NAJWYŻSZA IZBA KONTROLI
Delegatura w Łodzi

LLO.410.013.05.2018
P/18/006

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura w Łodzi
ul. Kilińskiego 210, 90-980 Łódź
T +48 42 239 32 00, F +48 42 239 32 90
llo@nik.gov.pl

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli

P/18/006 – Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego.

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli Delegatura w Łodzi.

Kontroler

Stanisław Wlazło główny specjalista kontroli państwowej, upoważnienie do kontroli nr LLO/101/2018 z dnia 2 lipca 2018 r.

(dowód: akta kontroli str. 1)

Jednostka kontrolowana

Urząd Miejski Kamieńsk, ul. Wieluńska 50, 97-360 Kamieńsk (zwany dalej „Urzędem").

Kierownik jednostki kontrolowanej

Bogdan Pawłowski, Burmistrz Kamieńska od dnia 5 grudnia 2014 r.

(dowód: akta kontroli str. 2-4)

Wykaz skrótów i objaśnienie pojęć użytych w wystąpieniu:

- RODO – 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)[1];
- rozporządzenie KRI – 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[2];
- Administrator – zgodnie z definicją zawartą w RODO oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
- Administrator Bezpieczeństwa Informacji, ABI – osoba nadzorująca, z upoważnienia Administratora, przestrzeganie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych;
- Administrator Systemów Informatycznych, ASI lub Informatyk – osoba odpowiedzialna za funkcjonowanie systemu (-ów) lub sieci informatycznych oraz za przestrzeganie zasad i wymagań bezpieczeństwa systemów i sieci informatycznych;
- incydent – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają prawdopodobieństwo zakłócenia działań biznesowych i zagrażają zachowaniu bezpieczeństwa informacji;
- Inspektor Ochrony Danych, IOD – wyznaczany w związku z art. 37 RODO. Zasadniczą rolą inspektorów ochrony danych jest doradzanie administratorowi danych i weryfikacja prawidłowości wykonywania obowiązków wynikających z przepisów prawa dotyczących przetwarzania danych;

---

[1] Dz. Urz. UE L 119 z 4 maja 2016 r., str. 1. Tekst rozporządzenia dostępny pod adresem: https://eur-lex.europa.eu/legal-content/PL/TXT/?qid=1527242776060&uri=CELEX:32016R0679.

[2] Dz. U. z 2017 r. poz. 2247.

- Polityka Bezpieczeństwa Informacji, PBI – zbiór reguł i procedur określających organizację i zarządzanie bezpieczeństwem informacji w jednostce;
- System Zarządzania Bezpieczeństwem Informacji, SZBI – system stanowiący część całościowego systemu zarządzania, zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

II. Ocena kontrolowanej działalności

Ocena ogólna i jej uzasadnienie

Najwyższa Izba Kontroli ocenia negatywnie działania podejmowane przez Burmistrza Kamieńska w zakresie zarządzania bezpieczeństwem informacji. Powyższą ocenę uzasadnia fakt, że pomimo przyjęcia i wdrożenia rozwiązań organizacyjno – technicznych w celu zapewnienia bezpieczeństwa informacji, w działalności Urzędu stwierdzono nieprawidłowości, które w ocenie NIK miały kluczowy wpływ na zapewnienie bezpieczeństwa informacji. Stwierdzone nieprawidłowości polegały na:

- niezapewnieniu utrzymania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującej ich rodzaj i konfigurację, co było niezgodne z § 20 ust. 2 pkt 2 rozporządzenia KRI;
- posiadaniu przez wszystkich skontrolowanych pracowników Urzędu (10) uprawnień administracyjnych na użytkowanych przez nich komputerach, co było niezgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI;
- niespełnianiu wymagań w zakresie złożoności haseł przez dwa systemy informatyczne, co było niezgodne z § 3 ust. 1 pkt 8 obowiązującej w Urzędzie Polityki Bezpieczeństwa Teleinformatycznego;
- nieprzeprowadzeniu w 2017 r. audytu bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI.

NIK zauważa, że w trakcie kontroli zostały podjęte działania w celu usunięcia stwierdzonych nieprawidłowości polegające m.in. na dostosowaniu jednego z systemów w zakresie złożoności haseł do Polityki Bezpieczeństwa Teleinformatycznego.

W Urzędzie została opracowana dokumentacja składająca się na System Zarządzania Bezpieczeństwem Informacji, w tym Polityka Bezpieczeństwa Informacji oraz szczegółowe procedury i instrukcje. Pracownicy Urzędu zostali zapoznani z obowiązującymi w Urzędzie wymogami w zakresie bezpieczeństwa informacji. Burmistrz, zgodnie z wymogami określonymi w RODO, powołał Inspektora Ochrony Danych i umożliwił mu realizację zadań w sposób niezależny. Osoba pełniąca tę funkcję, posiadała odpowiednie przygotowanie merytoryczne i doświadczenie zawodowe. Prowadzono aktualizację oprogramowania systemowego, zabezpieczono komputery programem antywirusowym przed szkodliwym oprogramowanie oraz sporządzano i weryfikowano prawidłowość kopii zapasowych. Spełniono wymóg przechowywania kopii poza miejscem ich wytwarzania. Zapewniono szkolenia dla pracowników w związku z wejściem w życie przepisów RODO.

III. Opis ustalonego stanu faktycznego

1. Organizacja bezpieczeństwa informacji

Opis stanu faktycznego

1.1. Stosownie do § 20 ust. 1 rozporządzenia KRI, w Urzędzie zostały opracowane i zatwierdzone regulacje wewnętrzne składające się na System Zarządzania Bezpieczeństwem Informacji. Z dniem 9 lipca 2018 r. w Urzędzie została wdrożona Polityka Bezpieczeństwa Informacji[3], o której mowa w § 20 ust. 3 w związku z ust. 1 rozporządzenia KRI. Pracownicy Urzędu zostali zapoznani z dokumentami wchodzącymi w skład SZBI oraz zobowiązani do stosowania zasad określonych w tych dokumentach.

Obowiązki w zakresie wdrożenia, oceny, przeglądu i modyfikacji PBI zostały przydzielone IOD.

Obowiązujące w Urzędzie do dnia 8 lipca 2018 r. Polityka Bezpieczeństwa Danych Osobowych oraz Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych[4] dotyczyły bezpieczeństwa danych osobowych.

(dowód: akta kontroli str. 5-156)

1.2 – 1.3. Obowiązująca w Urzędzie Polityka Bezpieczeństwa Informacji uwzględniała wymogi RODO. W związku z wejściem w życie RODO na tablicy informacyjnej Urzędu oraz w Biuletynie Informacji Publicznej została zamieszczona Klauzula informacyjna o przetwarzaniu danych osobowych w Urzędzie. Uruchomiono także skrzynkę e-mail do kontaktu z wyznaczonym w Urzędzie IOD. Ponadto opracowano wzory: wniosku o nadanie/zmianę/usunięcie upoważnienia do przetwarzania danych osobowych, ewidencji osób upoważnionych do przetwarzania danych osobowych, upoważnienia do przebywania w obszarze przetwarzania danych, ewidencji obszarów przetwarzania, umów powierzenia przetwarzania danych osobowych, klauzuli poufności podmiotu zewnętrznego, względem informacji, które zdobędzie na każdym etapie współpracy z Urzędem.

(dowód: akta kontroli str. 5-79, 157-158)

1.4. W Urzędzie wyznaczono pracownika na stanowisko odpowiedzialne za bezpieczeństwo informacji, tj. Administratora Bezpieczeństwa Informacji (do 24 maja 2018 r.) i Inspektora Ochrony Danych (od 25 maja 2018 r.). Podstawowe zadania ABI zostały określone w regulaminie organizacyjnym Urzędu[5] i zakresie czynności pracownika, natomiast zadania IOD w zarządzeniu Burmistrza[6].

ABI posiadał niezbędne kompetencje do pełnienia powierzonych mu zadań z zakresu bezpieczeństwa informacji poparte wykształceniem, praktyką zawodową i odpowiednimi szkoleniami, w tym w zakresie RODO.

(dowód: akta kontroli str. 159-202)

1.5. Zgodnie z art. 37 ust. 1 lit. a) RODO, w dniu 25 maja 2018 r. w Urzędzie został wyznaczony Inspektor Ochrony Danych. Pracownik pełniący tę funkcję posiadał niezbędne kwalifikacje, wynikające z art. 37 ust. 5 RODO. Osoba ta pełniła wcześniej funkcję ABI.

(dowód: akta kontroli str. 159-162)

1.6. W zmienionym w dniu 23 maja 2018 r. Regulaminie Organizacyjnym Urzędu[7] wyodrębniono Inspektora Ochrony Danych jako oddzielne stanowisko, podlegające

---

[3] Wprowadzona zarządzeniem Nr 53/18 Burmistrza Kamieńska z dnia 9 lipca 2018 r

[4] Zarządzenie nr 52/15 Burmistrza Kamieńska z dnia 30 września 2015 r.

[5] Zarządzenie Nr 18/17 Burmistrza Kamieńska z dnia 23 marca 2017 r. w sprawie Regulaminu Organizacyjnego Urzędu Miejskiego w Kamieńsku.

[6] Zarządzenie Nr 28/18 z dnia 23 maja 2018 r. w sprawie wyznaczenia inspektora ochrony danych.

[7] Zarządzenie Nr 27/18 Burmistrza Kamieńska z dnia 23 maja 2018 r. w sprawie zmiany zarządzenia Nr 18/17 Burmistrza Kamieńska z dnia 23 marca 2017 r. w sprawie Regulaminu Organizacyjnego Urzędu Miejskiego w Kamieńsku.

bezpośrednio Burmistrzowi. Zakres zadań IOD został określony w zarządzeniu Burmistrza dotyczącym wyznaczenia pracownika na to stanowisko. Spełniono tym samym wymóg art. 38 ust. 1 RODO. Osoba będąca IOD realizowała inne zadania w ramach zatrudnienia na stanowisku Zastępcy Kierownika Urzędu Stanu Cywilnego w Kamieńsku. Wykonywanie tych obowiązków nie wywołało konfliktu interesów, o którym mowa w art. 38 ust. 6 RODO.

(dowód: akta kontroli str. 203-205)

1.7. W ramach wdrożenia PBI sporządzono niżej wskazaną dokumentację zawierającą polityki i procedury, określające m.in. szczegółowe zasady wdrożenia zabezpieczeń technicznych:

- Politykę Bezpieczeństwa Danych Osobowych,
- Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych,
- Politykę Bezpieczeństwa Informacji, w której określono m.in. procedurę zastosowania monitoringu, zasady zarządzania bezpieczeństwem fizycznym, procedurę powierzenia danych osobowych, procedurę zarządzania incydentami,
- Politykę Bezpieczeństwa Teleinformatycznego, zawierającą m.in. zasady nadawania i wycofywania uprawnień do przetwarzania danych w systemie teleinformatycznym, procedury rozpoczęcia i zakończenia pracy przez użytkownika w systemie informatycznym, określenie środków bezpieczeństwa przed szkodliwym oprogramowaniem, zasady postępowania z urządzeniami mobilnymi, tworzenia kopii zapasowych, nadzór nad oprogramowaniem i postępowanie z nośnikami.
- zasady zapewnienia ciągłości działania i plan zachowania ciągłości działania: instrukcję bezpieczeństwa pożarowego, instrukcję działania Stanowiska Kierowania Burmistrza Kamieńska, instrukcję technicznego przystosowania oraz przemieszczenia Urzędu Gminy na stanowisko kierowania w zapasowym miejscu.
- Instrukcję postępowania z kluczami oraz zabezpieczenia pomieszczeń Urzędu.

(dowód: akta kontroli str. 5-156, 210)

1.8. Regulacje wewnętrzne stanowiące dokumenty wykonawcze PBI były dostępne dla wszystkich pracowników Urzędu, nie tylko dla osób odpowiedzialnych za realizację poszczególnych czynności wymaganych tymi dokumentami. Dokumenty SZBI publikowane były w sieci wewnętrznej Urzędu. (opisano w części „Uwagi").

(dowód: akta kontroli str. 206-209)

1.9. W Urzędzie zidentyfikowano zbiory danych Urzędu podlegających przetwarzaniu i zabezpieczeniu. Powyższe dane zawarte zostały w rejestrze czynności przetwarzania, identyfikującym m.in. kategorie osób, których dane dotyczą, informacje jakie są w posiadaniu Urzędu, w jakim zbiorze się znajdują, jaki jest ich cel przetwarzania, oznaczenie odbiorcy lub odbiorców danych, którym powyższe informacje mogą być przekazywane, rodzaj zastosowanych środków ochrony danych.

(dowód: akta kontroli str. 41-60)

1.10. Urząd nie posiadał aktualnej informacji dotyczącej zasobów informatycznych jednostki w zakresie posiadanego sprzętu informatycznego i jego konfiguracji. (dalszy opis w części „Ustalone nieprawidłowości"). Ewidencja zasobów informatycznych Urzędu prowadzona była w pliku Excel i obejmowała dane w zakresie sprzętu informatycznego i jego konfiguracji w odniesieniu do 6 zestawów komputerowych, co stanowiło zaledwie 17,6% użytkowanych w Urzędzie na dzień kontroli urządzeń.

(dowód: akta kontroli str. 211-218)

Ustalone nieprawidłowości

W działalności Urzędu w zakresie organizacji bezpieczeństwa informacji stwierdzono następującą nieprawidłowość:

W Urzędzie nie zapewniono utrzymania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującej ich rodzaj i konfigurację, co było niezgodne z § 20 ust. 2 pkt 2 rozporządzenia KRI.
Burmistrz Kamieńska wyjaśnił, że brak aktualnej ewidencji był wynikiem natłoku obowiązków. Wskazał ponadto, że w najbliższym czasie ewidencja zostanie uzupełniona o brakujące informacje.
NIK zauważa, że zakres informacji dostępnych w prowadzonym w Urzędzie rejestrze zasobów informatycznych jest niewystarczający, gdyż nie zawiera aktualnych informacji o posiadanych zasobach informatycznych, w tym ich rodzaju i konfiguracji, a zatem nie będzie możliwe sprawne odtworzenie infrastruktury informatycznej Urzędu w przypadku wystąpienia katastrofy lub innego zdarzenia losowego.

(dowód: akta kontroli str. 211-218, 429-435)

Uwagi dotyczące badanej działalności

Opracowane w ramach SZBI szczegółowe uregulowania, dotyczące: nadawania/cofania uprawnień oraz zarządzania bezpieczeństwem w systemach teleinformatycznych, w tym m.in. tworzenia kopii zapasowych i ochrony systemu przed szkodliwym oprogramowaniem zostały udostępnione wszystkim pracownikom Urzędu. NIK zwraca uwagę, że szczegółowe informacje w tym zakresie powinny być udostępniane pracownikom jedynie w zakresie niezbędnym do prawidłowej realizacji przypisanych im zadań. Udostępnienie ich wszystkim pracownikom stwarza bowiem ryzyko wykorzystania informacji do przełamania ustanowionych w Urzędzie zabezpieczeń.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonej nieprawidłowości działania Burmistrza w zakresie organizacji bezpieczeństwa informacji.

2. Wdrożone i wykorzystywane rozwiązania organizacyjne i techniczne zapewniające bezpieczeństwo informacji

Opis stanu faktycznego

2.1. W Polityce Bezpieczeństwa Teleinformatycznego określone zostały ograniczenia dotyczące instalacji i wykorzystywania oprogramowania przez pracowników. Na podstawie oględzin 10 komputerów ustalono, że zalogowani do nich użytkownicy mieli przyznane uprawnienia administracyjne, umożliwiające instalację dowolnego oprogramowania (opisano w części „Ustalone nieprawidłowości").

(dowód: akta kontroli str. 80-101, 282-311)

2.2. Zasady nadawania/cofania uprawnień do pracy w systemach informatycznych, określone zostały w Polityce Bezpieczeństwa Teleinformatycznego. Analiza zadań służbowych realizowanych przez 15 pracowników wykazała, że wszyscy, zgodnie z § 20 ust. 2 pkt 4 rozporządzenia KRI, uczestniczyli w procesie przetwarzania informacji w stopniu adekwatnym do realizowanych przez nich zadań.

(dowód: akta kontroli str. 219-223)

2.3. W badanym okresie pracę w Urzędzie zakończyły 3 osoby, które w czasie zatrudnienia wykonywały zadania w systemach informatycznych, w tym jedna w systemie, do którego logowanie następowało za pomocą karty z certyfikatem. Po zakończeniu zatrudnienia karta została zwrócona Burmistrzowi Kamieńska. W przypadku dwóch pozostałych osób badanie wykazało, że konta tych osób po ustaniu zatrudnienia zostały zablokowane. Było to zgodne z § 20 ust. 2 pkt 7 rozporządzenia KRI. Ww. osoby posiadały pisemne upoważnienia do przetwarzania danych w tych systemach wydane na czas trwania zatrudnienia w Urzędzie.

(dowód: akta kontroli str. 224-229)

2.4. W systemach informatycznych Urzędu w celu zapewnienia ochrony przetwarzanych informacji przed nieuprawnionym dostępem wprowadzono zabezpieczenia polegające na konieczności logowania się do systemu (identyfikator i hasło). Wymogi dotyczący złożoności haseł do systemów informatycznych zostały określone w Polityce Bezpieczeństwa Teleinformatycznego. W wyniku badania trzech systemów informatycznych w Urzędzie ustalono, że wymogi wynikające z powyższej Polityki zostały wdrożone w jednym systemie (SELWIN), natomiast w dwóch systemach („GOMIG – ODPADY" i oprogramowanie „Pakiet dla Administracji") do dnia 3 września 2018 r. zasady w zakresie złożoności haseł nie spełniały tych wymogów (dalszy opis w części „Ustalone nieprawidłowości").

(dowód: akta kontroli str. 80-101, 230-234, 278)

Badanie 10 stanowisk komputerowych pod kątem stosowanych przez użytkowników haseł dostępu wykazało, że we wszystkich przypadkach użytkownicy logując się do komputerów wprowadzali hasła, które spełniały wymogi w zakresie minimalnej liczby znaków.

(dowód: akta kontroli str. 230-232)

2.5. Na pięciu stanowiskach pracy realizujących zadania z zakresu rejestracji stanu cywilnego, ewidencji ludności, wydawania dowodów osobistych, ewidencji i wymiaru podatków oraz opłat z tytułu gospodarowania odpadami komunalnymi, monitory pracowników zostały usytuowane w sposób uniemożliwiający interesantom wgląd do wyświetlanych danych. Powyższe działanie spełniało wymogi określone w § 20 ust. 2 pkt 7 rozporządzenia KRI.

(dowód: akta kontroli str. 236)

2.6. Stosownie do § 20 ust. 2 pkt 8 rozporządzenia KRI w Urzędzie ustanowiono zasady umożliwiające bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość. Pracownicy korzystający ze sprzętu zostali zapoznani z powyższymi uregulowaniami i zobowiązani do ich stosowania.

(dowód: akta kontroli str. 80-101, 139-156, 206-209)

2.7. W Polityce Bezpieczeństwa Teleinformatycznego uregulowano zagadnienia dotyczące zabezpieczenia kryptograficznego w systemach teleinformatycznych. Wskazano w niej, że wprowadzenie takiego zabezpieczenia jest wykonywane z zachowaniem m.in. takich warunków jak adekwatność zabezpieczenia wobec przetwarzanych informacji. Burmistrz Kamieńska wyjaśnił, że w Urzędzie dyski twarde komputerów przenośnych nie były szyfrowane, gdyż komputery wykorzystywane były jako stacjonarne i nie były wynoszone poza siedzibę Urzędu.

(dowód: akta kontroli str. 80-101, 424-428)

2.8. W serwerowni Urzędu zapewniono rozwiązania w zakresie podtrzymania zasilania oraz warunków środowiskowych pracy serwera i urządzeń sieciowych. Zastosowane rozwiązania zabezpieczały to pomieszczenie przed nieuprawnionym ujawnieniem informacji będących w posiadaniu Urzędu, modyfikacją, usunięciem lub ich zniszczeniem.

(dowód: akta kontroli str. 238-240)

2.9. Analiza czterech umów dotyczących usług serwisowych dostarczonego oprogramowania obowiązujących w badanym okresie (100% umów w tym zakresie) wykazała, że zawarte w nich zostały stosowne zapisy dotyczące zachowania poufności informacji uzyskanych w związku z realizacją umów, co było zgodne z § 20 ust. 2 pkt 10 rozporządzenia KRI.

(dowód: akta kontroli str. 241-262)

2.10. Zasady dotyczące postępowania w przypadku przekazywania sprzętu informatycznego poza jednostkę, np. w celu wykonania napraw, zostały określone w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (rozdział XXII). Przewidziano w niej przed przekazaniem sprzętu do serwisu m.in. nieodwracalne usunięcie danych, a jeśli wiązałoby się to

z nadmiernymi utrudnieniami, to po podpisaniu umów powierzenia przetwarzania danych osobowych. W obowiązującej Polityce Bezpieczeństwa Teleinformatycznego brak było szczegółowych uregulowań w tym zakresie. Burmistrz Kamieńska wyjaśnił, że w przypadku serwisu jednostek komputerowych, sprzęt dostarcza się do serwisu po pozbawieniu go dysku twardego.

(dowód: akta kontroli str. 5-79, 139-156, 424-428)

2.11. Stosownie do § 20 ust. 2 pkt 12 lit. a i f rozporządzenia KRI w Urzędzie przeprowadzano aktualizacje systemów operacyjnych. Stwierdzono jednak przypadki wykorzystywania systemów operacyjnych nieobjętych wsparciem producenta – Windows XP (opisano w części „Uwagi")

(dowód: akta kontroli str. 263)

2.12. Zasady dotyczące tworzenia i przechowywania kopii zapasowych danych w Urzędzie zostały określone w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, a następnie po wejściu w życie przepisów RODO w Polityce Bezpieczeństwa Teleinformatycznego. Ustalono, że ostatnie kopie zapasowe wykonano zgodnie z harmonogramem. Kopie sporządzane były ręcznie przez informatyka Urzędu na dysku zewnętrznym i przechowywane w szafie zamkniętej na klucz, znajdującej się w pomieszczeniu poza serwerownią. W badanym okresie wystąpił jeden przypadek konieczności odtworzenia danych z kopii. Odtworzenie zakończyło się z wynikiem pozytywnym.

Burmistrz Kamieńska wyjaśnił, że kopie zapasowe były testowane i nigdy nie stwierdzono błędów lub nieprawidłowości danych.

Przyjęte rozwiązania i działania w ww. zakresie zapewniały zgodność z wymogami określonymi w § 20 ust. 2 pkt 7 oraz ust. 2 pkt 12 lit. b i e rozporządzenia KRI.

(dowód: akta kontroli str. 80-156, 264-268, 424-428)

2.13. Oględziny 10 komputerów wykazały, że był na nich zainstalowany i uruchomiony program antywirusowy, który wykorzystywał aktualną na moment oględzin wersję bazy definicji wirusów. Było to zgodne z § 20 ust. 2 pkt 12 lit. f rozporządzenia KRI.

(dowód: akta kontroli str. 269-279)

2.14. W ramach obowiązujących w Urzędzie uregulowań, nie zostały określone zasady monitorowania stanu pojemności przestrzeni dyskowej w serwerze Urzędu. Ustalono, że stosownie do zalecenia sformułowanego w punkcie A.12.1.3 załącznika A normy PN-ISO/IEC 27001-2017, pojemność była na bieżąco monitorowana przez informatyka.

Oględziny serwera wykorzystywanego w Urzędzie wykazały jednak dużą zajętość jego przestrzeni dyskowej (opisano w części „Uwagi").

(dowód: akta kontroli str. 280-281)

2.15. Burmistrz Kamieńska wyjaśnił, że procesy związane z aktualizacją oprogramowania występują w postaci zautomatyzowanej i ręcznej. Proces zautomatyzowany dotyczy oprogramowania biurowego oraz antywirusowego. W przypadku ręcznej aktualizacji występuje ona tylko w przypadku poprawek krytycznych bądź ważnych aktualizacji, które klasyfikowane są przez ASI w oparciu o jego wiedzę i doświadczenie. Zmiany ingerujące w integralność, dostępność i poufność sieci IT są najpierw sprawdzane i testowane przez ASI. ASI po podjęciu decyzji o wprowadzeniu rozwiązania (po uprzedniej konsultacji z najwyższym kierownictwem) wprowadza rozwiązanie, monitoruje je, zapewnia ciągłość działania oraz komunikowanie o zmianach.

(dowód: akta kontroli str. 429-432)

2.16. Stosownie do art. 30 RODO, w Urzędzie prowadzony był rejestr czynności przetwarzania. Rejestr zawierał informacje, wynikające z art. 30 RODO. Dokument ten został udostępniony pracownikom w sieci wewnętrznej Urzędu.

(dowód: akta kontroli str. 41-60)

Ustalone nieprawidłowości

W działalności Urzędu w zakresie wdrożonych i wykorzystywanych rozwiązań organizacyjnych i technicznych zapewniających bezpieczeństwo informacji, stwierdzono następujące nieprawidłowości:

1. Oględziny 10 komputerów wykazały, że zalogowani do nich użytkownicy posiadali przyznane uprawnienia administracyjne, umożliwiające im instalację dowolnego oprogramowania. Było to niezgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI.
   Burmistrz Kamieńska wyjaśnił, że każdy użytkownik systemu komputerowego zapoznany został z dokumentacją dotyczącą bezpieczeństwa informacji i odpowiadał za oprogramowanie zainstalowane na swoim komputerze. Wskazał ponadto, że w Urzędzie stosowany był zintegrowany system bezpieczeństwa, zapewniający m.in. filtrowanie treści www, ochronę przed atakami, spamem oraz wyciekiem informacji poufnej. Burmistrz wskazał także, że w najbliższym czasie planowana jest w Urzędzie zmiana uprawnień ograniczających dostęp użytkowników do systemu.
   (dowód: akta kontroli str. 282-311, 424-428)
2. Zasady w zakresie złożoności haseł w systemach: „Gomig - Odpady" i „Pakiet dla Administracji" nie spełniały wymogów określonych w § 3 ust. 1 pkt 8 Polityki Bezpieczeństwa Teleinformatycznego, gdyż w ustawieniach programów brak było odpowiednio wymogu znaku specjalnego dla hasła oraz wymagań jakie znaki powinno zawierać hasło. Burmistrz Kamieńska wyjaśnił, że na wszystkich stanowiskach z wykorzystaniem ww. systemów użytkownicy posiadali własne indywidualne hasła, ważne przez okres 30 dni, po którym programy wymuszały na użytkowniku zmianę hasła. W każdym przypadku minimalna długość haseł wynosiła 8 znaków. Burmistrz wyjaśnił, że opcje programu „Pakiet dla Administracji" w zakresie złożoności haseł zostały w trakcie kontroli NIK zmienione i dostosowane do Polityki Bezpieczeństwa Teleinformatycznego, natomiast w przypadku programu Gomig-Odpady trwają prace producenta nad systemem, które umożliwią wymuszanie hasła ze znakiem specjalnym.
   (dowód: akta kontroli str. 230-235, 424-428)

Uwagi dotyczące badanej działalności

1. Ustalono, że dyski twarde komputerów przenośnych wykorzystywanych przez pracowników Urzędu nie były szyfrowane.

Jak wskazał Burmistrz Kamieńska komputery wykorzystywane były jako stacjonarne i nie były wynoszone poza siedzibę Urzędu.

NIK zawraca uwagę, że podstawową funkcją urządzeń mobilnych jest praca w dowolnym miejscu z wykorzystaniem technik komunikacyjnych. A zatem nie można wykluczyć, że praca może być niekiedy wykonywana również poza siedzibą Urzędu, co powoduje szereg zagrożeń dla bezpieczeństwa danych na nich zgromadzonych (np. kradzież, zagubienie). Dzięki szyfrowaniu dysków twardych urządzeń przenośnych, w przypadku ich kradzieży lub zagubienia, osoby trzecie nie będą miały dostępu do danych na nich zgromadzonych.

(dowód: akta kontroli str. 424-428)

2. Na 12 komputerach spośród 34 użytkowanych w Urzędzie (35,3%) zainstalowany był system operacyjny Windows XP. NIK zwraca uwagę, że system ten nie posiadał wsparcia producenta, a tym samym jego użytkowanie zwiększało ryzyko bezpieczeństwa przetwarzania informacji.

3. Oględziny serwera wykorzystywanego w Urzędzie wykazały, że zajętość przestrzeni dyskowej na serwerze wynosiła 96%. NIK zwraca uwagę, że zbyt duża zajętość pojemności dyskowej może mieć wpływ na utrudnienie pracy

użytkowników, w tym obniżenie wydajności pracy serwera lub też zatrzymanie jego funkcjonowania.

(dowód: akta kontroli str. 263, 280-281)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie wdrożone i wykorzystywane w Urzędzie rozwiązania organizacyjne i techniczne, zapewniające bezpieczeństwo informacji. Powyższą ocenę uzasadnia przyznanie pracownikom Urzędu praw administracyjnych do użytkowanych przez nich komputerów, przez co możliwe było zainstalowanie na nich nieautoryzowanego oprogramowania oraz niedostosowanie zasad złożoności haseł w części skontrolowanych systemów.

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

3.1. W okresie objętym kontrolą w Urzędzie przeprowadzono analizę ryzyka związanego z bezpieczeństwem informacji, co było zgodne z § 20 ust. 2 pkt 3 rozporządzenia KRI. W ramach analizy dokonano m.in. określenia aktywów informacyjnych Urzędu, identyfikacji ryzyk, oceny ryzyka, jego poziomu, sposobów reakcji na ryzyko oraz planu postępowania z ryzykiem. W dokumentacji dotyczącej bezpieczeństwa informacji uwzględniono fakt, że prowadzenie analizy ryzyka jest procesem ciągłym.

(dowód: akta kontroli str. 312-397)

3.2 W Urzędzie zapewniono możliwość bezzwłocznego zgłaszania incydentów w zakresie bezpieczeństwa informacji i danych osobowych przez pracowników. Do dnia 8 lipca 2018 r. w Urzędzie obowiązywały zasady zarządzania incydentami bezpieczeństwa informacji i postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa zawarte w Polityce Bezpieczeństwa danych osobowych oraz Instrukcji zarządzania systemem informatycznym. Z dniem 9 lipca 2018 r. wprowadzono w Urzędzie Procedurę Zarządzana Incydentami[8] w celu monitorowania procesów związanych z koniecznością zapewnienia bezpieczeństwa informacji.

Wszyscy pracownicy Urzędu zostali zapoznani z powyższymi uregulowaniami i zobowiązani do ich stosowania.

Burmistrz Kamieńska wyjaśnił, że w badanym okresie w Urzędzie nie odnotowano incydentów związanych z naruszeniem bezpieczeństwa informacji.

(dowód: akta kontroli str. 5-156, 206-209, 424-428)

3.3. Stosownie do § 20 ust. 2 pkt 6 rozporządzenia KRI, w Polityce Bezpieczeństwa Informacji określono wymogi dotyczące realizacji szkoleń pracowników w zakresie bezpieczeństwa informacji. Ponadto wymogi pracowników tym zakresie określone były w obowiązującej do dnia 8 lipca 2018 r. Polityce Bezpieczeństwa Danych Osobowych.

W badanym okresie pracownicy Urzędu w czerwcu 2018 r. odbyli szkolenie z zakresu bezpieczeństwa informacji, w tym RODO. W szkoleniu udział wzięli wszyscy pracownicy Urzędu. Szkolenie przeprowadziła firma zewnętrzna. Burmistrz Kamieńska wyjaśnił ponadto, że w badanym okresie zagadnienia ochrony danych podnoszone były przez kierownictwo Urzędu przy okazji różnych spotkań merytorycznych z pracownikami.

W 2018 r. Administrator Bezpieczeństwa Informacji uczestniczył indywidualnie w trzech szkoleniach zewnętrznych dotyczących ochrony danych osobowych, w tym w zakresie RODO.

(dowód: akta kontroli str. 5-156, 199-202, 398-410)

[8] Procedura zawarta została w Polityce Bezpieczeństwa Informacji stanowiącej załącznik nr 1 do zarządzenia nr 53/18 Burmistrza Kamieńska z dnia 9 lipca 2018 r. w sprawie wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji.

3.4. W 2018 r. w Urzędzie został przeprowadzony audyt wewnętrzny z zakresu bezpieczeństwa informacji. W 2017 r. nie zapewniono natomiast audytu w powyższym zakresie (opisano w części „Ustalone nieprawidłowości").

(dowód: akta kontroli str. 409-423)

3.5. W związku z wejściem w życie przepisów RODO w Urzędzie dokonano analizy procesów przetwarzania danych osobowych i oceny stopnia ich bezpieczeństwa w stosunku do stwierdzonych ryzyk – zgodnie z wymogami art. 32 ust. 1 RODO.

(dowód: akta kontroli str. 312-397)

Ustalone nieprawidłowości

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

W 2017 r. w Urzędzie nie został przeprowadzony audyt z zakresu bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI. Burmistrz Kamieńska wyjaśnił, że w Urzędzie nigdy nie stwierdzono wycieku danych, dlatego też wydawało się niezasadne przeprowadzenie takiego audytu.

NIK nie podziela stanowiska przedstawionego w wyjaśnieniach i wskazuje, że § 20 ust. 2 pkt 14 nakłada obowiązek zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji nie rzadziej niż raz na rok. Obowiązek ten nie jest zatem uzależniony od wystąpienia zdarzenia polegającego na wycieku danych, czy też innego zdarzenia losowego mającego wpływ na bezpieczeństwo informacji. W związku z przeprowadzeniem w 2018 r. audytu, NIK odstępuje od formułowania wniosku pokontrolnego w tym zakresie.

(dowód: akta kontroli str. 424-428)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie działania Urzędu w zakresie zapobiegania incydentom bezpieczeństwa informacji, ze względu na nieprzeprowadzenie w 2017 r. audytu bezpieczeństwa informacji.

IV. Wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny i uwagi wynikające z ustaleń kontroli, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[9], wnosi o:

1. Prowadzenie aktualnej i kompletnej elektronicznej ewidencji sprzętu informatycznego, obejmującej jego rodzaj i konfigurację.
2. Dostosowanie liczby administratorów systemu oraz parametrów haseł dostępu do wymogów systemu bezpieczeństwa informacji.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

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

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 Łodzi.

[9] Dz. U. z 2017 r., poz. 524 ze zm., dalej „ustawa o NIK".

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK proszę o poinformowanie Najwyższej Izby Kontroli, w terminie 21 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag i wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

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

Łódź, dnia 14 września 2018 r.

Najwyższa Izba Kontroli
Delegatura w Łodzi

Kontroler
Stanisław Wlazło
Główny specjalista kontroli państwowej

.....
podpis

Dyrektor
Przemysław Szewczyk

.....
podpis