracy zdalnej związanej z przetwarzaniem danych osobowych, zarządzanie nośnikami informacji, zasady wynoszenia poza siedzibę Urzędu dokumentów papierowych zawierających dane osobowe, realizację praw przysługujących osobie, której dane dotyczą, przeprowadzanie audytów wewnętrznych testu bezpieczeństwa systemu przetwarzającego dane osobowe, postępowanie w przypadku naruszenia ochrony danych osobowych. W dokumentacji Urzędu nie uregulowano kwestii dotyczących: dokumentowania ograniczenia przetwarzania danych osobowych, powiadamiania o sprostowaniu lub usunięciu danych osobowych, oceny skutków dla ochrony danych osobowych.

Burmistrz wyjaśnił m.in., że Urząd uznaje konieczność dokumentowania ograniczania przetwarzania danych osobowych oraz ich sprostowania lub usunięcia, lecz do tej pory nie wystąpiły takie zdarzenia, a konieczność dokumentowania wynika wprost z przepisów RODO i nie wymaga konkretyzacji w Polityce Ochrony Danych Osobowych. Dodał, że obowiązek przeprowadzenia oceny skutków dla ochrony danych osobowych nie jest obligatoryjny dla wszystkich czynności przetwarzania.

(akta kontroli str. 5-6, 122-210, 215-216)

4. W Urzędzie prowadzone były analizy ryzyka w związku z potrzebą zachowania ciągłości działania systemów informatycznych. W sporządzonych sprawozdaniach podsumowujących wyniki oceny ryzyka (z 20 stycznia 2023 r. i 19 stycznia 2024 r.) zidentyfikowano ryzyka w odniesieniu do konkretnych zasobów, ustalono podatność, poziom ryzyka, dokonano ewaluacji oraz określono sposoby postępowania.

(akta kontroli str. 6, 211-214)

5. W Urzędzie nie ustanowiono polityk ciągłości działania i nie opracowano planów zapewnienia ciągłości działania oraz planów odtworzeniowych , co zostało opisane w sekcji „stwierdzone nieprawidłowości". Określono jednak m.in. procedurę zarządzania incydentami związanymi z bezpieczeństwem informacji, takimi jak klęski żywiołowe czy przerwy w zasilaniu, a także tworzenie kopii zapasowych danych (w tym metody i częstotliwość) i odzyskiwanie danych. Ponadto wprowadzono procedurę

[8] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.Urz.UE.L 119 z 04.05.2016, str. 1, ze zm., dalej: „RODO".

[9] Przyjęta zarządzeniem nr P.4.2019 Burmistrza Kcyni z dnia 11 marca 2019 r. w sprawie wprowadzenia Instrukcji postępowania w przypadku naruszenia ochrony danych w Urzędzie Miejskim w Kcyni.

wykonywania przeglądów i konserwacji, której celem jest zapewnienie ciągłości działania systemów informatycznych w sytuacjach awaryjnych.

(akta kontroli str. 6, 43-104, 122-194)

6. W Urzędzie nie przeprowadzano w okresie objętym kontrolą testów sprawdzających odtworzenie systemu, aplikacji, bazy danych lub dokumentów z kopii, co opisano w sekcji „stwierdzone nieprawidłowości".

(akta kontroli str. 7, 73)

7. W okresie objętym kontrolą dokonano jednego przeglądu regulacji wewnętrznych odnoszących się do bezpieczeństwa systemów informatycznych oraz ochrony danych osobowych (1 grudnia 2023 r.). W wyniku analizy dokonano m.in. zmiany dotyczącej regulowania pracy zdalnej.

(akta kontroli str. 7, 281-282)

8. W Urzędzie obowiązki dotyczące nadzoru nad bezpieczeństwem informacji nałożono na dwóch pracowników (dalej: „informatyków"). Do ich zadań należało m.in. administrowanie siecią informatyczną i bazami danych, nadzorowanie zabezpieczenia systemów informatycznych, realizowanie zadań związanych z cyberbezpieczeństwem (jeden z nich), prowadzenie ewidencji sprzętu komputerowego i oprogramowania., wykonywanie obowiązków określonych w PBI. Osoby te posiadały odpowiednie kompetencje do realizacji zadań w tym zakresie.

(akta kontroli str. 7, 283-294, 538-540)

9. W Urzędzie powołano inspektora ochrony danych (dalej także „IOD")[10], któremu przypisano obowiązki dotyczące m.in. informowania administratora systemów informatycznych[11], podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach spoczywających na nich na mocy rozporządzenia RODO oraz innych przepisów UE lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie; monitorowania przestrzegania rozporządzenia RODO, innych przepisów UE lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działań zwiększających świadomość, szkoleń personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty; udzielania na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 rozporządzenia RODO; współpracy z organem nadzorczym; pełnienia funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 rozporządzenia RODO. Osoba wyznaczona do pełnienia funkcji IOD uzyskała certyfikat ukończenia szkolenia praktycznego pełnienia funkcji Inspektora Ochrony Danych.

(akta kontroli str. 7, 295-302)

10. Pracownik wyznaczony na Inspektora Ochrony Danych wykonywał także inne zadania, lecz obowiązki te nie powodowały konfliktu interesów. W szczególności,

[10] Zarządzeniem nr P.10.2018 Burmistrza Kcyni z dnia 22 maja 2018 r. w sprawie powołania Inspektora Ochrony Danych w Urzędzie Miejskim w Kcyni.

[11] Tj. Burmistrza, dalej: „Administrator", „ASI".

zajmowane przez niego stanowiska nie wymagały udziału w określaniu celów i sposobów przetwarzania danych osobowych.

(akta kontroli str. 295-302)

12. W Urzędzie wyznaczono (od 19 października 2021 r.) osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa[12] – inspektora zatrudnionego na stanowisku pracy do spraw informatyki. Jego dane (w tym imię, nazwisko, nr telefonu, e-mail) zostały przekazane do CSIRT NASK[13] w terminie 14 dni od dnia wyznaczenia, tj. zgodnie z art. 22 ust. 1 pkt 5 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa[14].

(akta kontroli str. 368-371, 394)

13. W PBI przewidziano opracowanie i ustanowienie dokumentów wykonawczych mających na celu zapewnienie bezpieczeństwa informacji. Należało do nich: Procedura Kontroli Dostępu do Informacji, Regulamin Pracy ze Sprzętem Komputerowym, Procedura Tworzenia Kopii Zapasowych, Procedura Wykonywania Przeglądów i Konserwacji, Procedura Zarządzania Ryzykiem w Bezpieczeństwie Informacji, Procedura Zarządzania Incydentami Związanymi z Bezpieczeństwem Informacji, Ewidencja i Klasyfikacja Systemów Informatycznych, Instrukcja w Zakresie Profilaktyki Antywirusowej, Ustawienia Zabezpieczeń Systemów IT, Ochrona przed Nieautoryzowanym Dostępem do Sieci Lokalnej, Instrukcja Pracy na stanowisku. Dokumenty te zostały sporządzone.

(akta kontroli str. 44-104, 152-153, 395)

14. Oględziny oprogramowania inwentaryzującego, tj. elektronicznego rejestru zasobów teleinformatycznych (dalej: „Rejestr") oraz wybranych urządzeń elektronicznych wykazały że Rejestr m.in., zawierał informacje o nazwie urządzenia, adresie MAC, użytkowniku, zainstalowanym systemie operacyjnym i oprogramowaniu dodatkowym, stanie technicznym, numerze inwentaryzacyjnym. Spośród 12 wybranych losowo komputerów, 9 znajdowało się w Rejestrze. Zostały one przypisane do osób, które odpowiadały za dany sprzęt. Ustalenia w pozostałym zakresie opisano w sekcji „stwierdzone nieprawidłowości".

(akta kontroli str. 217-228)

15. Urząd przystąpił do programu grantowego „Cyberbezpieczny Samorząd", zawierając umowę ze Skarbem Państwa 20 czerwca 2024 r. o dofinansowanie w kwocie 546 300,00 zł[15]. W umowie przewidziano przeznaczenie otrzymanych środków m.in. na zakup: serwerów i macierzy dyskowej (wraz z ich instalacją i konfiguracją), dysków zewnętrznych do backupu, kluczy sprzętowych oraz systemu typu Xopero Unified Protection. Realizację tych zadań zaplanowano najpóźniej do 30 czerwca 2026 r. Pomiar poprawy cyberbezpieczeństwa w związku z realizacją

[12] Zarządzeniem nr P.10.2021 Burmistrza Kcyni z dnia 19 października 2021 r. w sprawie wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
[13] Computer Security Incident Response Team, Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy.
[14] Dz. U. z 2024 r., poz. 1077.
[15] Dofinansowanie ze środków UE w wysokości 442 503,00 zł i z budżetu państwa w wysokości 103 797,00 zł.

Programu przewidziano jako porównanie planowanych zakresów zmian do stanu zrealizowanego, zgodnie z układem tzw. Ankiety dojrzałości.

(akta kontroli str. 229-265, 278, 605, 632-644)

Stwierdzone nieprawidłowości

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

1. Polityka Bezpieczeństwa Informacji nie została zakomunikowana trzem pracownikom Urzędu - nie potwierdzili oni faktu zapoznania się i przyjęcia do stosowania PBI w sposób zgodny z załącznikiem nr 2 do zarządzenia w sprawie PBI, tj. poprzez podpisanie przez nich oświadczenia.

   (akta kontroli str. 104-106, 120-121, 279)

   Burmistrz wyjaśnił m.in., że niezakomunikowanie pracownikom Urzędu PBI wynikało z przeoczenia.

   (akta kontroli str. 278-279)

2. W Urzędzie nie przeprowadzano (w okresie objętym kontrolą) testów sprawdzających odtworzenie systemu, aplikacji, bazy danych lub dokumentów z kopii. Stanowiło to naruszenie § 1 pkt 8 Procedury Tworzenia Kopii Zapasowych PBI, w którym określono obowiązek przeprowadzenia udokumentowanego sprawdzenia testowego co najmniej dwa razy w roku.

   (akta kontroli str. 7, 73, 279)

   Burmistrz wyjaśnił m.in., że nie przeprowadzono ww. testów z powodu realizacji projektu Cyfrowa Gmina, które znacząco wpłynęło na kształt systemu informatycznego. Prowadzone były procesy wdrożeniowe i konfiguracyjne. W 2024 r. planowane są testy sprawdzające i odtworzeniowe.

   (akta kontroli str. 279)

   NIK zwraca uwagę, że istotne jest cykliczne testowanie sprawdzające możliwości odtworzenia systemów/aplikacji w celu potwierdzenia prawidłowości przyjętych rozwiązań zapewniających bezpieczeństwo informacji.

3. Urząd nie utrzymywał w aktualności inwentaryzacji sprzętu służącego do przetwarzania informacji, tj. nie przestrzegał obowiązku określonego w §19 ust. 2 pkt 2 rozporządzenia KRI[16] i w 20 ust. 2 pkt 2 nieobowiązującego rozporządzenia KRI. Prowadzony Rejestr nie zawierał następujących urządzeń: dwóch komputerów stacjonarnych, jednego laptopa, drukarki, serwera oraz routera.

   (akta kontroli str. 217-228)

   Burmistrz wyjaśnił m.in., że inwentaryzacja sprzętu skupiała się na komputerach i laptopach. Brak utrzymania aktualności inwentaryzacji był spowodowany m.in. natłokiem innych zajęć. Po zakończeniu czynności kontrolnych dokonano

[16] Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2024 r. poz. 773), dalej: „rozporządzenie KRI" Do wejścia w życie ww. rozporządzenia (tj. 23 maja 2024 r.) obowiązek ten w tożsamym brzmieniu był ujęty w § 20 ust. 2 pkt 2 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 „nieobowiązujące rozporządzenie KRI".

zinwentaryzowania pozostałych komputerów, laptopów, drukarek, serwerów i routerów.

(akta kontroli str. 279, 650)

4. Urzędzie nie ustanowiono polityk ciągłości działania i nie opracowano planów ciągłości działania oraz planów odtworzeniowych, co było nierzetelnym zapewnieniem warunków umożliwiających odtworzenie działalności po katastrofie lub innym incydencie zakłócającym działanie. Funkcjonowały jedynie rozwiązania dotyczące m.in. systemu backupowego, tworzenia kopii zapasowych, opracowanych scenariuszy odtwarzania. Nie określono w nich jednak:

   a) akceptowalnego czasu przywrócenia ciągłości funkcjonowania systemów informatycznych.

   Burmistrz wyjaśnił m.in., że nie określono akceptowalnego czasu przywrócenia ciągłości funkcjonowania systemów informatycznych, gdyż co do zasady ma to nastąpić niezwłocznie, tzn. możliwie najkrótszym czasie. Trudno przyjąć sztywne ramy czasowe przywrócenia ciągłości ze względu na różnorodność możliwych do wystąpienia zdarzeń.

   b) nie zaplanowano postępowania na wypadek incydentów odnoszących się do topologii sieci, klastrów i macierzy dyskowych, systemowych serwerów wirtualnych i urządzeń brzegowych.

   Burmistrz wyjaśnił m.in., że Urząd posiada plany na wypadek sytuacji awaryjnych, jednak nie jest w stanie przewidzieć wszystkich możliwych incydentów.

(akta kontroli str. 6-7, 43-104, 122-194, 277-278)

OCENA CZĄSTKOWA

W Urzędzie ustanowiono System Zarządzania Bezpieczeństwem Informacji, w tym opracowano i przyjęto do stosowania Politykę Bezpieczeństwa Informacji oraz powołano niezależnego Inspektora Ochrony Danych. Niemniej nie przeprowadzano w okresie objętym kontrolą testów sprawdzających odtworzenie systemu, aplikacji, bazy danych lub dokumentów z kopii, a także nie utrzymywano w aktualności inwentaryzacji sprzętu służącego do przetwarzania informacji. Ponadto nie ustanowiono polityk ciągłości działania i nie opracowano planów zapewnienia ciągłości działania oraz planów odtworzeniowych.

OBSZAR

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

Opis stanu faktycznego

1. Urząd zabezpieczył komputery stacjonarne i laptopy będące w jego zasobach przed możliwością zainstalowania nieautoryzowanego oprogramowania. Oględziny 10 urządzeń wykazały, że zalogowani na nich pracownicy nie mogli zainstalować pliku wymagającego uprawnień administratora systemu. Przy próbie instalacji każdorazowo pojawiał się komunikat o konieczności podania loginu i hasła administratora. Brak zabezpieczenia smartfonów opisano w sekcji „stwierdzone nieprawidłowości”.

(akta kontroli str. 303)

2. Badanie dotyczące 15 pracowników Urzędu (w tym pięciu zajmujących stanowiska kierownicze)[17] wykazało, że przyznane im uprawnienia do przetwarzania informacji są zgodne z czynnościami zapisanymi w zakresach obowiązków. Było to zgodne z rozdziałem X pkt 6a PBI.

(akta kontroli str. 54, 541-587)

Dla osób nowozatrudnionych w Urzędzie złożono wnioski o nadanie uprawnień do danego systemu informatycznego zgodnie z PBI.

(akta kontroli str. 59, 617-631)

3. Spośród 10 pracowników Urzędu, których stosunek pracy ustał w okresie od 1 stycznia 2023 r.,[18] w sześciu przypadkach ich konta zostały zablokowane. Ustalenia w odniesieniu do pozostałych pracowników opisano w sekcji „stwierdzone nieprawidłowości".

(akta kontroli str. 177, 266-267)

4. W celu zapewnienia ochrony przetwarzanych informacji przed nieuprawnionym dostępem, w PBODO (§ 9) zobowiązano każdego użytkownika do stosowania hasła o minimalnej długości ośmiu znaków, zawierającego kombinację małych i dużych liter oraz cyfr lub znaków specjalnych, stosowania haseł nieposiadających w swej strukturze części loginu oraz zbliżonych do poprzednich, a także zmieniania haseł nie rzadziej niż raz na 30 dni. W wyniku oględzin trzech systemów informatycznych zarządzanych przez Urząd stwierdzono, że hasła dostępu pracowników składały się z minimum ośmiu znaków (od ośmiu do 11), zaś złożoność haseł była zapewniona odpowiednią formułą oprogramowania, za wyjątkiem sytuacji opisanych w sekcji „stwierdzone nieprawidłowości".

(akta kontroli str. 143, 179, 268-271)

Systemy VULCAN i RESPONS pozwalały użytkownikom na stosowanie hasła wykorzystującego część loginu oraz na zmianę hasła na podobne do wcześniej wykorzystywanego, co było niezgodne z § 9 ust.1 pkt 6 i 7 PBODO. Programy te nie posiadały technicznej możliwości ustanowienia ww. wymogów systemowych dla haseł.

(akta kontroli str. 179, 272-273, 645-648)

Burmistrz wyjaśnił m.in., że systemy VULCAN i RESPONS są oprogramowaniem zewnętrznym i Urząd ma bardzo ograniczony wpływ na ich funkcjonalności. Możliwości, jakie istnieją w kwestii wymogów dotyczących haseł, to określenie minimalnej długości, częstotliwość zmiany hasła oraz ilości małych i dużych liter w haśle. Ponadto możliwości techniczne konfiguracji haseł w poszczególnych systemach informatycznych nie wykluczają obowiązków wynikających w przyjętych polityk.

(akta kontroli str. 395)

5. Oględziny pięciu stanowisk pracy pracowników realizujących zadania w miejscach, gdzie dostęp mają klienci Urzędu wykazały, że usytuowanie monitorów

[17] W okresie objętym kontrolą nie było przypadków zmiany stanowiska pracy i przejścia do innej komórki organizacyjnej Urzędu.
[18] Do 31 maja 2024 r.

gwarantowało, że dane wyświetlane na ekranach nie są widoczne dla osób nieuprawnionych. Było to zgodne z załącznikiem nr 11 do PBI (Instrukcją Pracy na Stanowisku Wyposażonym w Monitor i Drukarkę).

(akta kontroli str. 102, 268)

6. W Urzędzie ustanowiono (od 1 czerwca 2023 r.) zasady pracy zdalnej[19], zgodnie z którymi zobowiązano pracowników do zapewnienia bezpiecznych warunków technicznych oraz lokalowych pracy zdalnej, ochrony informacji prawnie chronionych m.in. poprzez oddzielenie sfery prywatnej od zawodowej (np. zabezpieczenie przetwarzanych danych), niekorzystania z otwartych sieci WiFi i regularnego aktualizowania oprogramowania urządzenia sieciowego. Pracownicy Urzędu zostali poinformowani o treści procedury pracy zdalnej i zobowiązani do jej stosowania. Było to zgodne z § 6 załącznika do PBODO[20].

(akta kontroli str. 194-199)

7. Dane zgromadzone na dyskach twardych laptopów były szyfrowane za pomocą specjalistycznego oprogramowania. Było to zgodne z Procedurą Wykonywania Przeglądów i Konserwacji PBI.

(akta kontroli str. 8, 78, 390)

8. W Urzędzie stosowano zabezpieczenia fizyczne dostępu do serwerowni w celu uniemożliwienia osobom nieuprawnionym ujawnienie, usunięcie lub zniszczenie danych tam zgromadzonych. Było to zgodne z Procedurą Tworzenia Kopii Zapasowych PBI. Oględziny dokonane w czasie przerwy w dostawie prądu do budynku Urzędu wykazały, że serwer główny był podtrzymywany przez zapasowe urządzenia zasilające.

(akta kontroli str. 274-276, 390)

9. W okresie objętym kontrolą zawarto trzy umowy z podmiotami zewnętrznymi w sprawie serwisowania oprogramowania[21] oraz jedną umowę na dostawę sprzętu informatycznego i oprogramowania[22]. W umowach w sprawie serwisowania oprogramowania zawarto klauzule zobowiązujące wykonawców do zachowania tajemnicy informacji. Było to zgodne z § 20 ust. 2 pkt 10 nieobowiązującego rozporządzenia KRI. Natomiast w umowie dotyczącej dostawy sprzętu brak było odpowiednich zapisów w tym zakresie, co opisano w sekcji „stwierdzone nieprawidłowości".

(akta kontroli str. 8, 372-383, 394, 404-486)

10. W Urzędzie określono zasady przekazywania sprzętu elektronicznego podmiotom zewnętrznym w celu wykonania napraw. Zgodnie z Procedurą Wykonywania Przeglądów i Konserwacji PBI konserwacja i naprawy sprzętu, na którym przetwarzane są dane osobowe, odbywa się po uprzednim zawarciu umowy powierzenia. Przed przekazaniem uszkodzonego sprzętu komputerowego z danymi

[19] Zarządzenie Nr P.16.2023 Burmistrza Kcyni z dnia 1 czerwca 2023 r. w sprawie wprowadzenia zmian w Polityce Bezpieczeństwa Ochrony Danych Osobowych w Urzędzie Miejskim w Kcyni.

[20] Załącznik do zarządzenia Nr P.16.2023 r. Burmistrza Kcyni z dnia 1 czerwca 2023 r. w sprawie wprowadzenia zmian w Polityce Bezpieczeństwa Ochrony Danych Osobowych w Urzędzie Miejskim w Kcyni.

[21] Umowa nr 23/0655/JU zawarta 26 stycznia 2024 r., umowa nr 218/OI/2023 z 13 stycznia 2023 r., umowa nr 218/OI/2024 z 7 grudnia 2023 r.

[22] Umowa nr RI.272.1/762780/2023 z 21 czerwca 2023 r.

osobowymi do naprawy poza obszar przetwarzania wymagane jest wymontowanie nośnika z danymi osobowymi, trwałe usunięcie danych osobowych z użyciem specjalistycznego oprogramowania lub nadzorowanie naprawy przez osobę upoważnioną przez ASI, gdy nie ma możliwości usunięcia danych z nośnika.

W okresie objętym kontrolą nie przekazywano sprzętu elektronicznego podmiotom zewnętrznym w celu wykonania napraw.

(akta kontroli str. 75-77, 588)

11. W Urzędzie wprowadzono Procedurę Tworzenia Kopii Zapasowych[23] i określono w niej m.in.: a) długość przechowywania kopii zapasowych (kopie miesięczne przez sześć miesięcy, zaś kopie roczne przez pięć lat); b) rodzaje wykonywanych kopii (kopie bezpieczeństwa i kopie archiwalne); c) obowiązek generowania raportu z wykonania kopii; d) sposób i miejsce przechowywania kopii e) zasady odzyskiwania kopii. Dostęp do kopii zapasowych został ograniczony do Burmistrza i Sekretarza Gminy poprzez nadanie wyłącznie tym osobom uprawnień do pobierania kluczy do szafy, w której zdeponowane są kopie zapasowe.

(akta kontroli str. 73-74, 394)

12. Procedura Tworzenia Kopii Zapasowych określała częstotliwość tworzenia kopii: w odniesieniu do kopii archiwalnych miesięcznie (na koniec każdego miesiąca) i rocznie (na koniec danego roku); w odniesieniu do kopii bezpieczeństwa – m.in. przed dokonaniem zmian w konfiguracji systemów operacyjnych lub oprogramowania.

W wyniku przeprowadzonych oględzin ustalono, że przeprowadzano miesięczne i roczne zapisywanie kopii archiwalnych wybranego systemu informatycznego (RESPONS). Dostęp do pomieszczeń był rejestrowany, zaś kopie archiwalne przechowywano w szafie blaszanej zabezpieczonej zamkiem. Dokonano testowego odzyskania danych z kopii zapasowej z programu RESPONS z kwietnia 2024 r., odzyskane dane pozwoliły na obsługę przez pracowników Urzędu.

(akta kontroli str. 73-74, 274-275, 305-363, 390)

13. W Urzędzie monitorowano pojemność pamięci masowych dysków twardych wykorzystywanych w serwerach. Oględziny trzech serwerów (domenowego, QNAP i RESPONS) wykazały, że ich pojemność była wykorzystana w od 33% do 70%.

(akta kontroli str. 364-367)

14. W Urzędzie nie zidentyfikowano w sposób formalny kluczowych elementów infrastruktury informatycznej oraz usług informatycznych. Nie określono również czasu przywracania do funkcjonalności poszczególnych systemów oraz procesów działania, co opisano w sekcji „stwierdzone nieprawidłowości".

(akta kontroli str. 44-103, 589)

Stwierdzone nieprawidłowości

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

1. Spośród 10 pracowników Urzędu posiadających uprawnienia użytkownika, których stosunek pracy ustał w okresie od 1 stycznia 2023 r.[24]:

[23] Załącznik nr 3 do PBI.
[24] Do 31 maja 2024 r.

a) konta trzech nie zostały zablokowane, co stanowiło naruszenie § 19 ust. 2 pkt 5 rozporządzenia KRI[25] i § 20 ust. 2 pkt 5 nieobowiązującego rozporządzenia KRI oraz § 5 ust. 2 pkt 1 PBODO – Polityki Bezpieczeństwa Systemu Informatycznego;

b) w odniesieniu do jednego byłego pracownika Urząd nie posiadał informacji co do usunięcia bądź zablokowania konta użytkownika;

c) w odniesieniu do trzech innych pracowników ich bezpośredni przełożeni nie złożyli wniosku o odebranie uprawnień do systemu informatycznego, pomimo takiego obowiązku wynikającego z § 5 ust. 1 PBODO – Polityki Bezpieczeństwa Systemu Informatycznego.

d) w trzech przepadkach Urząd nie posiadał wiedzy, kiedy zablokowano pracownikom dostęp do systemu informatycznego.

(akta kontroli str. 60, 177, 266-267, 280, 657)

Burmistrz wyjaśnił m.in., że brak usunięcia kont wynikał z przeoczenia lub z braku złożenia przez kierownika odpowiedniej komórki organizacyjnej wniosku o odebranie uprawnień z powodu niedopatrzenia.

(akta kontroli str. 279)

2. Urząd nie zapewnił odpowiednich warunków egzekwowania od pracowników Urzędu ochrony przetwarzania danych (zabezpieczenia komputerów), ponieważ:

a) system ADA[26] pozwalał na wprowadzenie nowego hasła składającego się z mniej niż 8 znaków, bez wielkich liter, bez cyfr i znaków specjalnych. Ponadto system pozwalał na stosowanie hasła wykorzystującego część loginu oraz na zmianę hasła na podobne i nie wylogowywał w przypadku wprowadzenia błędnego hasła (więcej niż trzy razy), co było niezgodne z § 9 ust. 1 pkt 5, 6, 7 oraz ust. 5 PBODO.

(akta kontroli str. 179, 272-273, 654)

Burmistrz wyjaśnił m.in., że taka była funkcjonalność programu uznana wówczas za wystarczającą. W lipcu 2024 r. dokonano zmiany w oprogramowaniu i obecnie system blokuje hasła, które nie mają długości 8 znaków i nie zawierają wielkich liter, bez cyfr i znaków specjalnych. Co do pozostałych wymogów, to Urząd podejmie prace nad uruchomieniem odpowiednich blokad, jeżeli będzie to technicznie możliwe.

(akta kontroli str. 395, 650-651)

b) system zabezpieczający dostęp do komputerów (ACTIVE DIRECTORY) pozwalał na zmianę hasła na podobne i nie wylogowywał użytkownika w przypadku wprowadzenia błędnego hasła (ponad trzy razy), a ponadto pozwalał na logowanie się na więcej niż jednym komputerze jednocześnie, wykorzystując ten sam identyfikator, co było niezgodne z § 9 ust.1 pkt 7 oraz ust. 5 i 6 PBODO.

(akta kontroli str. 179, 272-273)

Burmistrz wyjaśnił m.in., że system zarządzania środowiskiem domenowym nie blokował użytkownika, pozwalał na zmianę hasła na podobne oraz na logowanie się

[25] Tj. dokonywanie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji.
[26] Oprogramowanie do obsługi nieruchomości.

na więcej niż jednym komputerze, gdyż zostało to przeoczone i zostanie niezwłocznie wprowadzone.

(akta kontroli str. 396)

3. Urząd nie zapewnił odpowiedniego zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie, tj. obowiązku określonego w §19 ust. 2 pkt 9 rozporządzenia KRI: w serwerowni przechowywano materiały łatwopalne (tekturowe pudła) oraz nie rejestrowano długości przebywania w pomieszczeniu osób.

(akta kontroli str. 274-276)

Burmistrz wyjaśnił m.in., że w serwerowni przechowywane były kartony od sprzętu informatycznego na wypadek konieczności skorzystania z gwarancji w sytuacji wystąpienia awarii. W dniu 26 czerwca 2024 r. usunięto tekturowe pudła z serwerowni. Długość przebywania w serwerowni nie podlegała monitorowaniu, gdyż uznano to za niekonieczne ze względu na stosowane zabezpieczenia.

(akta kontroli str. 396)

4. Wykorzystywane w Urzędzie smartfony (łącznie 21 sztuk) nie zostały zabezpieczone przed instalacją przez użytkownika dowolnego oprogramowania, co stanowiło nierzetelne wypełnienie obowiązku zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie (§19 ust. 2 pkt 9 rozporządzenia KRI oraz § 20 ust. 2 pkt 9 nieobowiązującego rozporządzenia KRI).

(akta kontroli str. 303-304)

Burmistrz wyjaśnił m.in., że smartfony nie zostały zabezpieczone przed instalacją dowolnego oprogramowania, ponieważ nadano priorytet dla zabezpieczenia komputerów i laptopów jako najintensywniej wykorzystywanych urządzeń. W smartfonach dane wykorzystywane są sporadycznie i zostaną objęte większym zabezpieczeniem w najbliższym czasie.

(akta kontroli str. 396)

5. Urząd nie zabezpieczył odpowiednich warunków przechowywania kopii zapasowych danych, ponieważ:

a) kopie bezpieczeństwa były przechowywane w serwerowni, tzn. w tym samym pomieszczeniu, gdzie znajdował się serwer główny (a ponadto nie zabezpieczono ich np. poprzez umieszczenie w odrębnej szafie ochronnej), co stanowiło naruszenie § 19 ust. 2 pkt 9 rozporządzenia KRI i § 20 ust. 2 pkt 9 nieobowiązującego rozporządzenia KRI oraz § 1 pkt 6 i 7 Procedury Tworzenia Kopii Zapasowych PBI.

(akta kontroli str. 73-74, 305, 390)

Burmistrz wyjaśnił m.in., że zasoby lokalowe są ograniczone i nie ma możliwości technicznych wygospodarowania dodatkowego pomieszczenia w budynku Urzędu, które swoimi standardami mogłoby być porównywalne z obecną serwerownią i gwarantować odpowiedni poziom bezpieczeństwa kopiom bezpieczeństwa. Kopii bezpieczeństwa nie umieszczono w obudowie (np. w szafie), ponieważ uznano stosowane zabezpieczenia za wystarczające.

(akta kontroli str. 396)

b) miejsca przechowywania kopii archiwalnych i bezpieczeństwa nie zostały zabezpieczone przed skutkami takich zdarzeń jak: oddziaływanie silnego pola elektromagnetycznego i promieniowania, co stanowiło naruszenie § 19 ust. 2 pkt 9 rozporządzenia KRI i § 20 ust. 2 pkt 9 nieobowiązującego rozporządzenia KRI oraz § 1 pkt 6 Procedury Tworzenia Kopii Zapasowych PBI.

(akta kontroli str. 73-74, 305, 390)

Burmistrz wyjaśnił m.in., że wymóg ww. zabezpieczenia został wprowadzony w PBI. Analiza stanu faktycznego dokonywana na bieżąco i nieformalnie przez Administratora co do gromadzonych danych wskazała, że tego rodzaju zabezpieczenia powinny być stosowane do kategorii danych o charakterze danych krytycznych, a Administrator nie jest w posiadaniu takich danych. W związku z tym przepisy PBI zostaną doprecyzowane.

(akta kontroli str. 396, 650-651)

6. W Urzędzie (w okresie objętym kontrolą) nie przeprowadzano testowego sprawdzenia odtworzenia systemu, aplikacji, bazy danych lub dokumentów z kopii, pomimo takiego obowiązku (co najmniej dwa razy w roku) określonego w § 1 pkt 8 Procedury Tworzenia Kopii Zapasowych PBI.

(akta kontroli str. 73, 397)

Burmistrz wyjaśnił m.in., że w przeważającej mierze wynikało to ze znaczącego przebudowywania sytemu informatycznego w Urzędzie związanego z realizacją przedsięwzięcia w ramach programu Cyfrowa Gmina i zaangażowania pracowników w ten proces. W roku 2024 testowe odtworzenia zostaną przeprowadzone.

(akta kontroli str. 397)

7. W jednej z trzech objętych analizą umów (na dostawę sprzętu informatycznego i oprogramowania)[27] nie zamieszczono klauzuli zobowiązującej wykonawcę do zachowania tajemnicy informacji, co stanowi naruszenie § 20 ust. 2 pkt 10 nieobowiązującego rozporządzenia KRI zobowiązującego do zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

(akta kontroli str. 404-486)

Burmistrz wyjaśnił m.in., że dostawa sprzętu dotyczyła nowych fabrycznie urządzeń, na których nie było zapisanych żadnych informacji wytworzonych w Urzędzie Miejskim w Kcyni. W związku z tym nie było konieczności zwierania klauzul zobowiązujących wykonawcę do zachowania tajemnicy informacji. Niemniej w przypadku konieczności naprawy sprzętu w siedzibie Administratora lub poza nią obowiązują procedury opisane w PBI. Dostawca sprzętu nie miał dostępu do danych osobowych – podlegały one podwójnej ochronie poprzez: a) usunięcie danych przez ASI; lub b) zawarcie umowy powierzenia przetwarzania danych zabezpieczającej ochronę danych osobowych.

[27] Umowa nr RI.272.1/762780/2023 z 21 czerwca 2023 r.

(akta kontroli str. 588)

NIK zwraca uwagę, że zawarta umowa dotyczy również zapewnienia serwisu technicznego, zaś § 20 ust. 2 pkt 10 nieobowiązującego rozporządzenia KRI bezwzględnie wymagał wprowadzenia w umowach serwisowych zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

(akta kontroli str. 409)

8. W Urzędzie nie dokonano klasyfikacji systemów informacyjnych według rangi/znaczenia, co stanowiło obowiązek określony w sekcji I.6 Ewidencji i Klasyfikacji Systemów Informatycznych PBI[28]. Ponadto nie zidentyfikowano w sposób formalny kluczowych elementów infrastruktury informatycznej oraz usług informatycznych i nie określono również czasu przywracania do funkcjonalności poszczególnych systemów oraz procesów działania.

(akta kontroli str. 44-103, 589)

Burmistrz wyjaśnił m.in., że nie dokonywano klasyfikacji systemów informacyjnych według ich rangi/znaczenia, ponieważ Administrator przykłada identyczną wagę do wszystkich elementów systemu. W przyszłości zostanie przeprowadzona taka analiza. Kluczowe elementy infrastruktury informatycznej oraz usług informatycznych nie zostały zawarte/spisane w istniejącej dokumentacji, co nie oznacza, że Administrator nie ma wiedzy, które elementy infrastruktury mają krytyczne znaczenie. Całość systemu informatycznego, a przynajmniej jego najważniejsze elementy, opierają się na urządzeniach zamontowanych w serwerowni. Pomieszczenie to podlega szczególnym restrykcjom i procedurom. Dla Administratora oraz służb informatycznych Urzędu oczywiste jest, że właśnie serwerownia stanowi fundament całego systemu informatycznego Urzędu. Wymaga ona szczególnego nadzoru oraz utrzymania funkcjonalności i bezpieczeństwa, co wynika w dużej mierze ze specyfiki dotyczącej konfiguracji systemu jako całości. W Urzędzie obowiązuje zasada, że przywrócenie systemów i procesów ma nastąpić niezwłocznie, co należy rozumieć jako najkrótszy, możliwy przedział czasu. Liczba możliwych do wystąpienia sytuacji/awarii jest w zasadzie nieograniczona. Niemniej w każdym przypadku ma to być najkrótszy możliwy czas.

(akta kontroli str. 589)

OCENA CZĄSTKOWA

W Urzędzie, w okresie objętym kontrolą, podejmowano działania w zakresie zapewnienia bezpieczeństwa informacji m.in. poprzez nadawanie uprawnień pracownikom adekwatnie do realizowanych przez nich zadań. Wprowadzono również procedury dotyczące przekazywania sprzętu komputerowego podmiotom zewnętrznym oraz zasady pracy zdalnej. Stwierdzone w tym obszarze nieprawidłowości dotyczyły m.in.: niezapewnienia odpowiednich warunków przechowywania kopii zapasowych danych, egzekwowania od pracowników Urzędu ochrony przetwarzania danych, oraz niezabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu ujawnienie, modyfikację, usunięcie lub zniszczenie. Nie przeprowadzano także testowego sprawdzenia odtworzenia systemu, aplikacji, bazy danych lub dokumentów z kopii. Ponadto spośród 10

[28] Str. 51.

pracowników Urzędu posiadających uprawnienia użytkownika, których stosunek pracy ustał, konta trzech nie zostały zablokowane.

OBSZAR

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

1. W Urzędzie przeprowadzono 11 maja 2023 r. analizę zagrożeń i ryzyka przy przetwarzaniu danych osobowych, w tym poufności, integralności i rozliczalności systemów informatycznych pod kątem zagrożeń i ryzyka.

W analizie dokonano m.in. przeglądu wymogów ogólnych dotyczących bezpieczeństwa informacji, wyróżniono zagrożenia ze względu na utratę poufności, integralności i rozliczalności systemu informatycznego. Dokonano szacowania ryzyka i stwierdzono niski poziom ryzyka ogólnego, równoznaczny z niskim poziomem ryzyka utraty bezpieczeństwa danych osobowych. Administrator wskazał na działania naprawcze: 1) wzmocnienie zabezpieczeń urządzeń, 2) rygorystyczne przestrzeganie zmiany haseł, 3) weryfikacja cykliczna zakresu przyznawanych upoważnień.

(akta kontroli str. 514-535)

2. W okresie objętym kontrolą doszło do 37 incydentów naruszenia bezpieczeństwa informacji, w tym: 15 przypadków nieprawidłowego zabezpieczenia miejsc przechowywania danych (otwarte szafy, regały, biurka), pięciu przypadków nieprawidłowego zaadresowania korespondencji elektronicznej, ośmiu przypadków zablokowania użytkownika w systemie informatycznym, siedmiu awarii zasilania i dwóch uszkodzenia informacji.

(akta kontroli str. 536-537)

Zgodnie z Procedurą Zarządzania Incydentami Związanymi z Bezpieczeństwem Informacji PBI pracownicy Urzędu mają obowiązek zgłaszać zauważone przez siebie incydenty, zaś po ich dokładnym rozpoznaniu dane o incydencie powinny być wprowadzone do rejestru incydentów. Z Procedurą nie zostało zapoznanych trzech spośród 40 pracowników Urzędu, co opisano w sekcji „stwierdzone nieprawidłowości".

(akta kontroli str. 89-93, 105-119)

3. W okresie objętym kontrolą zorganizowano w Urzędzie dwa szkolenia z zakresu bezpieczeństwa informacji w następstwie przeprowadzonej kontroli ujawniającej nieprawidłowości w zapewnieniu bezpieczeństwa informacji. Szkolenia dotyczyły zagadnień będących przedmiotem kontroli tj. m.in. polityki czystego biurka, zasad zabezpieczania dostępu do pomieszczeń – polityki kluczy, polityki zarządzania nośnikami informacji, polityki niszczenia dokumentów w formie papierowej, polityki haseł. Szkolenia odbyły się w każdym z referatów Urzędu.

(akta kontroli str. 589-602)

Burmistrz wyjaśnił m.in., że Urząd nie sporządzał listy obecności pracowników obecnych na ww. szkoleniach, stąd nie jest w stanie ustalić, ilu pracowników wzięło w nich udział. Brak prowadzenia sprawozdawczości wynikał z uznania tego wówczas za niekonieczne. Niemniej można stwierdzić, że w szkoleniach wzięli udział prawie wszyscy pracownicy Urzędu.

(akta kontroli str. 650)

4. W okresie objętym kontrolą nie przeprowadzono w Urzędzie audytu wewnętrznego z zakresu bezpieczeństwa informacji, co opisano w sekcji „stwierdzone nieprawidłowości".

(akta kontroli str. 9)

W okresie objętym kontrolą nie wpłynęły do Urzędu skargi i wnioski dotyczące bezpieczeństwa informacji.

(akta kontroli str. 589)

Stwierdzone nieprawidłowości

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

1. W okresie objętym kontrolą nie przeprowadzono w Urzędzie audytu wewnętrznego z zakresu bezpieczeństwa informacji, co stanowiło naruszenie § 19 ust. 2 pkt 14 rozporządzenia KRI oraz § 20 ust. 2 pkt 14 nieobowiązującego rozporządzenia KRI.

(akta kontroli str. 9)

Burmistrz wyjaśnił m.in., że audytu nie przeprowadzono ze względów organizacyjnych i decyzyjnych wywołanych wygaśnięciem w sierpniu 2023 r. mandatu Burmistrza i długim okresem oczekiwania na wyznaczenie osoby pełniącej tą funkcję.

(akta kontroli str. 589)

2. Spośród 37 incydentów naruszenia bezpieczeństwa informacji, jakie wydarzyły się w okresie objętym kontrolą, żaden nie został wprowadzony do rejestru incydentów oraz nie zabezpieczono materiału dowodowego (za wyjątkiem protokołu z kontroli przeprowadzonej w dniu 18 stycznia 2023 r.)[29], co stanowiło naruszenie rozdziału VII pkt 3 i 5 Procedury Zarządzania Incydentami Związanymi z Bezpieczeństwem Informacji PBI.

(akta kontroli str. 92-93, 536, 590-596)

Burmistrz wyjaśnił m.in., incydenty te ze względu na ich charakter, wagę, wpływ na systemy informatyczne uznano za mało znaczące. W przyszłości rozważona zostanie możliwość wprowadzenia zmian do PBI uwzględniających wprowadzenie do rejestru incydentów, których wystąpienie może mieć istotny wpływ na bezpieczeństwo informacji. Kwalifikowanie (jak obecnie) każdego zdarzenia jako incydentu może prowadzić do nadmiernej biurokracji. W niektórych przypadkach usunięcie zdarzeń może zajmować o wiele mniej czasu niż zgromadzenie dokumentacji.

(akta kontroli str. 590)

3. W Urzędzie nie dołożono wystarczającej staranności w realizacji działań naprawczych sformułowanych w przeprowadzonej 11 maja 2023 r. analizie zagrożeń i ryzyka przy przetwarzaniu danych osobowych. We wnioskach wskazano na działania naprawcze: a) wzmocnienie zabezpieczeń urządzeń, b) rygorystyczne przestrzeganie zmiany haseł, c) weryfikacja cykliczna zakresu przyznawanych upoważnień. Działań w zakresie pierwszych dwóch punktów nie podjęto, zaś w przypadku ostatniego nie udokumentowano, co było niezgodne z Procedurą Kontroli Dostępu do Informacji PBI (sekcja XII pkt 5).

[29] Dotyczącej dostępu do pomieszczeń, polityki czystego biurka, ustawienia monitora, zabezpieczenia komputerów hasłem, dostępu do szafek i pieczęci.

(akta kontroli str. 65, 530, 589)

Burmistrz wyjaśnił m.in., że: ad a) planuje się wdrożenie do końca 2025 r. uwierzytelniania dwuskładnikowego (klucze sprzętowe), które ma zostać zrealizowane w ramach projektu pn. „Zwiększenie poziomu cyberbezpieczeństwa w Urzędzie Miejskim w Kcyni", ad b) uznano za wystarczające dotychczasowe ustawienia systemowe wymuszające zmianę hasła co określoną liczbę dni. Nie jest możliwe w obecnym stanie technicznym dokonywanie innych działań, ad c) weryfikacja prowadzona jest przez Sekretarza Gminy, Inspektora Ochrony Danych, ASI. Z czynności nie sporządzono notatek służbowych.

(akta kontroli str. 589-590)

OCENA CZĄSTKOWA

W Urzędzie, w okresie objętym kontrolą, podjęto działania w celu zapobiegania incydentom bezpieczeństwa informacji, tj. zorganizowano szkolenia pracowników oraz dokonano analizy zagrożeń i ryzyka przy przetwarzaniu danych osobowych, w tym poufności, integralności i rozliczalności systemów informatycznych pod kątem zagrożeń i ryzyka. Nie przeprowadzono natomiast audytu wewnętrznego z zakresu bezpieczeństwa informacji. Ponadto nie prowadzono rejestru incydentów zgodnie z przyjętą procedurą i nie dołożono wystarczającej staranności w realizacji działań naprawczych.

IV. Uwagi i wnioski

W związku ze stwierdzonymi nieprawidłowościami, Najwyższa Izba Kontroli na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, przedstawia następujące uwagi i wnioski:

Uwagi

Najwyższa Izba Kontroli nie formułuje uwag.

Wnioski

1. Zapoznanie z treścią PBI wszystkich pracowników Urzędu i określenie podmiotu odpowiadającego za jej ocenę, przegląd i modyfikację.
2. Przeprowadzanie testów sprawdzających odtworzenie systemu, aplikacji, bazy danych lub dokumentów z kopii.
3. Utrzymywanie aktualności inwentaryzacji sprzętu służącego do przetwarzania informacji.
4. Niezwłoczne blokowanie kont użytkowników systemu (pracowników), którzy zakończyli pracę w Urzędzie.
5. Zabezpieczenie wykorzystywanych w Urzędzie smartfonów przed instalacją nieautoryzowanego oprogramowania bez nadzoru służb informatycznych Urzędu.
6. Zabezpieczenie odpowiednich warunków przechowywania kopii zapasowych danych.
7. Zamieszczanie w umowach dotyczących serwisu technicznego urządzeń informatycznych zapisów gwarantujących odpowiedni pozom bezpieczeństwa informacji.
8. Dokonywanie klasyfikacji systemów informacyjnych według rangi/znaczenia i określenie czasu przywracania do funkcjonalności poszczególnych systemów oraz procesów.
9. Przeprowadzanie audytu wewnętrznego z zakresu bezpieczeństwa informacji.

10. Wprowadzanie do rejestru incydentów oraz zabezpieczanie materiału dowodowego z ich przebiegu.
11. Podejmowanie działań naprawczych opisanych w analizie zagrożeń i ryzyka przy przetwarzaniu danych osobowych.
12. Ustanowienie polityk ciągłości działania oraz opracowanie i wdrożenie planów zapewnienia ciągłości działania i planów odtworzeniowych.

V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Delegatury NIK w Bydgoszczy. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 28 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

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

Bydgoszcz, 22 sierpnia 2024 r.

Najwyższa Izba Kontroli
Delegatura w Bydgoszczy
z up. p.o. Wicedyrektor
(-) Adam Kończak

Kontroler:
(-) Leszek Murat
główny specjalista k.p.