NAJWYŻSZA IZBA KONTROLI
Delegatura w Łodzi

LLO.410.013.03.2018
P/18/006

Starostwo Powiatowe w Łęczycy
KANCELARIA OGÓLNA
WPŁYNĘŁO
018059
21. 09. 2018
Ilość zał. ..... podpis .....

OA
-wg przydziału
21/9/18
STAROSTA
Wojciech Zdziarski

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura w Łodzi
ul. Kilińskiego 210, 93-106 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

Arkadiusz Kałużny – starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LLO/110/2018 z dnia 18 lipca 2018 r.

(dowód: akta kontroli str. 1)

Jednostka kontrolowana

Starostwo Powiatowe w Łęczycy, Pl. Tadeusza Kościuszki 1, 99-100 Łęczyca (dalej: „Starostwo" lub „Urząd").

Kierownik jednostki kontrolowanej

Wojciech Zdziarski – Starosta Powiatu Łęczyckiego od 1 grudnia 2014 r.

(dowód: akta kontroli str. 2)

Okres objęty kontrolą

Od 1 czerwca 2017 r. do dnia zakończenia czynności kontrolnych w jednostce, tj. do 4 września 2018 r.

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

[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.

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;
- 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[3]

Ocena ogólna i jej uzasadnienie

Najwyższa Izba Kontroli ocenia negatywnie działalność Starosty w zakresie zarządzania bezpieczeństwem informacji, pomimo podejmowania działań na rzecz zapewnienia bezpieczeństwa informacji.

W Starostwie nie zastosowano odpowiednich rozwiązań służących ochronie danych, bowiem:
- nie zapewniono utrzymywania 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,
- z uwagi na przechowywanie kopii zapasowych w tym samym pomieszczeniu, co zgromadzone dane, nie zapewniono odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego na ochronie przed utratą, co stanowiło naruszenie § 20 ust. 2 pkt 12 rozporządzenia KRI,
- na komputerach przenośnych Urzędu nie zastosowano odpowiednich mechanizmów, mających na celu zabezpieczenie informacji na nich przechowywanych w sposób uniemożliwiający nieuprawnionemu jej udostępnienie, modyfikację, usunięcie lub zniszczenie, co stanowiło naruszenie § 20 ust. 2 pkt 9 i pkt 12 rozporządzenia KRI,
- w 2017 r. nie został przeprowadzony audyt z zakresu bezpieczeństwa informacji. Było to niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI, który stanowi, że audyt wewnętrzny w zakresie bezpieczeństwa informacji przeprowadza się nie rzadziej niż raz na rok.

Ponadto, Najwyższa Izba Kontroli zwraca uwagę na:
- brak ewidencji osób przebywających w pomieszczeniu serwerowni,
- zainstalowanie na 21,4% komputerów użytkowanych w Starostwie systemu operacyjnego Windows XP, który nie posiadał wsparcia producenta.

W Urzędzie prawidłowo realizowano zadania dotyczące m.in.:
- aktualizacji uregulowań wewnętrznych w zakresie ochrony danych osobowych, pod kątem ich dostosowania do wymogów w zakresie ochrony danych osobowych w związku z wejściem w życie 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.

– zapewnienia uczestnictwa pracowników w procesie przetwarzania informacji w stopniu adekwatnym do realizowanych przez nich zadań, zgodnie z § 20 ust. 2 pkt 4 rozporządzenia KRI.

III. Opis ustalonego stanu faktycznego

1. Organizacja bezpieczeństwa informacji

Opis stanu faktycznego

1.1. W Urzędzie zostały opracowane i zatwierdzone regulacje wewnętrzne, składające się na System Zarządzania Bezpieczeństwem Informacji. W zarządzeniu Starosty Łęczyckiego nr 46 z dnia 22 października 2015 r., zmienionym zarządzeniem nr 28/2018 z dnia 25 maja 2018 r. w Starostwie została wdrożona Polityka Bezpieczeństwa Informacji[4], o której mowa w § 20 ust. 3 w związku z ust. 1 rozporządzenia KRI. Informacje zaklasyfikowano wyodrębniając trzy poziomy ochrony informacji (informacje jawne, chronione, niejawne). Pracowników Starostwa zapoznano z dokumentami wchodzącymi w skład SZBI podczas przeprowadzonego szkolenia z zakresu bezpieczeństwa informacji i ochrony danych osobowych. W zarządzeniach wprowadzających uregulowania w zakresie bezpieczeństwa informacji zobowiązano wszystkich pracowników do stosowania zasad określonych w tych dokumentach.
Obowiązki w zakresie zarządzania dokumentacją PBI, szkolenia pracowników z ochrony danych osobowych, przeprowadzania sprawdzeń i sprawozdawczości, dostosowania organizacji do wymogów RODO, prowadzenia ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych, były przydzielone do dnia 25 maja 2018 r. osobie pełniącej funkcję ABI, a od 25 maja 2018 r. IOD.

(dowód: akta kontroli str. 38-177, 201-202, 209-219, 301, 304, 308, 312, 315, 320, 326, 330, 332, 336, 340, 344, 348, 352, 356, 358-359, 386-389)

1.2. – 1.3. W związku z wejściem w życie przepisów RODO, w Starostwie dokonano przeglądu dokumentacji SZBI i jej aktualizacji. Dokumentację PBI rozdzielono na Politykę bezpieczeństwa danych osobowych oraz wyodrębniono: procedury zarządzania incydentami, procedury zarządzania zmianą, ryzykiem i oceną skutków oraz procedury realizacji praw osób, których dane dotyczą. Dokonano aktualizacji Instrukcji zarządzania systemem informatycznym obowiązującej w Starostwie.
W związku z wejściem w życie RODO, na tablicach informacyjnych Urzędu oraz w Biuletynie Informacji Publicznej zostały zamieszczone klauzule informacyjne dla kontrahentów (klientów, usługodawców), dotyczące przetwarzania i ochrony danych osobowych. Została uruchomiona skrzynka e-mail, służąca do kontaktu z powołanym w Urzędzie IOD. Opracowane zostały wzory oświadczeń dla pracowników w zakresie przetwarzania danych osobowych, których podpisane egzemplarze przechowywano w Wydziale Organizacyjno-Administracyjnym i Spraw Obywatelskich (dalej Wydział OA). Przygotowano wzory umów z kontrahentami, zawierające uregulowania w zakresie powierzenia przetwarzania danych osobowych.

(dowód: akta kontroli str. 72-123, 178, 301, 304, 308, 312, 315, 320, 326, 330, 332, 336, 340, 344, 348, 352, 356)

---

[4] Zarządzenie nr 28/2018 w sprawie wprowadzenia dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (dalej „Zarządzenie nr 28/2018") i Zarządzenie nr 46 w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji oraz przyjęcia Instrukcji Zarządzania Systemem Informatycznym (dalej „Zarządzenie nr 46/2015").

1.4. Na podstawie Zarządzenia 28/2018 oraz umów o świadczenie usług ABI i IOD[5] wyznaczone zostały stanowiska odpowiedzialne za bezpieczeństwo informacji w Starostwie, tj. jako Administratora Danych Osobowych ustanowiono Starostę Powiatu, ABI (od 20 lipca 2017 r. do 25 maja 2018 r.), IOD (od 25 maja 2018 r.). Wyznaczono dwóch ASI: Informatyka w Wydziale OA i Informatyka w Wydziale Geodezji, Kartografii, Katastru i Gospodarki Nieruchomościami (dalej „Wydział GKN"), pomiędzy którymi podzielono administrowanie systemami informatycznymi. W Zarządzeniu nr 28/2018 i umowach o świadczenie usług ABI i IOD zostały określone podstawowe zakresy obowiązków na tych stanowiskach. Wyznaczeni pracownicy posiadali niezbędne kompetencje do pełnienia powierzonych im zadań z zakresu bezpieczeństwa informacji, poparte wykształceniem i praktyką zawodową.

(dowód: akta kontroli str. 75-78, 170-177, 179-200)

1.5. Zgodnie z art. 37 ust. 1 lit. a RODO, w dniu 25 maja 2018 r. w Urzędzie - na podstawie Zarządzenia nr 28/2018 - został wyznaczony IOD. IOD posiadał niezbędne kwalifikacje, wynikające z art. 37 ust. 5 RODO. Osoba ta pełniła wcześniej funkcję ABI w Starostwie.

(dowód: akta kontroli str. 76, 170-177, 179-182)

1.6. Zakres zadań IOD określono w umowach o świadczenie usług ABI/IOD i w Zarządzeniu nr 28/2018. Spełniono wymóg art. 38 ust. 1 RODO, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych, a także wymóg art. 38 ust. 3 RODO, stanowiącego o bezpośredniej podległości IOD najwyższemu kierownictwu administratora. Regulamin Organizacyjny Starostwa[6] w związku z wejściem w życie RODO zmieniono 8 sierpnia 2018 r.
Wykonywanie obowiązków IOD przez usługodawcę nie wywoływało konfliktu interesów, o którym mowa w art. 38 ust. 6 RODO.

(dowód: akta kontroli str. 76, 170-177, 228, 251, 254)

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

- Polityka bezpieczeństwa informacji;
- Polityka bezpieczeństwa danych osobowych;
- Instrukcja zarządzania systemem informatycznym zawierająca: procedury nadawania uprawnień do przetwarzania danych i rejestrowania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności, stosowane metody i środki uwierzytelniania, procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu, zarządzanie kopiami zapasowymi, zarządzanie nośnikami wymiennymi, sposób zabezpieczenia systemu przed szkodliwym oprogramowaniem, rejestrowanie działań użytkowników i monitorowanie sieci, procedury wykonywania przeglądów i konserwacji oraz zasady wycofywania sprzętu, ochrona sprzętu i oprogramowania, praca zdalna oraz zarządzanie urządzeniami mobilnymi,

---

[5] Umowa nr 99/2017 z dnia 20.07.2017 r. i Umowa nr 160/2017 z dnia 21.12.2017 r. o świadczenie usługi Administratora Bezpieczeństwa Informacji/Inspektora Ochrony Danych Osobowych na rzecz Starostwa Powiatowego w Łęczycy.

[6] Uchwała Nr 410/2018 Zarządu Powiatu Łęczyckiego z dnia 8 sierpnia 2018 roku w sprawie uchwalenia Regulaminu Organizacyjnego Starostwa Powiatowego w Łęczycy.

zabezpieczenia kryptograficzne, zasady korzystania z Internetu oraz poczty elektronicznej;
- Procedura realizacji praw osób, których dane dotyczą;
- Procedura zarządzania zmianą, ryzykiem i oceną skutków;
- Procedura zarządzania incydentami.

(dowód: akta kontroli str. 72-123)

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

(dowód: akta kontroli str. 72-123, 209-219)

1.9. W Starostwie zidentyfikowano zbiory danych podlegających zabezpieczeniu. ABI opracował rejestr zbiorów, zawierający dane określone w § 3 ust. 1 rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbioru danych.[7]

(dowód: akta kontroli str. 255)

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 (opisano w części „Ustalone nieprawidłowości").

(dowód: akta kontroli str. 256-290)

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.

(dowód: akta kontroli str. 220-221, 256-290, 386-387)

Starosta Powiatu Łęczyckiego wyjaśnił m.in., że rejestr zasobów teleinformatycznych w wersji elektronicznej nie był prowadzony, ponieważ na przestrzeni siedmiu lat zachodziły częste zmiany kadrowe na stanowisku informatyka. Obecnie zatrudniony informatyk dokłada wszelkich starań by uporządkować i stworzyć wyżej wymieniony rejestr oraz by utrzymywać go w stanie ciągłej aktualności. W planach jest zakup oprogramowania.

(dowód akta kontr. str. 220-223, 386-389)

Uwagi dotyczące kontrolowanej działalności

Opracowane w ramach SZBI szczegółowe uregulowania, dotyczące: nadawania/cofania uprawnień, zarządzania kopiami zapasowymi, sposobu zabezpieczenia systemu przed szkodliwym oprogramowaniem, wykonywania przeglądów i konserwacji oraz wycofywania sprzętu, ochrony sprzętu i oprogramowania, 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 stwierdzonych nieprawidłowości działania Starosty w zakresie organizacji bezpieczeństwa informacji.

[7] Dz.U. 2015, poz. 719.

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

Opis stanu faktycznego

2.1. W Instrukcji zarządzania systemem informatycznym (pkt. 10.7.-10.9.) zostały określone ograniczenia dotyczące instalacji i wykorzystania oprogramowania przez pracowników. Na podstawie oględzin 10 komputerów ustalono, że zalogowani do nich użytkownicy nie mieli przyznanych uprawnień administracyjnych, umożliwiających instalację dowolnego oprogramowania, co było zgodne z wymogami określonymi w § 20 ust. 2 pkt 4 rozporządzenia KRI.

(dowód: akta kontroli str. 291-293)

2.2. W Starostwie określono zasady nadawania/cofania uprawnień do pracy w systemach informatycznych. Zasady te zostały opisane w następujących dokumentach:

- w Zarządzeniu nr 46/2015 (obowiązującym do 25 maja 2018 r.):
  - w Instrukcji zarządzania systemem informatycznym w zakresie nadawania i rejestrowania uprawnień,
  - w PBI w załączniku dotyczącym procedury nadawania, odwołania, zmiany uprawnień do systemu informatycznego,
- w Zarządzeniu nr 25/2018 - w Instrukcji zarządzania systemem informatycznym, w zakresie nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazania osoby odpowiedzialnej za te czynności.

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. 232, 294-357)

2.3. W wyniku badania blokowania kont w systemach informatycznych, przeprowadzonego na próbie pięciu osób, które w okresie objętym kontrolą zakończyły pracę w Urzędzie i posiadały dostęp do systemów informatycznych ustalono, że ich konta zostały zablokowane. Było to zgodne z § 20 ust. 2 pkt 5 rozporządzenia KRI.

(dowód: akta kontroli str. 358-381)

2.4. Komputery Urzędu w Wydziale GKN, który zajmował oddzielny budynek Starostwa, były zarządzane w oparciu o mechanizm Active Directory. W budynku głównym Urzędu nie wprowadzono ww. rozwiązania. Wymogi dotyczące złożoności haseł do systemów informatycznych zostały określone w Instrukcji zarządzania systemem informatycznym (pkt 3). Rozwiązania i wymogi określone w Instrukcji były zgodne z § 20 ust. 2 pkt 7 rozporządzenia KRI. W wyniku badania trzech systemów informatycznych w Wydziale GKN ustalono, że wymogi wynikające z powyższej Instrukcji zostały wdrożone w tych systemach (EwOpis, EwMapa i Ośrodek).

(dowód: akta kontroli str. 382-384)

2.5. Na pięciu stanowiskach pracy, realizujących zadania z zakresu rejestracji pojazdów monitory pracowników zostały usytuowane w sposób uniemożliwiający interesantom wgląd do wyświetlanych danych. Powyższe działanie spełniało wymogi § 20 ust. 2 pkt 7 rozporządzenia KRI.

(dowód: akta kontroli str. 385)

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. 106, 209-219)

2.7. Starosta wyjaśnił m.in., że w Urzędzie nie stosowano programów specjalistycznych do szyfrowania/archiwizacji danych. Wskazał również, że komputery przenośne nie są wykorzystywane poza siedzibą Starostwa.
Zasady szyfrowania danych i dysków ustalono w Instrukcji zarządzania systemem informatycznym. Zgodnie z tymi zasadami (pkt. 11.2 i 12.2. Instrukcji), szyfrowanie jest stosowane na urządzeniach mobilnych oraz na nośnikach wymiennych zawierających dane osobowe. W wyniku oględzin sześciu z 13 laptopów użytkowanych w budynku głównym Starostwa stwierdzono, że żaden z nich nie został zaszyfrowany, a na jednym z tych laptopów znajdował się plik zawierający dane osobowe pracowników Urzędu (opisano w części „Ustalone nieprawidłowości").

(dowód: akta kontroli str. 106, 386-391)

2.8. W serwerowni budynku głównego Starostwa zapewniono rozwiązania w zakresie podtrzymania zasilania oraz warunków środowiskowych pracy serwerów i urządzeń sieciowych. W okresie objętym kontrolą serwisowano znajdujące się w pomieszczeniu klimatyzator i czujnik sygnalizacji pożaru. Zasilacze awaryjne podlegały codziennemu monitorowaniu przez Informatyka Wydziału OA podczas wizyt w serwerowni. W serwerowni znajdowały się wydzielone zabezpieczenia prądowe. W Urzędzie nie zostały zainstalowane zapasowe źródła zasilania sprzętu komputerowego, tj. równoległa linia zasilająca lub agregat prądotwórczy.
Nie była prowadzona ewidencja dotycząca dostępu do pomieszczenia serwerowni (opisano w części „Uwagi").

(dowód: akta kontroli str. 220-226, 392-394, 395-402)

2.9. W wyniku badania sześciu z 29 obowiązujących w okresie objętym kontrolą umów z kontrahentami, dotyczących dostaw sprzętu teleinformatycznego i/lub świadczenia usług telekomunikacyjnych/serwisowych/utrzymaniowych, ustalono, że zawarto w nich zapisy dotyczące zachowania poufności informacji uzyskanych w związku z realizacją tych umów, co było zgodne z § 20 ust. 2 pkt 10 rozporządzenia KRI.

(dowód: akta kontroli str. 403-535)

2.10. W Starostwie zostały określone zasady, dotyczące postępowania w przypadku przekazywania sprzętu teleinformatycznego poza jednostkę, np. w celu wykonania napraw. W Instrukcji zarządzania systemami informatycznymi (pkt 9.4.) przewidziano przed przekazaniem sprzętu m.in. usunięcie dysków twardych komputera, jeśli nie jest to możliwe do wykonania, na prace serwisowe zawierana jest umowa zgodnie z zasadami powierzania danych osobowych opisanych Polityce bezpieczeństwa danych osobowych.

(dowód: akta kontroli str. 105)

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

(dowód: akta kontroli str. 536)

2.12. Zasady dotyczące tworzenia i przechowywania kopii zapasowych danych w Starostwie zostały określone w Instrukcji zarządzania systemem informatycznym (pkt 5). Zgodnie z ww. instrukcją kopie zapasowe tworzone są w dwóch miejscach:

w budynku głównym Urzędu Starostwa i w Wydziale GKN, według harmonogramów wykonywania kopii. W wyniku oględzin ustalono, że ostatnie kopie zapasowe wykonano zgodnie z harmonogramami. W Instrukcji nie określono zasad dotyczących czasu przechowywania kopii zapasowych, częstotliwości testowania kopii zapasowych i sposobu dokumentowania z wykonania testu poprawności zapisanych kopii. W wyniku kontroli ustalono, że do testowania kopii w Wydziale GKN wykorzystywano oprogramowanie do weryfikacji poprawności procesu tworzenia kopii oraz że informatyk Wydziału OA weryfikował utworzone kopie tygodniowe okresowo, raz w miesiącu. Zgodnie z uregulowaniami w lokalizacji głównej kopie baz danych systemów, w tym bazy systemów SoftHard, Besti@, BankNet tworzono ręcznie – na komputer lokalny w pomieszczeniu ASI. Informatyk Wydziału OA przechowywał kopie tygodniowe na dysku zewnętrznym, który znajdował się w metalowej szafie zamykanej na klucz w pokoju Informatyka. Kopie tygodniowe przechowywane były także na dysku komputera użytkowanego przez ASI budynku głównego Starostwa. Zgodnie z Instrukcją zarządzania systemem informatycznym w Wydziale GKN kopie baz danych systemów GKN tworzone były codziennie na macierz dyskową serwera oraz dodatkowo ręcznie na dysk zewnętrzny raz w tygodniu. Utworzone w Wydziale GKN dzienne kopie zapasowe przechowywane były na serwerze w Serwerowni Wydziału GKN (opisano w części „Ustalone nieprawidłowości").

(dowód: akta kontroli str. 103-104, 386-389, 537-576)

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.

(dowód: akta kontroli str. 291-293)

2.14. W ramach obowiązujących w Starostwie uregulowań nie zostały określone zasady monitorowania stanu pojemności przestrzeni dyskowej w serwerach Urzędu. Ustalono jednak, 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 informatyków.

(dowód: akta kontroli str. 582-588)

2.15. W uregulowaniach Starostwa z zakresu bezpieczeństwa informacji zostały uwzględnione działania związane z zarządzaniem zmianami - w Procedurze zarządzania zmianą, ryzykiem i oceną skutków. W procedurze uwzględniono identyfikowanie zmian wynikających między innymi: z konieczności dostosowania istniejących lub wprowadzenia nowych procesów, zgłoszenia przez pracownika stwierdzonej niedoskonałości SZBI, zmian prawnych, zmian w otoczeniu Starostwa, mających wpływ na bezpieczeństwo informacji. W Procedurze zarządzania zmianą uwzględniono planowanie wprowadzenia zmian w oparciu o analizę wpływu zmian na bezpieczeństwo informacji. W ww. analizie uwzględniono sytuacje powstawania nowych zbiorów i procesów przetwarzania danych osobowych, wykorzystywanie nowych technologii i związanych z nimi zagrożeń, skalę oraz kontekst przetwarzanych danych. Do analizy wpływu zmian na bezpieczeństwo informacji w procedurze wprowadzono przeprowadzanie szacowania ryzyka i ocenę skutków naruszeń. W ocenie skutków naruszeń zawarto opis planowanych operacji przetwarzania, ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów, a także środki planowane w celu zaradzenia ryzyku.

(dowód: akta kontroli str. 119-122)

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

(dowód: akta kontroli str. 255)

Ustalone nieprawidłowości

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

1. Na komputerach przenośnych Urzędu nie zastosowano odpowiednich mechanizmów, mających na celu zabezpieczenie informacji na nich przechowywanych w sposób uniemożliwiający nieuprawnionemu jej udostępnienie, modyfikację, usunięcie lub zniszczenie, co stanowiło naruszenie § 20 ust. 2 pkt 9 i pkt 12 rozporządzenia KRI. W Starostwie nie przestrzegano bowiem zasad zdalnej pracy oraz zarządzania urządzeniami mobilnymi zawartych w punkcie 11 Instrukcji zarządzania systemem informatycznym. Zgodnie z tą zasadą, urządzenia mobilne są wyposażone w mechanizmy szyfrujące, jeśli występuje na nich przetwarzanie danych osobowych. W wyniku kontroli sześciu laptopów stwierdzono, że jeden z nich nie został zaszyfrowany, pomimo iż zawierał plik z danymi osobowymi.
   Starosta wyjaśnił, że instrukcja wskazuje na szyfrowanie, gdyż Polityka bezpieczeństwa oraz dokumentacja powiązana opisuje stan bezpieczeństwa do jakiego należy dążyć. Ponadto instrukcja wskazuje na zasady pracy zdalnej, które nie są obecnie realizowane, ze względu na brak sytuacji wykonywania pracy zdalnej. Planowo zostanie wdrożone szyfrowanie dysków laptopów jednak nie zostało to zrealizowane w pierwszej kolejności, gdyż laptopy nie są wynoszone poza teren Starostwa.

   (dowód: akta kontroli str. 106, 386-394)

2. W Urzędzie nie zapewniono odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego na ochronie przed utratą, co stanowiło naruszenie § 20 ust. 2 pkt 12 rozporządzenia KRI. Informatyk w Wydziale OA przechowywał kopie zapasowe dzienne na serwerze w serwerowni budynku głównego Starostwa, a Informatyk w Wydziale GKN przechowywał kopie zapasowe dzienne na serwerze w serwerowni Wydziału GKN. W obu przypadkach kopie zapasowe dzienne były przechowywane w miejscu ich wytworzenia. Także w przypadku przechowywania kopii tygodniowych na komputerze Informatyka Wydziału GKN kopie były przechowywane w miejscu ich wytworzenia – w tym samym pomieszczeniu, w którym znajdowała się serwerownia.
   Starosta wyjaśnił, że w najbliższym czasie zostanie wdrożone rozwiązanie zapewniające wykonywanie kopii zamiennie w obu lokalizacjach, co dodatkowo podniesie bezpieczeństwo wykonywanych kopii.

   (dowód: akta kontroli str. 103-104, 386-389, 537-580)

Uwagi dotyczące kontrolowanej działalności

1. W Urzędzie nie była prowadzona ewidencja dostępu do pomieszczenia serwerowni. Zdaniem NIK, wprowadzenie ewidencji wejść i wyjść do serwerowni wpłynie na zwiększenie bezpieczeństwa infrastruktury IT zlokalizowanej w tym pomieszczeniu.

2. Na 18 komputerach z 84 użytkowanych w Starostwie (21,4%) 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.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie wdrożone i wykorzystywane w Starostwie rozwiązania organizacyjne i techniczne, zapewniające bezpieczeństwo informacji. Ocenę uzasadnia przechowywanie kopii zapasowych w miejscu ich wytworzenia, a także brak szyfrowania danych zgromadzonych i przetwarzanych na urządzeniach przenośnych.

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

3.1. Stosownie do § 20 ust. 2 pkt 3 rozporządzenia KRI, w PBI Urzędu opracowano Procedurę zarządzania zmianą, ryzykiem i oceną skutków, w której wyszczególniono z jakich procesów może wynikać potrzeba zastosowania zasad zarządzania zmianami.
W związku z wejściem w życie rozporządzenia RODO, ABI opracował - z dniem 15 maja 2018 r. - arkusz szacowania ryzyka . W arkuszu tym uwzględnione zostały - zgodnie z Procedurą zarządzania zmianą, ryzykiem i oceną skutków: rodzaj aktywów poddanych zmianie, przykłady podatności na ryzyko, prawdopodobieństwo oraz skutki wystąpienia zagrożeń, przykłady zagrożeń, wynik szacowania zagrożeń, plan postępowania z oszacowanymi zagrożeniami, szczegóły planu i status wykonania planu.

(dowód: akta kontroli str. 119-122, 255)

3.2. Zgodnie z § 20 ust. 2 pkt 13 rozporządzenia KRI, w Urzędzie została opracowana procedura zarządzania incydentami, stanowiąca element Polityki bezpieczeństwa informacji. W procedurze tej uwzględniono rodzaje naruszeń, określono zasady zgłaszania i wstępnej oceny incydentów, podejmowania działań dotyczących stwierdzonych incydentów oraz zasad ich zgłaszania do Urzędu Ochrony Danych Osobowych.
Starosta wyjaśnił, że nie było zgłoszeń dotyczących incydentów, w związku z czym nie powstała żadna dokumentacja z postępowania z naruszeniem. W okresie od 1 czerwca 2017 r. nie wystąpiły żadne naruszenia bezpieczeństwa informacji.

(dowód: akta kontroli str. 115-118, 577-580)

3.3. Stosownie do § 20 ust. 2 pkt 6 rozporządzenia KRI, w Starostwie przeprowadzono szkolenie dotyczące bezpieczeństwa informacji.
W dniu 11 maja 2018 r. odbyło się szkolenie wewnętrzne dla pracowników w zakresie obowiązujących w Starostwie przepisów bezpieczeństwa informacji, ochrony danych, a także przepisów RODO. Szkolenie to prowadził ABI.

(dowód: akta kontroli str. 201-202, 589-590)

3.4. W 2017 r. w Urzędzie nie został przeprowadzony audyt z zakresu bezpieczeństwa informacji, wymagany na podstawie § 20 ust. 2 pkt 14 rozporządzenia KRI (opisano w części „Ustalone nieprawidłowości").

(dowód: akta kontroli str. 220-226)

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

(dowód: akta kontroli str. 80-107, 115-122, 255)

Ustalone nieprawidłowości

W działalności Starostwa w zakresie podejmowanych działań w celu zapobiegania incydentom bezpieczeństwa informacji stwierdzono następującą nieprawidłowość:

W 2017 r. w Urzędzie nie przeprowadzono audytu z zakresu bezpieczeństwa informacji. Było to niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI.

Starosta Powiatu Łęczyckiego wyjaśnił m.in., że okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji nie był przeprowadzany w latach 2017 i 2018 z uwagi na wysoki koszt i częste zmiany kadrowe na stanowisku informatyka.

(dowód: akta kontroli str. 220-226)

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[8] wnosi o:

1. Prowadzenie aktualnej i kompletnej elektronicznej ewidencji sprzętu informatycznego, obejmującej jego rodzaj i konfigurację.
2. Stosowanie odpowiednich mechanizmów zabezpieczających komputery przenośne zawierające dane osobowe.
3. Wdrożenie rozwiązań mających na celu ochronę danych przed utratą, poprzez przechowywanie kopii zapasowych poza miejscem ich wytwarzania.
4. Prowadzenie 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.

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

Zgodnie z art. 62 ustawy o NIK proszę o poinformowanie Najwyższej Izby 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.

Łódź, dnia 14 września 2018 r.

Najwyższa Izba Kontroli
Delegatura w Łodzi
Dyrektor
Przemysław Szewczyk

Kontroler:
Arkadiusz Kałużny
Starszy inspektor k. p.

.....
podpis

.....
podpis

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