NAJWYŻSZA IZBA KONTROLI
Departament Administracji Publicznej

KAP.410.3.1.2024

Pan
Lucjan Krzysztof Chrzanowski
Prezydent Miasta Żyrardowa
ul. Bolesława Limanowskiego 44
96-300 Żyrardów

WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
ul. Filtrowa 57, 02-056 Warszawa
T +48 22 444 53 08, F +48 22 444 52 52
kap@nik.gov.pl
Adres korespondencyjny: Skr. poczt. P-14, 00-950 Warszawa 1

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miasta Żyrardowa (dalej: Urząd), ul. Limanowskiego 44, 96-300 Żyrardów
Kierownik jednostki kontrolowanej	Lucjan Krzysztof Chrzanowski, Prezydent Miasta Żyrardowa od 4 listopada 2018 r. (dalej: Prezydent).
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 zakończenia czynności kontrolnych, tj. do 11 lipca 2024 r.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[1]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Departament Administracji Publicznej
Kontroler	Paweł Łukasiewicz, doradca ekonomiczny, upoważnienie do kontroli nr KAP/40/2024 z 21.05.2024 r.

(akta kontroli str. 1-3)

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

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

W okresie objętym kontrolą Prezydent Miasta Żyrardowa na ogół prawidłowo, rzetelnie i skutecznie realizował zadania związane z organizacją bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych. Wprowadzono System Zarządzania Bezpieczeństwem Informacji (dalej: SZBI), a w ramach niego Politykę Bezpieczeństwa Informacji (dalej: PBI).

Opracowano *Plan ciągłości działania systemu teleinformatycznego Urzędu Miasta Żyrardowa*[3] oraz harmonogramy testów tego planu, jednak dokumenty te dotyczyły wyłącznie 2024 roku i zgodnie z nimi przeprowadzono testy. Prezydent Miasta Żyrardowa, zgodnie z wymogami określonymi w RODO[4], powołał Inspektora Ochrony Danych (dalej: IOD) i umożliwił mu realizację zadań w sposób niezależny. Osoba pełniąca tę funkcję, a także inni pracownicy, którzy byli odpowiedzialni za bezpieczeństwo informacji, posiadali odpowiednie przygotowanie merytoryczne i doświadczenie zawodowe.

Wprowadzono i stosowano zasady tworzenia haseł dostępu do systemów informatycznych, a zabezpieczenia komputerów pracowników uniemożliwiały zainstalowanie nieautoryzowanego oprogramowania. Zapoznano pracowników z ustanowionymi w Urzędzie zasadami pracy zdalnej i mobilnej. Prowadzono także elektroniczny rejestr zasobów teleinformatycznych, który umożliwiał weryfikację sprzętu oraz jego konfiguracji.

Objęte kontrolą umowy z podmiotami zewnętrznymi, dotyczące m.in. wsparcia oraz serwisu sprzętu informatycznego, zawierały postanowienia gwarantujące odpowiedni poziom bezpieczeństwa informacji i poufności danych.

W Urzędzie wprowadzono procedury dotyczące zarządzania incydentami naruszenia bezpieczeństwa informacji, a w przypadku stwierdzenia incydentów podejmowano właściwe działania wyjaśniające i naprawcze. W Urzędzie przeprowadzona została również analiza ryzyka utraty integralności, dostępności lub poufności informacji. Przeprowadzono także okresowy audyt z zakresu bezpieczeństwa informacji.

Stwierdzone w trakcie kontroli nieprawidłowości polegały m.in. na:

- niesporządzeniu harmonogramów testów *Planu ciągłości działania systemu teleinformatycznego Urzędu Miasta Żyrardowa* na 2023 r. i nieprzeprowadzeniu testów tego planu w 2023 r., co było działaniem nierzetelnym i stanowiło naruszenie wytycznych określonych w punkcie 5.2. *Procedury zarządzania ciągłością działania systemu teleinformatycznego Urzędu Miasta Żyrardowa*[5],
- niewyznaczeniu i niezgłoszeniu do CSIRT NASK, w okresie od 1 marca 2024 r. do 27 maja 2024 r., osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, co było niezgodne z art. 21 ust. 1 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa[6] (dalej: ustawa o ksc),
- niesporządzeniu aktualnego zakresu czynności dla jednego pracownika Urzędu spośród 15 badanych, co było działaniem nierzetelnym, oraz niedokonaniu dla niego zmiany uprawnień do jednego z modułów w systemie informatycznym, co stanowiło naruszenie §19 ust. 2 pkt 5 rozporządzenia Rady Ministrów z dnia

[2] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[3] Nr BCP-ST01, zatwierdzony 17.09.2020 r.
[4] 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 r., str. 1, ze zm.
[5] Zatwierdzonej 17.09.2020 r.
[6] Dz. U. z 2024 r. poz. 1077.

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[7] (dalej: rozporządzenie KRI) oraz wewnętrznych uregulowań w tym zakresie,

- niesporządzeniu dla wszystkich 14 objętych kontrolą pracowników, którzy zakończyli pracę w Urzędzie, wniosków o odebranie upoważnienia i odebranie uprawnień do korzystania z systemu informatycznego, co było działaniem nierzetelnym i stanowiło naruszenie zasad określonych w punkcie 5.5. ppkt. 1 *Procedury kontroli dostępu do informacji chronionych Urzędu Miasta Żyrardowa*,
- zablokowaniu dostępu do systemów informatycznych jednemu spośród 14 objętych kontrolą pracowników, którzy zakończyli pracę w Urzędzie, dopiero po upływie 40 dni od rozwiązania z nim umowy o pracę, co było niezgodne z § 20 ust. 2 pkt 5 rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[8] (dalej: stare rozporządzenie KRI).

III. Opis ustalonego stanu faktycznego

OBSZAR

1. Organizacja bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych.

Opis stanu faktycznego

1. W Urzędzie dokonano identyfikacji zbiorów danych podlegających zabezpieczeniu. Sporządzony został rejestr czynności przetwarzania oraz wykaz aktywów informacyjnych, w których określono m.in. rodzaj wykonywanych czynności, cel przetwarzania danych, właściciela zbioru danych/procesu, okres przechowywania danych, zasoby wspomagające (oprogramowanie, sprzęt, infrastruktura, zasoby ludzkie), a także określono krytyczność i wrażliwość informacji ze względu na ich wagę.

(akta kontroli str. 4-250)

2. W okresie objętym kontrola obowiązywało zarządzenie Nr 369/20 Prezydenta Miasta Żyrardowa z dnia 17 września 2020 r. w sprawie ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji oraz wprowadzenia „Polityki Bezpieczeństwa Informacji". Na podstawie ww. zarządzenia, ustanowiono w Urzędzie System Zarządzania Bezpieczeństwem Informacji (dalej: SZBI), o czym powiadomiono pracowników Urzędu mailem wysłanym 9 października 2020 r. W skład SZBI wchodziły:

- Polityka Bezpieczeństwa Danych Osobowych,
- Polityka Bezpieczeństwa Informacji (dalej: PBI),
- Polityka Bezpieczeństwa Systemu Teleinformatycznego,
- Deklaracja Stosowania Zabezpieczeń,
- Regulamin Bezpieczeństwa Informacji,
- Procedury Bezpieczeństwa,
- Standardy Bezpieczeństwa.

(akta kontroli str. 251-432, 453-461, 477-484, 538-545, 566-573, 592-608, 609, 1194-1195,1225-1226)

W okresie objętym kontrolą realizację zadań dotyczących m.in. opracowywania, aktualizacji oraz dostosowywania dokumentacji SZBI do wymogów prawa unijnego

[7] Dz. U. poz. 773.
[8] Dz. U. z 2017 r. poz. 2247, uchylone z dniem 23 maja 2024 r.

i krajowego, a także w przypadku zmian organizacyjnych w Urzędzie, powierzono firmie zewnętrznej.

(akta kontroli str. 735-780)

Prezydent Miasta Żyrardowa poinformował, że *Od czasu wprowadzenia w Urzędzie Miasta Żyrardowa (17.09.2020 r.) Systemu Zarządzania Bezpieczeństwem Informacji nie dokonywano modyfikacji dokumentacji SZBI, ponieważ nie było żadnych istotnych zmian, które by tego wymagały. System Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Żyrardowa podlega cyklicznemu sprawdzaniu i monitorowaniu, które kończy się raportem. W dotychczasowych raportach nie wskazywano na konieczność zmian dokumentacji SZBI. Od początku 2023 r. planowana jest zmiana siedziby głównej Urzędu Miasta Żyrardowa, która spowoduje konieczność zmiany większości dokumentów wchodzących w skład SZBI*.

(akta kontroli str. 1199-1209)

3. W okresie objętym kontrolą obowiązywała *Polityka Bezpieczeństwa Danych Osobowych Urzędu Miasta Żyrardowa*[9], uwzględniająca wymogi RODO. Ww. dokument został zakomunikowany mailowo wszystkim pracownikom Urzędu z obowiązkiem stosowania. W ww. dokumencie określono m.in. obowiązki administratora danych osobowych oraz osób zaangażowanych w przetwarzanie danych osobowych.

(akta kontroli str. 253-294)

4. W celu zapewnienia ciągłości działania systemów informatycznych, w Urzędzie sporządzono Rejestr ryzyk, w którym wskazano m.in. komórki organizacyjne Urzędu, źródła ryzyka, opis zdarzeń powodujących ryzyko, obszar ryzyka, zagrożenia oraz ich skutki, a także prawdopodobieństwo ich wystąpienia.

(akta kontroli str. 243-250)

Ponadto w listopadzie 2023 r. firma zewnętrzna sporządziła *Raport z cyklicznego szacowania ryzyka dla bezpieczeństwa informacji i przetwarzania danych osobowych w Urzędzie Miasta Żyrardowa*. W ww. raporcie zawarto następujące wnioski:

a) zaktualizować systemy bez wsparcia producenta do nowszych wersji,
b) opracować, zatwierdzić, a następnie przetestować plany ciągłości działania,
c) przeprowadzać regularne przeglądy logów systemowych, a fakt ten odnotowywać w dzienniku administratora,
d) wykonać testy podatności infrastruktury IT,
e) przeprowadzić test odzysku maszyn wirtualnych w środowisku zapasowym (na zapasowym serwerze),
f) odnotowywać w postaci krótkiego raportu fakt przeprowadzenia testów kopii zapasowych,
g) każdorazowo odnotowywać w dzienniku administratora fakt wprowadzenia zmian w konfiguracji systemów.

Na dzień zakończenia kontroli, zrealizowano wnioski A i C, częściowo zrealizowano wnioski B i F, a realizację wniosków D i G zaplanowano na sierpień 2024 r.

(akta kontroli str. 1161-1188)

5. W okresie objętym kontrolą obowiązywała *Procedura zarządzania ciągłością działania systemu teleinformatycznego Urzędu Miasta Żyrardowa, zatwierdzona 17 września 2020 r*. Na jej podstawie sporządzono w Urzędzie:

[9] Wprowadzona Zarządzeniem nr 369 /20 Prezydenta Miasta Żyrardowa z 17 września 2020 r. w sprawie ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji oraz wprowadzenia „Polityki Bezpieczeństwa Informacji".

- Analizę wpływu na ciągłość działania (BIA) systemu teleinformatycznego Urzędu Miasta Żyrardowa,
- Plan ciągłości działania systemu teleinformatycznego Urzędu Miasta Żyrardowa Nr BCP-ST01,
- Harmonogram testów Planu ciągłości działania systemu teleinformatycznego Urzędu Miasta Żyrardowa tylko na 2024 r., natomiast harmonogramu nie sporządzono na 2023 r. (co szerzej opisano w sekcji *Stwierdzone nieprawidłowości)*.
- Raporty z testów Planu ciągłości działania systemu teleinformatycznego Urzędu Miasta Żyrardowa (testy przeprowadzono w miesiącu styczniu oraz maju 2024 r.). Testów nie przeprowadzono w 2023 r. (co szerzej opisano w sekcji *Stwierdzone nieprawidłowości)*.

(akta kontroli str. 485-537, 1161-1188, 1199-1208)

Dyrektor Wydziału Informatyki i Technologii Urzędu poinformował, że *w Urzędzie obowiązuje plan ciągłości działania dla systemu teleinformatycznego nr BCP-ST01 (…). Plan ten obejmuje wszystkie elementy wchodzące w skład systemu teleinformatycznego urzędu, tj. infrastruktura teletechniczna, sprzęt komputerowy, sprzęt serwerowy, zasilanie serwerowni, sprzęt sieciowy oraz oprogramowanie, w tym systemy teleinformatyczne (dziedzinowe), których wykaz w postaci tabelki przekazano (…). Opracowane w styczniu 2024 r. harmonogramy testowania planów ciągłości działania oraz instrukcje odzysku, zgodnie z którymi dokonuje się testowania, dotyczą składników krytycznych systemu teleinformatycznego nr BCP-ST01 w punkcie 2.1.2. Pierwszy scenariusz przetestowany w styczniu 2024 r., dotyczy odtworzenia bazy danych systemu INFO-SYSTEM, co pozwala na odtworzenie danych wszystkich modułów systemu INFO-SYSTEM, które stanowią wszystkie krytyczne systemu teleinformatyczne (dziedzinowe), podane w wykazie systemów teleinformatycznych urzędu. Drugi scenariusz przetestowany w maju 2024 r., dotyczy zmiany przełącznika głównego (rdzeniowego core), po wystąpieniu awarii, co stanowi element kluczowy dla działania całej infrastruktury sieciowej urzędu, a co za tym idzie całości systemu teleinformatycznego. Trzeci scenariusz przewidziany na sierpień 2024 r. dotyczy odtworzenia serwera Hyper-V (klaster wirtualizacji) dla systemu INFO-SYSTEM, co pozwoli na odtworzenie całego środowiska produkcyjnego systemu INFO-SYSTEM, tj. wszystkie systemy dziedzinowe, które stanowią element krytyczny planu BCP-ST01. Do pozostałych systemów teleinformatycznych, które wraz z systemami dziedzinowymi (INFO-SYSTEM) podane są w wykazie systemów teleinformatycznych, nie opracowano harmonogramów testów planów ciągłości działania i instrukcji odzysku, ponieważ nie stanowią one elementu krytycznego dla ciągłości działania urzędu lub dostęp do nich realizowany jest za pomocą przeglądarki internetowej i internetu (systemy zlokalizowane poza infrastrukturą urzędu)*.

(akta kontroli str. 1224)

6. W okresie objętym kontrolą dokonano jednego przeglądu adekwatności i skuteczności Systemu Zarządzania Bezpieczeństwem Informacji. W protokole przeglądu sporządzonym 12 grudnia 2023 r. zawarto następujące konkluzje:

- ustalono, że zakres SZBI jest aktualny i nie wymaga zmian,
- w nadchodzącym roku należy zwrócić szczególną uwagę na realizację procedur w zakresie zachowania ciągłości działania, w tym przede wszystkim przeprowadzać testy i ćwiczenia w tym zakresie,
- dokonano przeglądu raportu z szacowania ryzyka. Zostały przyjęte rekomendacje Pełnomocnika ds. SZBI zawarte w raporcie szacowania ryzyka, a plany postępowania z ryzykiem są sukcesywnie realizowane,

- nie zidentyfikowano konieczności aktualizacji obowiązującej dokumentacji SZBI.

(akta kontroli str. 662-663)

W Urzędzie wyznaczone zostały osoby odpowiedzialne za bezpieczeństwo informacji oraz zapewnienie ciągłości działania systemów teleinformatycznych. Do powyższych zadań wyznaczono trzech pracowników Wydziału Informatyki i Technologii Urzędu. Zakres powierzonych do realizacji ww. zadań został określony w zakres obowiązków ww. pracowników. Pracownicy ci posiadali wyższe wykształcenie o profilu informatycznym, a także ukończyli szkolenia związane z bezpieczeństwem systemów teleinformatycznych.

(akta kontroli str. 1210-1212)

7. W okresie objętym kontrolą funkcję Inspektora Ochrony Danych w Urzędzie Miasta Żyrardowa powierzono firmie zewnętrznej[10]. W umowach określono obowiązki IOD, do których zaliczono m.in. monitorowanie oraz zalecanie działań dostosowujących działalność Zamawiającego pod kątem wymagań określonych w przepisach unijnych i krajowych w zakresie ochrony danych osobowych. Do zadań IOD zaliczono w szczególności:

- przeprowadzanie telekonferencji stron i wizyt konsultacyjnych w siedzibie Zamawiającego uzgodnionych w ramach potrzeb,
- dokonywanie analizy zgłaszanych przez Zamawiającego problemów dotyczących przedmiotu umowy,
- dokonywanie analizy dokumentacji,
- dokonywanie analizy incydentu w realizacji zadań publicznych przez Zamawiającego,
- aktualizacja dokumentacji ochrony danych osobowych Zamawiającego.

(akta kontroli str. 735-814)

8. W latach 2023-2024 r. (z wyjątkiem okresu od 1 marca 2024 r. do 27 maja 2024 r., co szerzej opisano w sekcji *Stwierdzone nieprawidłowości*), zgodnie z art. 21 ust. 1 ustawy o ksc, w Urzędzie wyznaczono i zgłoszono do CSIRT NASK osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.

(akta kontroli str. 1161-1191, 1216)

9. W Urzędzie prowadzono elektroniczny rejestr zasobów teleinformatycznych w postaci wykazu systemów informatycznych wykorzystywanych w Urzędzie. Ponadto do inwentaryzacji sprzętu informatycznego oraz monitorowania dostępu do danego urządzenia i systemu informatycznego, wykorzystywany był system Axence nVision.

W wyniku przeprowadzonych oględzin sprzętu informatycznego znajdującego się w Urzędzie, tj. próby 10 komputerów stacjonarnych, jednego serwera, dwóch laptopów, jednego routera i jednej drukarki stwierdzono, że dane zawarte w systemie Axence nVision umożliwiały zweryfikowanie, który pracownik jest użytkownikiem ww. sprzętu informatycznego oraz w jaki sposób sprzęt ten jest skonfigurowany.

(akta kontroli str. 243-250, 609, 1063-1106)

10. Urząd przystąpił do rządowego projektu „Cyberbezpieczny Samorząd". Umowę o powierzenie grantu podpisano 6 maja 2024 r.[11]. We wniosku o przyznanie grantu określono m.in.:

[10] Na 2023 r. zawarto Umowę Nr IT.1.2023 z 30.12.2022 r. wraz z Umową Powierzenia Przetwarzania Danych Osobowych z 30.12.2022 r. Na 2024 r. zawarto Umowę Nr 1.IT.2024 z 28.12.2023 r. wraz z Umową Powierzenia Przetwarzania Danych Osobowych z 28.12.2023 r.

[11] Umowa o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/0563/FERC.02.02-CS.01-001/23/2024.

- zakres finansowy, tj. zakupy w ramach wydatków rzeczowych:
  a) urządzenia do składowania danych kopii zapasowych – 1 szt. – 223.245 zł (w tym dofinansowanie 209.850,3 zł),
  b) oprogramowanie do wykonywania kopii bezpieczeństwa – 4 szt. – 27.552 zł (w tym dofinansowanie 25.898,89 zł),
  c) oprogramowanie do analizy logów – 1 szt. – 41.328 zł (w tym dofinansowanie 38.848,33 zł),
  d) oprogramowanie antywirusowe – 1 szt. – 49.200 zł (w tym dofinansowanie 46.248,02 zł),
  e) oprogramowanie do zarządzania infrastrukturą IT – 1 szt. – 14.760 zł (w tym dofinansowanie 13.874,40 zł),
  f) serwer – 1 szt. – 139.092,09 zł (w tym dofinansowanie 130.746,61 zł),
  g) licencja UTM – 1 szt. – 27.892,71 zł (w tym dofinansowanie 26.219,16 zł),
  h) macierz – 1 szt. – 104.395,02 zł (w tym dofinansowanie 98.131,35 zł),
  i) doradztwo techniczne – 1 szt. – 36.900 zł (w tym dofinansowanie 34.686,01 zł),
  j) dokumentacja cyberbezpieczeństwa SZBI wraz z audytami, KRI – 1 szt. – 86.100 zł (w tym dofinansowanie 80.934,03 zł),
  k) szkolenia dla informatyków – 1 szt. – 73.800 zł (w tym dofinansowanie 69.372,02 zł),
  l) platforma szkoleniowa – 1 szt. – 55.350 zł (w tym dofinansowanie 52.029,02 zł),
  m) szkolenie pracowników i kadry kierowniczej – 1 szt. – 24.600 zł (w tym dofinansowanie 23.124,01 zł).
- źródła finansowania wydatków, tj.:
  a) wartość dofinansowania z grantu – 849.962,22 zł,
  b) wkład własny beneficjenta – 54.252,60 zł.

(akta kontroli str. 860-914)

Na dzień 7 lipca 2024 r. w ramach ww. grantu Urząd otrzymał środki finansowe w wysokości 254.988,66 zł i nie dokonano jeszcze żadnych wydatków określonych we wniosku o dofinansowanie.

(akta kontroli str. 1217-1220)

W związku z przystąpieniem do ww. programu, Prezydent Miasta Żyrardowa poinformował, że *audyt przedwdrożeniowy ma za zadanie wskazać obszary, w których należy podwyższyć poziom cyberbezpieczeństwa, natomiast audyt powdrożeniowy wskaże, jak bardzo realizacja programu przyczyniła się do poprawy poziomu cyberbezpieczeństwa w urzędzie*. Dodał także, że *na dzień dzisiejszy wypełniono i wysłano, wymaganą w projekcie ankietę dojrzałości. Jako pierwsze zadanie realizacji projektu zaplanowano audyt przedwdrożeniowy, którego elementem jest bezpieczeństwo informacji. Realizacja tego audytu nastąpi do końca 3 kwartału 2024 r*.

(akta kontroli str. 1210-1212)

Stwierdzone nieprawidłowości

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

1. Nie sporządzono Harmonogramu testów Planu ciągłości działania systemu teleinformatycznego Urzędu Miasta Żyrardowa na 2023 r. i w związku z tym w 2023 r. nie przeprowadzono takich testów, co było działaniem nierzetelnym i stanowiło naruszenie wytycznych określonych w punkcie 5.2. *Procedury zarządzania ciągłością działania systemu teleinformatycznego Urzędu Miasta Żyrardowa*.

(akta kontroli str. 1161-1188, 1199-1209)

Prezydent Miasta Żyrardowa wyjaśnił, że *W związku z planowaną, od samego początku roku 2023 , zmianą siedziby Urzędu Miasta Żyrardowa i związaną z tym również zmianą infrastruktury teleinformatycznej, Dyrektor Wydziału Informatyki i Technologii podjął decyzję, iż harmonogramy testów planu ciągłości działania zostaną ustalone i przetestowane po zmianie siedziby urzędu. Niestety, z uwagi na opóźnienia związane z dostosowywaniem nowej siedziby urzędu do codziennej pracy, zmiana siedziby możliwa stała się dopiero w 2024 r. Konieczność ustalania i przetestowania harmonogramów testów ciągłości działania zauważono w „raporcie z cyklicznego szacowania ryzyka dla bezpieczeństwa informacji i przetwarzania danych osobowych w Urzędzie Miasta Żyrardowa" z listopada 2023 roku. Zgodnie z zaleceniami ww. raportu harmonogramy na rok 2024 ustalono w styczniu 2024 roku. Do chwili obecnej zrealizowano dwa z trzech, zaplanowanych na rok 2024, scenariuszy testowania*.

(akta kontroli str. 1222-1223)

Zdaniem NIK, fakt zmiany siedziby Urzędu nie może stanowić uzasadnienia odstąpienia od obowiązku sporządzenia ww. harmonogramów i testów planu ciągłości działania Urzędu, zwłaszcza w sytuacji, kiedy nie było możliwości określenia precyzyjnie dnia zmiany siedziby Urzędu.

2. W okresie od 1 marca 2024 r. do 27 maja 2024 r. w Urzędzie nie wyznaczono i nie zgłoszono do CSIRT NASK osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, co było niezgodne z art. 21 ust. 1 ustawy o ksc.

(akta kontroli str. 1161-1191, 1216)

W kwestii niewyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w okresie od 1 marca do 27 maja 2024 r., Prezydent Miasta Żyrardowa wyjaśnił, że *Zakończenie zatrudnienia […] nastąpiło w sposób nagły, bez okresu wypowiedzenia (pracownik przesunięty pomiędzy jednostkami samorządu terytorialnego) i przypadło w okresie przygotowawczym do wyborów samorządowych (7.04.2024 r.). Powyższe okoliczności, w dużej mierze, przyczyniły się do przeoczenia i spowodowały opóźnienie w wyznaczeniu nowej osoby odpowiedzialnej za utrzymywanie kontaktów z krajowymi podmiotami cyberbezpieczeństwa*.

(akta kontroli str. 1217-1219)

W związku z wyznaczeniem 28 maja 2024 r. i zgłoszeniem do CSIRT NASK osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, NIK odstępuje od formułowania wniosku pokontrolnego w tym zakresie.

OCENA CZĄSTKOWA

W Urzędzie na ogół prawidłowo zrealizowano zadania związane z bezpieczeństwem informacji i zapewnienia ciągłości działania systemów informatycznych. Ustanowiono System Zarządzania Bezpieczeństwem Informacji, w tym Politykę Bezpieczeństwa Informacji, z którymi zapoznano pracowników Urzędu. Wskazano osoby odpowiedzialne za zapewnienie bezpieczeństwa informacji oraz zapewnienie

ciągłości działania systemów informatycznych. Sporządzono harmonogramy testów *Planu ciągłości działania systemu informatycznego* tylko na 2024 r., zgodnie z którymi zostały przeprowadzone testy. W 2023 r. testy takie nie były prowadzone.

OBSZAR

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

Opis stanu faktycznego

1. W Urzędzie została zablokowana możliwość instalacji przez użytkowników systemów informatycznych nieautoryzowanego oprogramowania na komputerach służbowych.

Na podstawie oględzin przeprowadzonych na próbie 10 komputerów ustalono, że we wszystkich przypadkach użytkownicy nie mieli możliwości zainstalowania nieautoryzowanego oprogramowania, ze względu na brak uprawnień. Było to zgodne z § 20 ust. 2 pkt 4 starego rozporządzenia KRI i § 19 ust. 2 pkt 4 nowego rozporządzenia KRI.

(akta kontroli str. 585-591, 1055-1062)

W kwestii stosowanych zabezpieczeń na urządzeniach wykorzystywanych przez pracowników Urzędu (np. tablety czy smartfony), Prezydent Miasta Żyrardowa poinformował, że *w Urzędzie Miasta Żyrardowa nie są używane urządzenia typu tablet. Służbowe smartfony wykorzystywane są jedynie do wykonywania rozmów telefonicznych i nie są wykorzystywane do przetwarzania informacji. Nie mają również dostępu do zasobów teleinformatycznych Urzędu Miasta Żyrardowa*.

(akta kontroli str. 1161-1167)

2. W celu sprawdzenia czy osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków, dokonano weryfikacji dokumentacji 15 losowo wybranych pracowników Urzędu. W wyniku przeprowadzonych badań stwierdzono, że:

- wszyscy pracownicy objęci badaniem posiadali upoważnienia do przetwarzania danych w systemach informatycznych, które wykorzystywali przy wykonywaniu czynności służbowych,
- 14 spośród 15 objętych badaniem pracowników posiadało uprawnienia i dostęp do systemów informatycznych zgodny z zakresem czynności. Jeden z pracowników, który w dniu 5 lipca 2023 r. został przeniesiony z Wydziału Gospodarki Mieszkaniowej do Urzędu Stanu Cywilnego i Spraw Obywatelskich, do dnia 7 lipca 2024 r. nie posiadał aktualnego zakresu czynności oraz posiadał dostęp do jednego z modułów w systemie informatycznym, powiązany z pracą w Wydziale Gospodarki Mieszkaniowej (co szerzej opisano w sekcji *Stwierdzone nieprawidłowości)*,
- wszyscy pracownicy posiadali uprawnienia związane z czynnościami wykonywanymi na zajmowanym stanowisku pracy w Urzędzie.

(akta kontroli str. 915-920, 1212—1215, 1221)

3. Kontrola wykazała, że spośród losowo wybranych 14 pracowników, którzy zakończyli pracę w Urzędzie w okresie od 1 stycznia 2023 r. do 27 maja 2024 r., wszystkim pracownikom zablokowano dostęp do systemów informatycznych, w ramach których wykonywali oni swoje czynności służbowe.

Dostęp taki został zablokowany, pomimo niezłożenia przez pracowników lub przełożonych, wniosków o odebranie uprawnień, do czego zobowiązywała

obowiązująca w Urzędzie *Procedura kontroli dostępu do informacji chronionych Urzędu Miasta Żyrardowa.* Stwierdzono także, że w jednym przypadku na 14 objętych badaniem, dostęp do systemów informatycznych został zablokowany pracownikowi po upływie 40 dni od rozwiązania umowy o pracę (co szerzej opisano w sekcji *Stwierdzone nieprawidłowości*).

(akta kontroli str. 546-565, 925-1054, 1196-1198)

4. W celu sprawdzenia zabezpieczeń technicznych wprowadzonych w systemach informatycznych Urzędu stosowanych w celu zapewnienia ochrony przetwarzanych informacji przed nieuprawnionym dostępem, dokonano sprawdzenia trzech systemów informatycznych stosowanych w Urzędzie. Kontrola wykazała, że:

- w odniesieniu do każdego z badanych systemów ustalone były wymagania dla haseł dostępu do tych systemów,
- we wszystkich systemach ustawiane przez użytkownika systemu hasło, musiało składać się z minimum 8 znaków,
- maksymalny czas ważności hasła wynosił 90 dni (dla dwóch systemów) oraz 30 dni (dla jednego systemu),
- na podstawie listy identyfikatorów w systemach ustalono, że nazwy loginów umożliwiały bezpośrednie ich powiązanie z daną osobą (tj. login powstał od połączenia pierwszych liter imienia i nazwiska użytkownika). Nie stwierdzono loginów o nazwie bezosobowej, np. Departament, Wydział, Biuro itp.

(akta kontroli str. 585-591, 609, 1140-1146)

5. W wyniku przeprowadzonych oględzin dwóch stanowisk pracy w Urzędzie, gdzie obywatele załatwiali sprawy z zakresu wydawania dowodów osobistych stwierdzono, że znajdujące się na stanowiskach pracy monitory komputerowe uniemożliwiały obsługiwanym obywatelom wgląd do danych wyświetlanych na tych monitorach. Powyższe działania spełniały wymogi § 19 ust. 2 pkt 7 rozporządzenia KRI.

(akta kontroli str. 1154-1160)

6. W załączniku nr 1 do *Procedury kontroli dostępu do informacji chronionych Urzędu Miasta Żyrardowa*, określono *Zasady zabezpieczenia dostępu zdalnego*. Powyższe zostało zakomunikowane mailowo wszystkim pracownikom Urzędu z obowiązkiem stosowania. W ww. dokumencie określono m.in. sposób uzyskiwania dostępu zdalnego do zasobów systemu teleinformatycznego Urzędu zarówno dla pracowników Urzędu, jak i pracowników firm zewnętrznych, a także stosowane zabezpieczenia pracy zdalnej i pracy mobilnej.

(akta kontroli str. 558-565)

7. W celu zabezpieczenia danych na dyskach komputerów przenośnych będących w posiadaniu Urzędu wykorzystywane było szyfrowanie dysków z użyciem specjalistycznego oprogramowania.

(akta kontroli str. 243-250, 859)

8. W urzędzie zastosowano właściwe zabezpieczenie serwerowni w celu ochrony informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie.

(akta kontroli str. 574-584, 1107-1132)

9. W okresie objętym kontrolą Urząd zawarł cztery umowy na zakup sprzętu komputerowego, cztery umowy na zakup oprogramowania, pięć umów na utrzymanie oprogramowania. Kontrola czterech umów[12] wykazała, że we wszystkich umowach zawarto zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji,

[12] Umowa Nr ZP.271.2.12.2023 z 23 maja 2023 r., Umowa nr BIP/0038/2024 z 25.10.2023 r., Umowa Nr 035/2024 z 24.11.2023 r., Umowa Nr U/0060/2024 z 25.10.2023 r.

co spełniało wymogi określone w § 20 ust. 2 pkt 10 starego rozporządzenia KRI. Przykładowo w umowie Nr ZP.271.2.12.2023 podano m.in., że *Wszelkie informacje uzyskane przez Wykonawcę w związku z realizacją Przedmiotu Umowy mogą być wykorzystywane tylko i wyłącznie w celu realizacji Przedmiotu Dostawy. Wykonawca będzie zachowywał zasady najściślejszej poufności w stosunku do wszystkich w/w informacji*.

(akta kontroli str. 243-250, 681-734)

10. W okresie objętym kontrolą w Urzędzie obowiązywała *Procedura niszczenia nośników oraz przekazywania do ponownego użycia Urzędu Miasta Żyrardowa*[13]. W ww. procedurze określono m.in. zasady likwidacji sprzętu komputerowego, zasady niszczenia nośników oraz przekazywania ich do ponownego użycia. Wdrożone rozwiązania uniemożliwiały dostęp do danych znajdujących się na tych urządzeniach.

(akta kontroli str. 243-250, 462-471)

11. W celu zapewnienia ciągłości działania systemów informatycznych Urzędu, w okresie objętym kontrolą obowiązywała *Procedura wykonywania kopii zapasowych Urzędu Miasta Żyrardowa*[14]. W procedurze tej określono m.in. częstotliwość wykonywania kopii bezpieczeństwa (codziennie w przypadku baz danych, dokumentów użytkowników oraz do 30 dni w przypadku plików instalacyjnych programów, sterowników itp.), osoby odpowiedzialne i uprawnione do ich wykonywania, przechowywanie kopii zapasowych oraz zasady dostępu do nich, a także konieczność testowania poprawności kopii zapasowych (minimum jeden raz na pół roku).

Ustalono, że kopie zapasowe danych z systemów informatycznych zarządzanych przez Urząd znajdowały się na macierzach dyskowych umieszczonych w budynkach w różnych lokalizacjach (tj. kopia danych z systemu użytkowanego w jednym budynku urzędu, znajdowała się na macierzy dyskowej znajdującej się w innym budynku urzędu). Kopie zapasowe znajdowały się w każdym z trzech budynków Urzędu.

W wyniku przeprowadzonych oględzin pomieszczenia jednego z budynków Urzędu stwierdzono, że kopie zapasowe danych znajdowały się na macierzach w szafach RACK w pomieszczeniu serwerowni. Dostęp do pomieszczenia był zabezpieczony. Do tworzenia kopii zapasowych używano systemów rekomendowanych przez producenta danego oprogramowania. Potwierdzeniem prawidłowego wykonania kopii zapasowej danych było otrzymanie maila na adres mailowy, dostępny dla pracowników Wydziału Informatyki i Technologii w Urzędzie. Dyrektor Wydziału Informatyki i Technologii w Urzędzie poinformował, że kopie zapasowe dotyczące dokumentacji elektronicznej pracowników tworzone są codziennie (poza weekendami).

W celu sprawdzenia poprawności wykonywania kopii zapasowej, dokonano testu odzyskiwania danych z kopii zapasowej wykonanej w dniu 18 kwietnia 2024 r. dotyczącej jednego modułu wybranego systemu. Po wgraniu danych z ww. kopii wyświetliły się prawidłowe dane z ww. modułu do miesiąca kwietnia 2024 r.

(akta kontroli str. 472-476, 1133-1139)

12. Pracownicy Wydziału Informatyki i Technologii prowadzili na bieżąco monitorowanie zasobów informatycznych, w tym wydajności i pojemności nośników pamięci systemów Urzędu. Podejmowane były działania w zakresie zwiększenia zasobów informatycznych, w szczególności serwerowni w związku z rosnącymi

[13] Oznaczona PB-06 i zatwierdzona 17.09.2020 r.
[14] Oznaczona PB-11 i zatwierdzona 17.09.2020 r.

potrzebami. W tym celu dokonywano zakupów sprzętu informatycznego, jak np. serwera, dysków SSD oraz dysków do macierzy NAS, pamięci operacyjnej.

(akta kontroli str. 243-250, 845-857)

W wyniku przeprowadzonych oględzin trzech serwerów znajdujących się w Urzędzie ustalono, że zajętość dysków twardych w poszczególnych serwerach wynosiła 2,5%, 4,7% oraz 83,4% całkowitej dostępnej pojemności serwerów.

(akta kontroli str. 1147-1153)

Prezydent Miasta Żyrardowa poinformował, że *(…) nie opracowano oddzielnych procedur dotyczących sposobu monitorowania pojemności pamięci masowych w serwerach. Zasady monitorowania systemu teleinformatycznego (w tym pamięci masowych) zostały opisane w Polityce Bezpieczeństwa Systemu Teleinformatycznego. Pracownicy Wydziału Informatyki i Technologii prowadzą stałe monitorowanie zasobów informatycznych, w tym wydajności i pojemności. Do monitorowania używane jest oprogramowanie Axence nVision, w którym ustawiono alarmy dotyczące kończących się zasobów (w tym między innymi miejsca na dyskach twardych serwerów). (…) Próg alarmu na serwerze nr (…) ustawiony jest na 10GB, co w przypadku tego serwera, pracownicy wydziału IT uznali za wystarczający. Dodatkowo serwer ten jest w trakcie przenoszenia na nowe urządzenie o znacznie większych zasobach, gdzie próg alarmowy będzie mógł być ustawiony na większym poziomie*.

(akta kontroli str. 1210-1212)

NIK zauważa, że w przypadku serwera, który posiada jedynie 16,6% wolnej przestrzeni na dysku twardym, może to powodować obniżenie wydajności pracy serwera.

13. W ramach zapewnienia ciągłości działania urzędu zidentyfikowane zostały kluczowe elementy infrastruktury i usługi IT oraz ich zabezpieczenie pod kątem wpływu czynników zewnętrznych. W celu zapewnienia ciągłości działania Urzędu została przeprowadzona *Analiza wpływu na ciągłość działania (BIA) systemu teleinformatycznego Urzędu Miasta Żyrardowa*[15]. W ww. dokumencie określono m.in. wymagania ciągłości działania dla krytycznych elementów infrastruktury informatycznej. Ponadto Urząd posiadał opracowany Plan ciągłości działania dla systemu informatycznego BCP-ST01 oraz instrukcję odzyskiwania (przywracania do działania) poszczególnych elementów infrastruktury informatycznej.

(akta kontroli str. 243-251)

Stwierdzone nieprawidłowości

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

1. Jeden spośród 15 pracowników objętych badaniem, do dnia 7 lipca 2024 r. nie posiadał aktualnego zakresu czynności oraz posiadał dostęp do jednego z modułów w systemie informatycznym, powiązany z Wydziałem Gospodarki Mieszkaniowej Urzędu, pomimo, iż od 5 lipca 2023 r. został przeniesiony innego wydziału w Urzędzie, tj. do Urzędu Stanu Cywilnego i Spraw Obywatelskich. Stosownie do §2 ust. 2 zarządzenia Nr 194/22 Prezydenta Miasta Żyrardowa z dnia 8 czerwca 2022 r. w sprawie wprowadzenia wzoru Zakresu czynności, uprawnień i odpowiedzialności pracowników Urzędu Miasta Żyrardowa, w przypadku zmiany Zakresu, nowy Zakres przekazuje się do Wydziału Organizacyjnego, w terminie określonym w §2 ust. 2 ww. zarządzenia, tj. w terminie 14 dni. Ponadto w myśl §19

[15] Zatwierdzona 5 stycznia 2021 r.

ust. 2 pkt 5 rozporządzenia KRI, należy dokonywać bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji

(akta kontroli str. 858, 1221, 1234-1237)

Prezydent Miasta Żyrardowa wyjaśnił, że *w aktach nie ma aktualnego zakresu czynności, ponieważ nie został przekazany do kadr przez Kierownika USCO (…)*

Ponadto wyjaśnił, że *W dniu 7 lipca 2023 r. w związku ze zmianą stanowiska i przeniesieniem do USCO Prezydent Miasta wydał upoważnienie do przetwarzania danych osobowych i do systemów informatycznych. Skan tego upoważnienia został przekazany do WIiT. W przekazanym upoważnieniu nie ma żadnej informacji odnośnie systemu informatycznego Info System – moduł Umowy/Faktury, dlatego pracownicy Wydziału Informatyki i Technologii nie dokonali w powyższym systemie żadnych zmian*.

(akta kontroli str. 1213-1215)

Kierownik Urzędu Stanu Cywilnego i Spraw Obywatelskich wyjaśniła, że *pracownik USCO (…) nie posiadała karty stanowiska pracy, bowiem do dnia 30.06.2024 r. była jedynie pomocą administracyjną i wykonywała tylko polecenia służbowe bezpośredniego przełożonego. Ponadto informuję, że w dniu 8.07.2024 r. złożyłam wniosek do Wydziału OR tutejszego Urzędu Miasta o cofnięcie wymienionej uprawnień do dostępu do modułu faktury/umowy*.

(akta kontroli str. 1229)

W związku z faktem, że w trakcie kontroli, tj. w dniu 8 lipca 2024 r. został sporządzony aktualny zakres czynności dla ww. pracownika oraz wniosek o odebranie pracownikowi dostępu ww. modułu, NIK nie formułuje wniosku pokontrolnego w tym zakresie.

(akta kontroli str. 1227-1228, 1230-1233)

2. W przypadku 14 pracowników objętych badaniem, którzy zakończyli pracę w Urzędzie, nie zostały złożone przez nich lub ich przełożonych, wnioski o odebranie upoważnienia i odebranie uprawnień do korzystania z systemu informatycznego Urzędu, do czego zobowiązywały postanowienia zawarte w punkcie 5.5. ppkt. 1 *Procedury kontroli dostępu do informacji chronionych Urzędu Miasta Żyrardowa*.

(akta kontroli str. 921-1013)

Prezydent Miasta Żyrardowa wyjaśnił, że *Zgodnie z Procedurą kontroli dostępu do informacji chronionych w przypadku osób pracujących na stanowiskach samodzielnych oraz kierowników komórek organizacyjnych za wystosowanie wniosku odpowiedzialne są te osoby. Taka sytuacja dotyczy kierowników komórek organizacyjnych wskazanych w piśmie (…). Ponieważ Dyrektorzy ci odchodząc z pracy nie wystąpili z takimi wnioskami, WIiT został poinformowany ustnie przez pracownika kadr. To samo dotyczy (…). W kwietniu 2023 r. Biuro Prawne, którego te Panie były pracownikami zostało zlikwidowane, a Koordynator Biura przekazał ustnie informację do WIiT. Jeśli chodzi o pozostałe osoby (…) o zakończeniu pracy przez te osoby WIiT został poinformowany w procedurze „obiegówki" oraz telefonicznie przez pracownika kadr*".

(akta kontroli str. 1196-1198)

3. Pomimo zakończenia pracy w Urzędzie przez jednego pracownika[16] w dniu 31 stycznia 2023 r., dostęp do systemów informatycznych, w ramach których wykonywał on swoje czynności, został zablokowany dopiero po upływie 40 dni od rozwiązania

[16] Pan T.H.

z nim umowy o pracę. Było to niezgodne z zasadą określoną w § 20 ust. 2 pkt 5 starego rozporządzenia KRI, zgodnie z którą należy dokonywać bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji.

(akta kontroli str. 926-927, 1014-1054, 1196-1198)

Prezydent Miasta Żyrardowa wyjaśnił, że *powodem opóźnienia jest błędne wybranie miesiąca w dacie automatycznego blokowania konta użytkownika w systemie informatycznym urzędu. Pracownik Wydziału Informatyki i Technologii omyłkowo zaznaczył miesiąc marzec zamiast miesiąca stycznia – błąd ludzki.*

(akta kontroli str. 1196-1198)

OCENA CZĄSTKOWA

NIK pozytywnie ocenia działalność Urzędu w zakresie wdrożonych i wykorzystywanych rozwiązań organizacyjnych i technicznych zapewniających bezpieczeństwo informacji oraz ciągłość działania, z wyjątkiem nieprawidłowości, które dotyczyły m.in. niesporządzenia wniosków o odebranie upoważnienia i odebranie uprawnień do korzystania z systemów informatycznych oraz zablokowania dostępu do systemów informatycznych jednemu pracownikowi dopiero po upływie 40 dni od rozwiązania z nim umowy o pracę. W Urzędzie prawidłowo realizowano zadania w zakresie zabezpieczenia komputerów przed nieuprawnioną instalacją oprogramowania przez użytkowników. Ustanowiono i zapoznano pracowników z procedurami pracy zdalnej i mobilnej. Zapewniono także bezpieczeństwo informacji poprzez ustawienie monitorów w sali obsługi obywateli w sposób uniemożliwiający wgląd do danych przez osoby nieuprawnione. W umowach z firmami zewnętrznymi wprowadzano postanowienia gwarantujące odpowiedni poziom bezpieczeństwa i poufności informacji.

OBSZAR

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji.

Opis stanu faktycznego

1. W okresie objętym kontrolą, w 2023 r. firma zewnętrzna sporządziła *Raport z cyklicznego szacowania ryzyka dla bezpieczeństwa informacji i przetwarzania danych osobowych w Urzędzie Miasta Żyrardowa.* W dokumencie tym opisano w jaki sposób przeprowadzono szacowanie ryzyka, tj., że kalkulacja ryzyka została oparta o kombinację wartości aktywów, poziomu prawdopodobieństwa wykorzystania podatności i materializacji zagrożenia, przy uwzględnieniu obecnie zastosowanych zabezpieczeń. Podano, że jako wpływ zagrożenia na Urząd przyjmuje się skutki dla Urzędu, w wyniku materializacji opisanego scenariusza zdarzenia i w tym przypadku wpływ określono jako utratę bezpieczeństwa dla poufności, integralności oraz dostępności zasobu.

(akta kontroli str. 610-661)

2. W okresie objętym kontrolą w Urzędzie obowiązywała *Procedura zarządzania incydentami naruszenia bezpieczeństwa informacji*[17]. Ww. procedura została zakomunikowana wszystkim pracownikom mailowo z obowiązkiem jej przestrzegania. W dokumencie tym określono m.in. co stanowi incydent i jakie są jego rodzaje oraz sposób postępowania w przypadku wystąpienia incydentu.

(akta kontroli str. 433-452)

[17] Oznaczona PB-04 i zatwierdzona 17.09.2020 r.

Ponadto w Urzędzie obowiązywał *Regulamin Bezpieczeństwa Informacji Urzędu Miasta Żyrardowa*[18], w którym opisano m.in. zasady postępowania w przypadku naruszenia bezpieczeństwa informacji i danych osobowych.

(akta kontroli str. 296-305)

W okresie objętym kontrolą w prowadzonym w Urzędzie rejestrze incydentów odnotowano trzy incydenty naruszenia bezpieczeństwa informacji[19]. W każdym przypadku przeprowadzono postępowanie wyjaśniające i podjęto działania korygujące. W jednym przypadku pracownik Urzędu, który spowodował zdarzenie, został skierowany na szkolenie z zakresu ochrony danych osobowych i bezpieczeństwa informacji.

(akta kontroli str. 243-250, 1161-1167)

3. W okresie objętym kontrolą w Urzędzie nie opracowywano harmonogramu szkoleń dla pracowników związanych z przetwarzaniem informacji. W okresie od 1 stycznia 2023 r. do 14 czerwca 2024 r. nie przeprowadzono w Urzędzie żadnego szkolenia z bezpieczeństwa informacji.

(akta kontroli str. 1161-1167)

Prezydent Miasta Żyrardowa poinformował, że *Szkolenia z zakresu bezpieczeństwa przetwarzania informacji realizuje dla Urzędu firma (…), świadcząca dla Urzędu usługi Inspektora Ochrony Danych oraz Pełnomocnika ds. Cyberbezpieczeństwa. W miarę możliwości szkolenia z bezpieczeństwa przetwarzania informacji organizowane są raz na 12 miesięcy dla wszystkich pracowników przetwarzających informacje. W 2023 r. szkolenia z zakresu bezpieczeństwa informacji nie zostały zrealizowane, dlatego też w roku 2024 planowane są dwie sesje szkoleniowe. Pierwsze szkolenie odbędzie się na przełomie czerwca i lipca, zaś druga sesja szkoleniowa na przełomie października i listopada. W dniu 24 czerwca 2024 r., na skrzynki mailowe pracowników zostały wysłane wiadomości z systemu szkoleniowego (…) o utworzeniu indywidualnych kont na platformie e-learningowej.*

(akta kontroli str. 1161-1195)

Zdaniem NIK, istotne jest opracowanie harmonogramu szkoleń na dany rok z zakresu bezpieczeństwa informacji, szczególnie, że w zaleceniach po audycie z wymagań KRI i ustawy o ksc przeprowadzonym w Urzędzie 2023 r., wskazane to było jako działanie doskonalące.

4. W okresie objętym kontrolą, zgodnie z § 20 ust. 2 pkt 14 starego rozporządzenia KRI, w Urzędzie przeprowadzono okresowy audyt z zakresu bezpieczeństwa informacji. Firma zewnętrzna sporządziła w 2023 r. *Raport z audytu wymagań KRI i ustawy o krajowym systemie cyberbezpieczeństwa w Urzędzie Miejskim w Żyrardowie*. W dokumencie sformułowano 12 zaleceń/rekomendacji, z których na dzień 25 czerwca 2024 r. zrealizowano cztery, natomiast realizacja pozostałych, jak poinformował Prezydent Miasta Żyrardowa, planowana jest na drugą połowę 2024 r.

(akta kontroli str. 664-680, 1199-1209)

Stwierdzone nieprawidłowości

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

OCENA CZĄSTKOWA

NIK pozytywnie ocenia działania Urzędu w celu zapobiegania incydentom bezpieczeństwa danych. W Urzędzie ustanowiono i stosowano procedury dotyczące

[18] Zatwierdzony 17.09.2020 r.
[19] Incydenty nie dotyczyły naruszenia danych osobowych.

zarządzaniem incydentami naruszenia bezpieczeństwa informacji. W przypadkach wystąpienia incydentów z zakresu naruszenia bezpieczeństwa informacji podejmowano bezzwłoczne działania wyjaśniające i korygujące. Przeprowadzono także analizę ryzyka utraty integralności, dostępności lub poufności informacji. W Urzędzie przeprowadzono także okresowy audyt z zakresu bezpieczeństwa informacji.

IV. Wnioski

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

Wnioski

1. Sporządzanie harmonogramów testów Planu ciągłości działania systemu teleinformatycznego Urzędu oraz przeprowadzanie testów w każdym roku, zgodnie z obowiązującymi w Urzędzie procedurami w tym zakresie.
2. W przypadku rozwiązania z pracownikiem umowy o pracę, sporządzanie wniosków o odebranie upoważnienia i odebranie uprawnień do korzystania z systemu informatycznego Urzędu, stosownie do obowiązującej *Procedury kontroli dostępu do informacji chronionych Urzędu Miasta Żyrardowa*.
3. Blokowanie dostępu do systemów informatycznych niezwłocznie po rozwiązaniu z pracownikiem umowy o pracę.

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 Departamentu Administracji Publicznej Najwyższej Izby Kontroli. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykonania wniosków

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

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.

Warszawa, sierpnia 2024 r.

Najwyższa Izba Kontroli
Departament Administracji Publicznej

Kontroler
Paweł Łukasiewicz
Doradca ekonomiczny

/podpisano elektronicznie/

p.o. Dyrektor
Bogdan Skwarka
wz. p.o. Wicedyrektora
Dariusz Łubian

/podpisano elektronicznie/