NAJWYŻSZA IZBA KONTROLI
Delegatura w Łodzi

LLO.410.013.01.2018
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
Kontrolerzy	Marek Tarnawski – doradca techniczny, upoważnienie do kontroli nr LLO/113/2018 z dnia 23 lipca 2018 r. [akta kontroli str. 1-2]
Jednostka kontrolowana	Starostwo Powiatowe w Brzezinach, ul. Sienkiewicza 16, 95-060 Brzeziny
Kierownik jednostki kontrolowanej	Edmund Kotecki – Starosta Brzeziński, wybrany w dniu 1 grudnia 2014 r. [akta kontroli str. 3]
Okres objęty kontrolą	Od 1 czerwca 2017 r. do dnia zakończenia czynności kontrolnych w jednostce, tj. do 7września 2018 r.

Wykaz skrótów i objaśnienie pojęć użytych w wystąpieniu:

- 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[1];
- 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)[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 danych osobowych przestrzeganie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych;
- Administrator Systemów Informatycznych, ASI – 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

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

[2] 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

z przepisów prawa dotyczących przetwarzania danych;
- Polityka Bezpieczeństwa Informacji, PBI – zbiór reguł i procedur określających organizację i zarządzanie bezpieczeństwem informacji w jednostce;
- System Zarządzania Bezpieczeństwem Informacji, SZBI – system stanowiący cześć 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[3] działalność Starosty w zakresie zarządzania bezpieczeństwem informacji. W działalności Urzędu stwierdzono szereg nieprawidłowości, w tym m.in.:
- nie opracowano kompletnego systemu zarządzania bezpieczeństwem informacji, w szczególności kompletnej polityki bezpieczeństwa informacji, co było niezgodne z § 20 ust. 1 w związku z ust. 3 rozporządzenia KRI,
- nie prowadzono inwentaryzacji zasobów informatycznych, która zawierałoby pełne i aktualne informacje w zakresie posiadanego sprzętu informatycznego oraz jego konfiguracji, co było niezgodne z § 20 ust. 2 pkt 2 rozporządzenia KRI,
- nie dokumentowano procesu nadawania uprawnień użytkownikom do pracy w systemach innych, niż służące przetwarzaniu danych osobowych, co było działaniem nierzetelnym,
- nie określono zasad (procedur) dotyczących bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość, co stanowiło naruszenie z § 20 ust. 2 pkt. 8 rozporządzenia KRI, nie została również przyjęta jednolita procedura w zakresie wdrożenia odpowiednich mechanizmów zabezpieczających informacje przechowywane na urządzeniach przenośnych, w celu minimalizowania ryzyka nieuprawnionego dostępu do informacji, co było niezgodne z wymogami § 20 ust. 2 pkt 9 i 11 rozporządzenia KRI,
- w trzech z pięciu badanych umów z podmiotami zewnętrznymi nie zobowiązano wykonawców do zachowania w tajemnicy informacji, do jakich mogą mieć dostęp w związku z realizacją tych umów, co było to niezgodne z § 20 ust. 2 pkt 10 rozporządzenia KRI,
- nie prowadzono cyklicznej analizy ryzyka związanego z bezpieczeństwem informacji, o której mowa w § 20 ust. 2 pkt 3 rozporządzenia KRI,
- nie przeprowadzono w 2017 r. audytu z zakresu bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI,
- w systemach innych niż służące przetwarzaniu danych osobowych zmiana hasła nie była generowana automatycznie i nie była wymuszana przez system (poza programem Płatnik), a zastosowane hasła dostępu nie gwarantowały bezpieczeństwa dostępu do danych przez osoby nieuprawnione. Stanowiło to naruszenie § 20 ust. 2 pkt 7 lit. a i c rozporządzenia KRI.

W Urzędzie prawidłowo realizowano zadania dotyczące m.in.:
- przeprowadzenia aktualizacji *Polityki bezpieczeństwa danych osobowych Urzędu* oraz *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie,* pod kątem dostosowania do wymogów przepisów RODO,
- powołania Inspektora Ochrony Danych i umożliwienia mu realizacji zadań w sposób niezależny, stosownie do art. 37 ust. 1 lit. a *RODO*,

[3] Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.

– zabezpieczenia komputerów programem antywirusowym przed szkodliwym oprogramowaniem, stosownie do § 20 ust. 2 pkt 9 rozporządzenia KRI.

NIK zauważa, że w trakcie kontroli zostały podjęte działania w celu usunięcia stwierdzonych nieprawidłowości, polegające m.in. na zleceniu zewnętrznej firmie audytu z zakresu bezpieczeństwa informacji oraz opracowania i wdrożenia PBI. Urząd usunął również materiały łatwopalne z serwerowni oraz zabezpieczył klucze do serwerowni.

III. Opis ustalonego stanu faktycznego

1 Organizacja bezpieczeństwa informacji

Opis stanu faktycznego

1.1. W Urzędzie nie zostały opracowane kompletne regulacje wewnętrzne składające się na System Zarządzania Bezpieczeństwem Informacji, wskazane w § 20 ust. 1 rozporządzenia KRI w związku z § 20 ust. 3 rozporządzenia KRI. Obowiązujące w Urzędzie *Polityki bezpieczeństwa danych osobowych Urzędu* oraz *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie* dotyczyły bezpieczeństwa danych osobowych. Zgodnie z wymogami wynikającymi z rozporządzenia KRI, ww. dokumentacja powinna odnosić się do wszystkich danych przetwarzanych w Urzędzie (nie zaś ograniczać do danych osobowych).

[akta kontroli str.: 147-278]

1.2.-1.3. W związku z wejściem w życie przepisów RODO, w Urzędzie przeprowadzono aktualizację *Polityki bezpieczeństwa danych osobowych Urzędu* oraz *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie*[4], pod kątem dostosowania do wymogów tego rozporządzenia.

Ponadto, w Biuletynie Informacji Publicznej zostały zamieszczone klauzule informacyjne dla kontrahentów (klientów, usługodawców)[5], dotyczące przetwarzania i ochrony danych osobowych. Została uruchomiona skrzynka e-mail, służąca do kontaktu z powołanym w Urzędzie IOD[6]. Ponadto, opracowano wzory oświadczeń dla pracowników w zakresie przetwarzania danych osobowych, których podpisane egzemplarze przechowywano w aktach osobowych. Zostały przygotowane wzory umów z kontrahentami, zawierające uregulowania w zakresie administrowania danymi osobowymi, powierzenia ich przetwarzania oraz zabezpieczenia danych.

[akta kontroli, str.: 144-278; 337; 132-133]

1.4. Na podstawie zarządzenia Starosty Brzezińskiego[7] został wyznaczony pracownik Urzędu na stanowisko odpowiedzialne za bezpieczeństwo informacji, tj. Administrator Bezpieczeństwa Informacji.

[akta kontroli str.: 3-5; 17; 334;347;349]

1.5. Zgodnie z art. 37 ust. 1 lit. a) RODO, 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. Starosta przesłał do Urzędu Ochrony Danych Osobowych zawiadomienie o jego wyznaczeniu. Osoba ta pełniła wcześniej funkcję ABI. Zarządzeniem zostały określone podstawowe zakresy obowiązków na tym stanowisku. Pracownik, któremu powierzono funkcje IOD posiadał niezbędne kompetencje do pełnienia powierzonych mu zadań z zakresu

[4] Wprowadzone zarządzeniem nr 14 Starosty Brzezińskiego z dnia 25 maja 2017 r.
[5] http://www.powiat-brzeziny.4bip.pl zakładka polityka prywatności RODO.
[6] iod@powiat-brzeziny.pl
[7] Zarządzenie nr 11 Starosty Brzezińskiego z dnia 5 maja 2017 r. ws. powołania administratora bezpieczeństwa informacji w Starostwie Powiatowym w Brzezinach.

bezpieczeństwa informacji, poparte wykształceniem, praktyką zawodową, szkoleniami i kursami, obejmującymi również problematykę RODO.

[akta kontroli str.: 3-5; 17; 334;347;349]

1.6. W Urzędzie spełniono wymóg art. 38 ust. 1 RODO stanowiący, że IOD podlega bezpośrednio najwyższemu kierownictwu Urzędu tj. Staroście. Pracownik będący IOD realizował w Urzędzie zadania pomocy informatyka. Wykonywanie tych obowiązków nie wywoływało konfliktu interesów, o którym mowa w art. 38 ust. 6 RODO.

[akta kontroli str. 6-9; 342-346]

1.7. W ramach wdrożenia obowiązującej w Urzędzie dokumentacji w zakresie ochrony danych osobowych sporządzono następujące procedury tj.: *Politykę bezpieczeństwa danych osobowych* i *Instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.* Dokumenty te określały sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

[akta kontroli str.: 147-278]

1.8. Regulacje wewnętrzne w zakresie polityki bezpieczeństwa danych osobowych zostały udostępnione kierownictwu Urzędu[8]. Pracownicy Starostwa zostali zapoznani z dokumentacją dotyczącą ochrony danych osobowych na szkoleniach wewnętrznych.

[akta kontroli str. 17; 110-139]

1.9. W Urzędzie sporządzono zestawienie aktywów informacyjnych podlegających ochronie. Informacje posiadane i przetwarzane przez Urząd zostały zidentyfikowane w postaci wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych. Wykaz stanowił załącznik do *Polityki bezpieczeństwa danych osobowych*. W Wykazie określono nazwę zbioru i podzbioru danych osobowych, formę jego przetwarzania, sposób zabezpieczenia informatycznego i fizycznego danych oraz przyjęte zasady organizacyjne dotyczące zabezpieczenia zbiorów.

[akta kontroli str. 186-245]

1.10. W Urzędzie nie prowadzono wymaganej na podstawie § 20 ust. 2 pkt 2 rozporządzenia KRI inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującej ich rodzaj i konfigurację.
Urząd prowadził spis zasobów teleinformatycznych w formie papierowej[9]. Spis zawierał informacje o typie/modelu i oznaczeniu numerycznym oraz usytuowaniu: ruterów z konfiguracją firewall, switch-y, elementów łączności bezprzewodowej, serwerów, stacji roboczych (zestawów z podaniem modelu/firmy i ilości w sztukach), drukarek i kopiarek. Sprzęt był również ewidencjonowany w książkach inwentarzowych Starostwa.

[akta kontroli, str.: 11-12; 142-143; 334]

Ustalone nieprawidłowości

W działalności Urzędu w zakresie organizacji bezpieczeństwa informacji stwierdzono następujące nieprawidłowości:

1. W Urzędzie nie zostały opracowane kompletne regulacje wewnętrzne składające się na system zarządzania bezpieczeństwem informacji, w szczególności nie opracowano kompletnej polityki bezpieczeństwa informacji. Było to niezgodne z § 20 ust. 1 rozporządzenia KRI stanowiącego, że podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda

[8] Naczelnikom wydziałów Starostwa, Pełnomocnikowi ds. ochrony Informacji Niejawnych, radcom pranym oraz Powiatowemu Rzecznikowi Konsumentów i Przewodniczącej Powiatowego Zespołu ds. orzekania niepełnosprawności.

[9] Spis z datą aktualizacji na dzień 31 maja 2018 r.

oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Ponadto, § 20 ust. 3 *rozporządzenia KRI* wskazuje, że wymagania określone w ww. ust. 1 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-EN ISO/IEC 27001[10], a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą[11]. W pkt. 5.1 normy PN-EN ISO/IEC 27002 wskazano opracowanie i stosowanie dokumentu polityki bezpieczeństwa informacji.

Jak wyjaśnił Starosta Powiatu: *W urzędzie niezwłocznie zostanie wdrożona Polityka Bezpieczeństwa Informacji, we współpracy z firmą zewnętrzną (termin wykonania umowy -30 września 2018 r.)*

[akta kontroli str.: 334-337]

2. W Urzędzie nie prowadzono inwentaryzacji zasobów informatycznych, która zawierałaby pełne i aktualne informacje w zakresie posiadanego sprzętu informatycznego oraz jego konfiguracji, co było niezgodne z § 20 ust. 2 pkt 2 *rozporządzenia KRI*.

   Starosta Powiatu wyjaśnił, że w Urzędzie niezwłocznie zostanie zakupione oprogramowanie umożliwiające inwentaryzację i bieżącą aktualizację sprzętu i oprogramowania, które służy do przetwarzania informacji.

   [akta kontroli, str.: 334-337]

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie działania Urzędu w zakresie organizacji bezpieczeństwa informacji. Ocenę uzasadnia brak opracowania kompletnego systemu zarządzania bezpieczeństwem informacji, o którym mowa w § 20 ust. 1 w związku z § 20 ust. 3 rozporządzenia KRI, a także brak prowadzenia wymaganej na podstawie § 20 ust. 2 pkt 2 rozporządzenia KRI inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji.

2 Wdrożone i wykorzystywane rozwiązania organizacyjne i techniczne zapewniające bezpieczeństwo informacji

Opis stanu faktycznego

2.1. W pkt. 9 i 13 *Instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych* zostały określone obowiązki, odpowiedzialność, zasady i ograniczenia, dotyczące instalacji i wykorzystania oprogramowania przez pracowników. Na podstawie oględzin 10 użytkowanych komputerów ustalono, że w dziewięciu przypadkach zalogowani do nich użytkownicy nie mieli przyznanych uprawnień administracyjnych umożliwiających instalację dowolnego oprogramowania. W jednym przypadku próba zainstalowania oprogramowania na laptopie wykorzystywanym przez pracownika Wydziału Finansowego Urzędu zakończona została pomyślnie i oprogramowanie zostało zainstalowane.

[akta kontroli str. 10; 256-278; 335]

2.2. *Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych* określała zasady nadawania, aktualizacji i wycofania uprawnień do przetwarzania danych osobowych w systemach informatycznych i rejestrowanie

---

[10] Polska Norma PN-EN ISO/IEC 27001:2017 *Technika Informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania.*

[11] W tym: PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem, PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

tych uprawnień, a także metody i środki uwierzytelnienia użytkowników w systemach informatycznych.
Na podstawie badania próby 15 użytkowników systemów informatycznych ustalono, że wszyscy posiadali uprawnienia do pracy w systemach adekwatne do zakresu realizowanych zadań. Uprawnienia dwóch pracowników w systemach informatycznych, którzy w okresie objętym kontrolą zmienili stanowiska pracy, zostały zmodyfikowane i były zgodne z nowym zakresem obowiązków. Powyższe działania były zgodne z § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI.
Ustalono, że w Urzędzie nie dokumentowano procesu nadawania uprawnień użytkownikom do pracy w systemach innych, niż służące przetwarzaniu danych osobowych, np. *BeSTi@*, itp.

[akta kontroli str.:11-12; 256-285; 335]

2.3. W wyniku badania jedenastu osób, które w okresie objętym kontrolą zakończyły pracę w Urzędzie ustalono, że ich konta w systemach informatycznych zostały zablokowane. Blokowanie kont odbywało się niezwłocznie po otrzymaniu przez administratora systemu informatycznego informacji o zakończeniu przez pracownika zatrudnienia, co było zgodne z *Instrukcją postępowania w przypadku nadawania/cofania uprawnień do pracy w systemie informatycznym* oraz z § 20 ust. 2 pkt 5 rozporządzenia KRI.

[akta kontroli str. 286-287; 329]

2.4. Dla wszystkich systemów działających w Urzędzie zmiana haseł dostępu była wymuszana automatycznie (komputery są zarządzane centralnie w oparciu o mechanizm Microsoft Active Directory[12]). Wymogi dotyczące złożoności haseł do systemów informatycznych zostały określone w *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych*. Ustawiono m.in.: maksymalny okres ważności hasła na 30 dni, minimalną długość hasła na 8 znaków oraz włączono wymagania co do złożoności hasła. Powyższe rozwiązania i wymogi określone w *Instrukcji* były zgodne z § 20 ust. 2 pkt 7 rozporządzenia KRI.
W Urzędzie przy pracy w systemach innych niż służące przetwarzaniu danych osobowych[13] zmiana hasła nie była generowana automatycznie i wymuszana przez system (poza programem Płatnik).

[akta kontroli str.:294-297; 304]

2.5. Na czterech stanowiskach pracy w pomieszczeniach Starostwa, w których realizowano zadania z zakresu rejestracji pojazdów i wydawania praw jazdy, ustawienie monitorów uniemożliwiało odczytanie wyświetlanych danych przez osoby nieuprawnione. Powyższe działanie spełniało wymogi § 20 ust. 2 pkt 7 rozporządzenia KRI.

[akta kontroli str.: 305; 330]

2.6. Urząd nie opracował zasad (procedur) dotyczących bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość, o których mowa w § 20 ust. 2 pkt. 8 rozporządzenia KRI. *Polityka Bezpieczeństwa Danych Osobowych* zawierała ogólne wymogi dotyczące postępowania z komputerami i dyskami przenośnymi nakazując *pilnego strzeżenia nośników danych w tym akt, płyt, pamięci przenośnych i komputerów przenośnych, których nie należy pozostawiać bez kontroli w miejscach w których narażone są na nieuprawnione pozyskanie przez osoby trzecie.*

[dowód: akta kontroli str. 147-255]

2.7. W Urzędzie nie została przyjęta jednolita procedura w zakresie szyfrowania urządzeń przenośnych.

[akta kontroli, str.: 335-336]

---

[12] Umożliwia centralne zarządzanie komputerami.
[13] Program Besti@ - system do sprawozdawczości budżetowej; program – Księgowość budżetowa, Program Vucan i Program Płatnik.

2.8. W serwerowni Urzędu zapewniono rozwiązania w zakresie podtrzymania zasilania oraz warunków środowiskowych pracy serwerów i urządzeń sieciowych. W okresie objętym kontrolą testowano lub serwisowano znajdujące się w pomieszczeniu zasilacze awaryjne i klimatyzator. Część zastosowanych rozwiązań służących zabezpieczeniu serwerowni w niewystarczającym stopniu chroniła pomieszczenie, co zostało skorygowane w trakcie trwania kontroli. W serwerowni znajdowały się także materiały łatwopalne, które zostały wyniesione z tego pomieszczenia do czasu zakończenia kontroli NIK.
W Urzędzie nie zostały zainstalowane zapasowe źródła zasilania sprzętu komputerowego, tj. równoległa linia zasilająca lub agregat prądotwórczy.

[akta kontroli, str.: 306-314; 330; 335; 348]

2.9. Starostwo w okresie objętym kontrolą zawarło pięć umów[14] z zakresu dotyczących dostaw sprzętu informatycznego i/lub świadczenia usług telekomunikacyjnych/serwisowych/utrzymaniowych. Dwie umowy dotyczące obsługi serwisowej, świadczenia i dostawy usług i specjalistycznego oprogramowania komputerowego zawierały zapisy dotyczące zachowania poufności informacji, uzyskanych w związku z ich realizacją. Trzy pozostałe umowy takich zapisów nie zawierały (w tym dwie dotyczące zakupu i dostawy sprzętu komputerowego i systemów operacyjnych).

[akta kontroli str.: 20-45; 435-436]

2.10. W Urzędzie zostały określone zasady dotyczące postępowania w przypadku przekazywania sprzętu informatycznego poza jednostkę, np. w celu wykonania napraw. W *Instrukcji określającej sposób zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych* w pkt. 12 określone zostały zasady bezpiecznego przechowywania, transportu i niszczenia urządzeń oraz innych elektronicznych nośników informacji, zaś w pkt. 15 określone zostały procedury wykonywania napraw, przeglądów i konserwacji systemu informatycznego oraz elektronicznych nośników informacji służących do przetwarzania danych.

[akta kontroli str.: 256-278]

2.11. Stosownie do § 20 ust. 2 pkt 12 lit. a i f rozporządzenia KRI w Urzędzie przeprowadzano aktualizacje systemów operacyjnych. Nie stwierdzono wykorzystywania systemów operacyjnych, nieobjętych wsparciem producenta (np. *Windows XP*).

[akta kontroli str.: 335]

2.12. Zasady dotyczące tworzenia i przechowywania kopii zapasowych danych w Urzędzie zostały określone w pkt. 11 *Instrukcji określającej sposób zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.* Proces tworzenia kopii został zautomatyzowany poprzez zastosowanie systemu informatycznego i skryptów. Kopie serwerów realizowano co 24 godziny, a kopie komputerów klienckich w dni robocze. Kopie były przechowywane poza miejscem ich wytwarzania, tj. w drugiej serwerowni oraz na dyskach twardych zabezpieczonych w zamkniętej szafie w odrębnym pomieszczeniu. W okresie objętym kontrolą nie wystąpiły przypadki konieczności odtworzenia danych z kopii zapasowych.
W Urzędzie nie sporządzono pisemnych procedur testowania kopii zapasowych. Testowanie, według oświadczenia Informatyka Urzędu, realizowane było raz na

[14] 1) Umowa stałej obsługi serwisowej stanowisk komputerowych z dnia 2 listopada 2017 r.; 2) Umowa nr 202/2017 z dnia 05.09.2017 r. na sprzedaż – sześciu sztuk systemów operacyjnych; 3) Umowa nr 201/2017 z dnia 05.09.2017 r .na sprzedaż i dostawę dwóch sztuk zestawów komputerowych wraz z oprogramowaniem operacyjnym; 4) Umowa nr 26/2018 z dnia 25 kwietnia 2018 r. na wykonanie serwisu pogwarancyjnego oprogramowania finansowo-księgowego; 5) Umowa nr 35/2018 z dnia 01.03.2018 r. na dostawę , szkolenie i wsparcie informatyczne we wdrożeniu programu vEdukacja Nabór: szkoły ponadgimnazjalne.

miesiąc. Starosta Powiatu zobowiązał się do niezwłocznego sporządzenia procedury testowania kopii zapasowych.
W Urzędzie brak było rejestru pracowników uprawnionych do dostępu do serwerowni i dysków z kopiami zapasowymi. Rejestr ten został utworzony w trakcie trwania kontroli NIK.

[akta kontroli str.: 256-278; 298-303; 330; 336]

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

[akta kontroli str.: 315-324]

2.14. W ramach obowiązujących w Urzędzie uregulowań nie zostały określone zasady monitorowania stanu pojemności przestrzeni dyskowej w serwerach Urzędu. Ustalono jednak, że stosownie do zalecenia sformułowanego w pkt A.12.1.3 załącznika A normy PN-ISO/IEC 27001:2017, pojemność była na bieżąco monitorowana przez informatyków. W systemie określono progi ostrzegawcze: pierwszy po przekroczeniu 80% zajętości dysku oraz drugi czerwony gdy zajętości dysku przekroczy 95 %. System przesyłał automatycznie ostrzeżenia o zajętości dyskowej na skrzynkę e-maill informatyka Urzędu. Ustalono, że zajętość dysków serwera wynosiła od 25% do 71%.

[akta kontroli str.: 325-328]

2.15. W Urzędzie nie zostały uregulowane zasady związane z zarządzaniem zmianami w wykorzystywanym oprogramowaniu.

[akta kontroli str.: 336]

2.16. Stosownie do art. 30 RODO, Inspektor Ochrony Danych sporządził i prowadził rejestr czynności przetwarzania. Rejestr zawierał informacje, wynikające z art. 30 RODO.

[akta kontroli str.: 140]

Ustalone nieprawidłowości

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

1. Jeden z 10 objętych kontrolą komputerów nie został zabezpieczony przed możliwością zainstalowania nieautoryzowanego oprogramowania, co naruszało wymogi określone w § 20 ust. 2 pkt 4 rozporządzenia KRI. Starosta Powiatu wyjaśnił, że: „Laptop nie posiadał zabezpieczeń administratora systemu ponieważ zainstalowana wersja systemu operacyjnego (Windows 7 Home) na tym urządzeniu nie posiada funkcji podłączenia stacji roboczej do domeny AD. Niezwłocznie zostanie zakupione oprogramowanie w wersji Professional i laptop zostanie podłączony do domeny AD."

   [akta kontroli str.: 10; 256-278; 335]

2. W Urzędzie nie dokumentowano procesu nadawania uprawnień użytkownikom do pracy w systemach innych, niż służące przetwarzaniu danych osobowych, np. BeSTi@, itp. Starosta Powiatu wyjaśnił, że „w urzędzie niezwłocznie zostanie sporządzone zestawienie użytkowników z uprawnieniami do pracy w systemach innych niż do przetwarzania danych osobowych".

   [akta kontroli str.: 11-12; 256-285; 335]

3. W Urzędzie nie określono zasad (procedur) dotyczących bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość, wymaganych na podstawie § 20 ust. 2 pkt. 8 rozporządzenia KRI. Nie została również przyjęta jednolita procedura w zakresie szyfrowania urządzeń przenośnych, w celu minimalizowania ryzyka nieuprawnionego dostępu do informacji, co było niezgodne z wymogami § 20 ust. 2 pkt 9 i 11 rozporządzenia KRI. Starosta

Powiatu wyjaśnił, że: „w urzędzie zostanie sporządzona procedura dotycząca bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość we współpracy z firmą zewnętrzną."

[akta kontroli, str.: 147-255; 334-337]

4. Zastosowane do zabezpieczenia serwerowni rozwiązania w niewystarczającym stopniu chroniły to pomieszczenie. Stanowiło to naruszenie § 20 ust. 2 pkt 9 rozporządzenia KRI.
   Zgodnie z wyjaśnieniami Starosty, w trakcie kontroli zostały podjęte stosowne działania i nieprawidłowości w tym zakresie zostały usunięte.

   [akta kontroli, str.: 306-314; 330; 335; 338-341; 348]

5. W trzech umowach (na pięć zbadanych) z podmiotami zewnętrznymi, dotyczących zakupów i usług informatycznych dla Urzędu, nie zobowiązano wykonawców do zachowania w tajemnicy informacji, do jakich mogą mieć dostęp w związku z realizacją umów. Stanowiło to naruszenie § 20 ust. 2 pkt 10 rozporządzenia KRI.
   Starosta Powiatu wyjaśnił, że „W kolejnych podpisywanych w przyszłości umowach, które będą dotyczyły zakupu sprzętu, oprogramowania lub obsługi serwisowej będą zawierane zapisy dot. zachowania poufności informacji przez dostawcę/wykonawcę."

   [akta kontroli, str.: 20-45; 435-436]

6. W Urzędzie przy pracy w systemach innych niż służące przetwarzaniu danych osobowych[15] zmiana hasła nie była wymuszana przez system (poza programem Płatnik), a zastosowane hasła dostępu nie gwarantowały bezpieczeństwa dostępu do danych przez osoby nieuprawnione. Stanowiło to naruszenie § 20 ust. 2 pkt 7 lit. a i c rozporządzenia KRI.

   Starosta Powiatu wyjaśnił, że „W urzędzie niezwłocznie zostanie sporządzone zestawienie użytkowników z uprawnieniami do pracy w systemach innych niż służące do przetwarzania danych osobowych. Jeżeli będzie tylko taka możliwość/funkcjonalność, oprogramowanie zostanie skonfigurowane w taki sposób, aby wymuszało na użytkowniku stosowanie odpowiednich polityk haseł (po konsultacji ze wsparciem technicznym na dzień dzisiejszy w oprogramowaniu Besti@ nie ma możliwości skonfigurowania stosownych polityk haseł). Należy jednak zauważyć, że komputery na których zainstalowane są aplikacje finansowo-kadrowe pracują w domenie AD i wdrożone są stosowne polityki haseł dla kont użytkowników."

   [akta kontroli, str.: 294-297; 435-436]

Uwaga dotycząca kontrolowanej działalności

NIK zwróciła uwagę, że w Urzędzie nie była prowadzona ewidencja dostępu do pomieszczenia serwerowni.

[akta kontroli, str.: 306-314; 334-341]

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie pomimo stwierdzonych nieprawidłowości wdrożone i wykorzystane w Urzędzie rozwiązania organizacyjne i techniczne, zapewniające bezpieczeństwo informacji. W powyższym zakresie stwierdzono nieprawidłowości, które dotyczyły m.in.:

- nieokreślenia zasad i procedur korzystania przez pracowników ze sprzętu i urządzeń przenośnych Urzędu poza jego siedzibą,
- zastosowania do zabezpieczenia serwerowni rozwiązań, które w niewystarczającym stopniu chroniły to pomieszczenie i przechowywania w nim materiałów łatwopalnych (nieprawidłowość ta została usunięta w trakcie kontroli),

[15] Program Besti@ - system do sprawozdawczości budżetowej; program – Księgowość budżetowa (firmy info-system), Program Vucan (Place Optivum) i Program Płatnik.

– nieuwzględnienia w trzech z pięciu badanych umów z podmiotami zewnętrznymi zapisów o zachowaniu w poufności informacji uzyskanych/przetwarzanych w związku z realizacją tych umów,
– przy pracy w niektórych systemach zmiana hasła nie była wymuszana przez system, a zastosowane hasła dostępu nie gwarantowały bezpieczeństwa dostępu do danych przez osoby nieuprawnione.

Pozytywnie należy ocenić, że komputery Urzędu zostały zabezpieczone przed szkodliwym oprogramowaniem, w Urzędzie prowadzono także na bieżąco aktualizację oprogramowania systemowego oraz sporządzano i weryfikowano prawidłowość kopii zapasowych. Spełniono również wymóg przechowywania kopii poza ich miejscem wytwarzania.

3 Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

3.1. W Urzędzie w okresie objętym kontrolą nie były prowadzone okresowe analizy ryzyka utraty integralności, poufności lub dostępności informacji, o których mowa w § 20 ust. 2 pkt 3 rozporządzenia KRI .

[akta kontroli, str.: 435-436]

3.2. W Urzędzie opracowano instrukcję postepowania w przypadku stwierdzenia naruszenia ochrony danych osobowych.
W badanym okresie nie miały miejsca incydenty z zakresu naruszenia bezpieczeństwa informacji.

[akta kontroli, str.: 435-436]

3.3. W okresie objętym kontrolą w Starostwie przeprowadzone zostały trzy wewnętrzne szkolenia skierowane do wszystkich pracowników w zakresie przetwarzania i ochrony danych osobowych oraz cyberbezpieczeństwa.

[akta kontroli str.: 336; 351-433]

3.4. W 2017 r. w Urzędzie nie został przeprowadzony audyt z zakresu bezpieczeństwa informacji, o którym mowa w § 20 ust. 2 pkt 14 rozporządzenia KRI.

[akta kontroli, str.: 435-436]

3.5. Przed wejściem w życie przepisów RODO została przeprowadzona w Urzędzie szczegółowa analiza procesów przetwarzania danych osobowych, o której mowa w art. 32 RODO. Umową z 10 kwietnia 2018 r. Urząd zlecił usługi w zakresie wdrożenia do stosowania w Starostwie przepisów RODO[16], w ramach której m.in.:
- przeprowadzony został w Urzędzie audyt obejmujący stosowane zabezpieczenia, prowadzoną dokumentację, obieg dokumentów i zagrożenia;
- opracowane zostały projekty dokumentacji zgodnej z RODO;
- zweryfikowane zostały upoważnienia oraz ewidencja osób upoważnionych do przetwarzania danych osobowych.

W ramach realizacji ww. umowy sporządzony został w dniu 25 maja 2018 r. raport z audytu ochrony danych osobowych w Starostwie Powiatowym w Brzezinach wraz z zaleceniami poaudytowymi oraz procedurą wdrożenia RODO z wzorami dokumentów.

[akta kontroli, str.: 47-108; 141]

Ustalone nieprawidłowości

W działalności Urzędu w zakresie podejmowanych działań w celu zapobiegania incydentom bezpieczeństwa informacji stwierdzono następujące nieprawidłowości:

1. W Urzędzie nie przeprowadzano okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji, co było niezgodne z § 20 ust. 2 pkt 3 rozporządzenia KRI, w myśl którego zarządzanie bezpieczeństwem informacji

[16] Umowa o świadczenie usług w zakresie ochrony danych osobowych.

jest realizowane m.in. poprzez przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, oraz podejmowanie działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy. Starosta Powiatu wyjaśnił, że: „W urzędzie niezwłocznie zostanie uregulowany obowiązek przeprowadzenia cyklicznej analizy ryzyka związanego z bezpieczeństwem informacji poprzez wdrożenie odpowiedniej procedury, we współpracy z firmą zewnętrzną (termin wykonania – 30 września 2018 r., dnia 5 września rozpoczęto audyt informatyczny)."

[akta kontroli, str.: 435-436]

2. W 2017 r. w Urzędzie nie został przeprowadzony audyt z zakresu bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI. Starosta Powiatu w złożonych wyjaśnieniach wskazał, że audyt z zakresu bezpieczeństwa informacji został zlecony firmie zewnętrznej i zostanie wykonany do końca września 2018 r.

[akta kontroli, str.: 435-436]

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie działania Urzędu w zakresie zapobiegania incydentom bezpieczeństwa informacji, ze względu na:

- nieprzeprowadzenie cyklicznej analizy ryzyka związanego z bezpieczeństwem informacji, co było niezgodne z § 20 ust. 2 pkt 3 rozporządzenia KRI,
- nieprzeprowadzenie w 2017 r. audytu z zakresu bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI.

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[17], wnosi o:

1. opracowanie i wdrożenie kompletnego systemu zarządzania bezpieczeństwem informacji, uwzględniającego zalecenia normy PN-EN ISO/IEC 27001 i norm z nią związanych (PN-EN ISO/IEC 27002, PN-EN ISO/IEC 27005, PN-EN ISO/IEC 24762),
2. prowadzenie aktualnej i kompletnej elektronicznej ewidencji sprzętu informatycznego, obejmującej jego rodzaj i konfigurację,
3. zapewnienie dokumentowania procesu nadawania uprawnień do wszystkich systemów informatycznych w Urzędzie;
4. określenie zasad dotyczących bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość oraz zapewnienie odpowiednich mechanizmów zabezpieczających komputery przenośne w celu minimalizowania ryzyka nieuprawnionego dostępu;
5. zawieranie w umowach dotyczących zakupów i usług informatycznych dla Urzędu zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
6. prowadzenie okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji,
7. zapewnienie prowadzenia co najmniej raz w roku okresowego audytu wewnętrznego z zakresu 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.

[17] Dz. U. z 2017 r. poz. 524 ze zm.

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.

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

Nadzorująca kontrolę
Emilia Wyciszkiewicz
Główny specjalista k. p.

podpis

Dyrektor
Przemysław Szewczyk

podpis