204

KANCELARIA OGÓLNA URZĘDU MIASTA I GMINY NOWA DĘBA WPŁYNĘŁO 2016 -04- 20 Ilość załączników: podpis: 2802/2016

WOJEWODA PODKARPACKI
ul. Grunwaldzka 15
35-959 Rzeszów
skr. poczt. 297

OA-VII.431.1.2016

Rzeszów, 2016 – 04 - 14

Pan
Wiesław Ordon
Burmistrz
Miasta i Gminy Nowa Dęba

Na podstawie art. 47 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. Nr 185, poz. 1092) – przekazuję wystąpienie pokontrolne po kontroli problemowej dotyczącej działania systemów teleinformatycznych używanych do realizacji zadań zleconych z zakresu administracji rządowej, przeprowadzonej w Urzędzie Miasta i Gminy Nowa Dęba w dniach 8, 10 i 14 marca 2016 r.

WYSTĄPIENIE POKONTROLNE

po kontroli problemowej **działania systemów teleinformatycznych używanych do realizacji zadań zleconych z zakresu administracji rządowej** przeprowadzonej w dniach 8, 10 i 14 marca 2016 r. w Urzędzie Miasta i Gminy Nowa Dęba.

Kontrolę przeprowadził zespół kontrolerów: Alicja Trygar (starszy specjalista), oraz Marcin Adamczyk (starszy informatyk) na podstawie upoważnień do kontroli udzielonych przez działającego z upoważnienia Wojewody Podkarpackiego – Dyrektora Wydziału Organizacyjno-Administracyjnego (pisma z dnia 12.02.2016 r., znak OA-VII.431.1.2016).

Kontrolą, prowadzoną na podstawie art. 25 ust. 1 pkt 3 lit. a w zw. z ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jednolity z 2014 r., Dz. U. poz. 1114), objęto działanie systemów teleinformatycznych używanych do realizacji zadań zleconych z zakresu administracji rządowej w okresie od 1.01.2015 r. do dnia badania.

Zakres kontroli obejmował spełnianie minimalnych wymagań dla systemów teleinformatycznych, tj. zgodność z rodz. IV rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 526, ze zm.).

Wykonywanie zadań w kontrolowanym zakresie przez Urząd Miasta i Gminy Nowa Dęba zostało ocenione **pozytywnie z uchybieniami**.

Podstawą powyższej oceny są następujące ustalenia kontroli:

1. **Projektowanie, wdrażanie i eksploatowanie systemów teleinformatycznych:**
   a. W okresie objętym kontrolą Urząd Miasta i Gminy Nowa Dęba wykorzystywał dziesięć systemów teleinformatycznych do realizacji zadań zleconych z zakresu administracji rządowej, w tym dwa systemy centralne (aplikacja „Źródło" oraz aplikacja Centralna Ewidencja i Informacja o Działalności Gospodarczej – CEIDG), zintegrowany system informatyczny wspomagający realizację zadań Urzędu Miasta i Gminy Nowa Dęba w zakresie m.in. ewidencji ludności i dopłat paliwowych, a także system, nabyty przez Urząd, realizujący zadania Urzędu Miasta i Gminy Nowa Dęba w zakresie Urzędu Stanu Cywilnego - USC.
   b. Systemy centralne, dostępne przez stronę WWW podlegały kontroli w ograniczonym zakresie.
   c. Systemy informatyczne wspomagające realizację zadań Urzędu Miasta i Gminy Nowa Dęba w zakresie m.in. ewidencji ludności, dopłat paliwowych i USC zostały zaprezentowane w czasie kontroli i w ocenie kontrolujących były intuicyjne, a także zrozumiałe w użytkowaniu. Administrator Systemu Informatycznego (ASI) nie zgłaszał problemów z wydajnością, niezawodnością lub funkcjonalnością systemów. Były na bieżąco rozwijane, a w jednostce była zainstalowana aktualna wersja oprogramowania. Aktualizację oprogramowania realizował wyznaczony pracownik jednostki lub Wykonawca, z którym zawarto umowę na obsługę serwisową zintegrowanych systemów informatycznych wspomagających realizację zadań Urzędu.

2. **Zarządzanie usługami realizowanymi przez systemy teleinformatyczne:**
   a. Umowa zawarta z Wykonawcą o asystę techniczną systemu informatycznego wspomagającego realizację zadań Urzędu Miasta i Gminy Nowa Dęba w zakresie tworzenia plików XML aktów stanu cywilnego przeznaczonych do przeniesienia za pośrednictwem aplikacji Źródło do centralnego rejestru - zawierała postanowienia określające poziom świadczenia usług poprzez wskazanie maksymalnych czasów usunięcia błędów oraz zdefiniowanie grup błędów.

   Umowa zawarta z Wykonawcą na obsługę serwisową zintegrowanego systemu informatycznego wspomagającego realizację zadań Urzędu Miasta i Gminy Nowa Dęba w zakresie m.in ewidencji ludności, dopłat paliwowych, świadczeń rodzinnych itd. zawierała zapisy czasu reakcji na zgłoszony problem w § 3 ust 4. "Wykonawca zobowiązuje się do podjęcia naprawy niezwłocznie po otrzymaniu zgłoszenia".

   Umowa zawarta z Wykonawcą na świadczenie usług hostingowych (serwer pocztowy) w § 3 Regulaminu świadczenia usług określała parametry dostępności usługi, takie jak: łączny czas trwania przerw technicznych w ciągu roku i czas trwania jednorazowej przerwy technicznej.
   b. W przypadku systemów informatycznych wspomagających realizację zadań Urzędu Miasta i Gminy Nowa Dęba w zakresie ewidencji ludności i USC czasy reakcji były zachowane. Wszystkie konsultacje z producentem oprogramowania odbywały się drogą telefoniczną lub za pomocą poczty elektronicznej. Serwis producenta oprogramowania reagował zgodnie z umową.
   c. Brak ustalonych ogólnych procedur zarządzania usługami w Urzędzie Miasta i Gminy Nowa Dęba. W umowie zawartej z Wykonawcą o asystę techniczną systemu informatycznego wspomagającego realizację zadań Urzędu Miasta i Gminy

Nowa Dęba w zakresie USC zawarto zapisy dotyczące zgłoszenia przez Użytkownika *Awarii Oprogramowania* oraz przyjęcia tego zgłoszenia przez Wykonawcę. Również umowa z Wykonawcą na obsługę serwisową zintegrowanego systemu informatycznego wspomagającego realizację zadań Urzędu zawierała zapisy o dokonaniu zawiadomienia o nieprawidłowościach.

3. Wymogi WCAG 2.0

a. Systemy informatyczne wspomagające realizację zadań Urzędu Miasta i Gminy Nowa Dęba nie były objęte wymogami WCAG 2.0 w zakresie dostępności ze względu na brak interakcji z klientami za pośrednictwem sieci publicznej. Systemy centralne w tym zakresie nie były objęte kontrolą.

4. System zarządzania bezpieczeństwem informacji:

a. Urząd Miasta i Gminy Nowa Dęba wdrożył system ochrony bezpieczeństwa danych osobowych, w tym przetwarzanych w postaci elektronicznej. System powyższy składał się z *Polityki Bezpieczeństwa Informacji ze szczególnym uwzględnieniem Ochrony Danych Osobowych* oraz *Instrukcji Zarządzania Systemami Informatycznymi Służącymi do Przetwarzania Danych Osobowych*, które weszły w życie w dniu 1 marca 2016 r. (zarządzenie nr 233/2016 Burmistrza Miasta i Gminy Nowa Dęba z dnia 23 lutego 2016 r.). Ze względu na przetwarzanie we wszystkich badanych systemach danych osobowych były one objęte ww. systemem ochrony danych.

b. Wskazane powyżej dokumenty weszły w życie od 1 marca 2016 r. i według wyjaśnień specjalisty ds. ochrony danych osobowych w uzupełnieniu były jeszcze niektóre załączniki. Wcześniej obowiązującymi dokumentami były: *Polityka Bezpieczeństwa Danych Osobowych Gminy Nowa Dęba* oraz *Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych Gminy Nowa Dęba* - Zarządzenie nr 111/2011 Burmistrza Miasta i Gminy Nowa Dęba.

c. System ochrony danych wskazany w pkt a nie był w całości zgodny z Polską Normą PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie nie odbywało się na podstawie Polskich Norm PN-ISO/IEC 27002, PN-ISO/IEC 27005 oraz PN-ISO/IEC 24762. Równocześnie, – z wyjątkami opisanym w pozostałej części niniejszego wystąpienia – ustanowiono i wdrożono wymagane elementy systemu zarządzania bezpieczeństwem informacji, w tym zwłaszcza strukturę organizacyjną, procedury i procesy.

d. *Polityka Bezpieczeństwa Informacji ze szczególnym uwzględnieniem ochrony danych osobowych* oraz *Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych* zawierały zestaw przygotowanych do wdrożenia oraz udokumentowania zasad i procedur w obszarach istotnych dla bezpieczeństwa informacji za wyjątkiem:
- Zasad i procedur zarządzania ryzykiem bezpieczeństwa informacji;
- Zasad i procedur dokonywania przeglądów (audytów) systemu bezpieczeństwa informacji;
- Zasad i procedur zapewnienia w niekorzystnej sytuacji wymaganego poziomu ciągłości bezpieczeństwa informacji.

Specjalista ds. ochrony danych osobowych poinformował, że w przygotowaniu jest opracowanie, ustanowienie i wdrożenie pełnego systemu bezpieczeństwa informacji - zgodnie z wymogami § 20 ust.1-3 rozporządzenia KRI, wymaga to jednak pewnego okresu czasowego.

e. W Urzędzie Miasta i Gminy Nowa Dęba, co najmniej jeden raz w roku przeprowadzana była kontrola wewnętrzna w zakresie oceny ochrony danych osobowych. Zakres kontroli na 2015 rok obejmował takie elementy jak: funkcjonowanie zabezpieczeń fizycznych i systemowych, prawidłowość funkcjonowania mechanizmów dostępu do zbioru danych, inwentaryzację oprogramowania, sprawdzenie zasilania energetycznego sieci komputerowej, sprawdzenie kopii zapasowych, okresów ich tworzenia i przechowywania, stan ochrony przeciwpożarowej.

Ponadto w jednostce przeprowadzony był audyt wewnętrzny w okresie od 26 listopada 2015 r. do 8 stycznia 2016 r. w temacie: "ocena efektów realizacji projektu pn. Podkarpacki System e-Administracji Publicznej oraz organizacji komunikacji zewnętrznej w Urzędzie za pośrednictwem EPUAP". Audytor w sprawozdaniu przedstawił zalecenia i rekomendacje.

Dodatkowo zgodnie z wyjaśnieniami specjalisty ds. ochrony danych - corocznie analizowana i oceniana jest aktualność uprawnień pracowników (upoważnień) do przetwarzania danych osobowych.

Jednak nie jest to pełny zakres kontroli w rozumieniu § 20 ust. 14 rozporządzenia Rady Ministrów z dnia 12.04.2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. poz. 526).

Specjalista ds. ochrony danych osobowych poinformował, że w planie audytu na 2016 rok powyższy audyt zostanie uzupełniony o pełny zakres.

f. W jednostce dokonano inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. Zmiany nanoszone są na bieżąco. Należy rozważyć możliwość wykorzystania oprogramowania do automatycznego audytu sprzętu i oprogramowania.

g. W okresie objętym badaniem kontrolnym, w Urzędzie Miasta i Gminy Nowa Dęba nie wprowadzono jeszcze w życie udokumentowanego, formalnego zarządzania ryzykiem bezpieczeństwa informacji zgodnego z Polską Normą PN-ISO/IEC 27005. Funkcjonował natomiast system zarządzania ryzykiem w ramach systemu kontroli zarządczej.

Polityka Bezpieczeństwa Informacji ze szczególnym uwzględnieniem ochrony danych osobowych oraz *Instrukcja Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych* zawierały zasady postępowania w przypadku naruszenia bezpieczeństwa systemu informatycznego i ochrony danych wraz z Analizą organizacyjnych środków bezpieczeństwa informacji oraz Analizą technicznych i informatycznych środków bezpieczeństwa informacji. Załącznik nr 10 do Polityki Bezpieczeństwa Informacji zawierał Wykaz identyfikacji i oceny ryzyka w obszarze bezpieczeństwa informacji.

Pośrednio o monitorowaniu zagrożeń dla bezpieczeństwa informacji mogą świadczyć wdrożone mechanizmy kontrolne (wewnętrzne kontrole i audyty), a także zasady nadawania upoważnień i uprawnień w systemach, zabezpieczenia fizyczne i logiczne systemów.

h. Pomimo braku formalnego zarządzania ryzykiem, w Urzędzie Miasta i Gminy Nowa Dęba były stosowane mechanizmy ograniczania ryzyka bezpieczeństwa informacji. W trakcie kontroli pracownicy Urzędu mieli kontakt z Administratorem Systemu Informatycznego poprzez telefon wewnętrzny i telefon komórkowy. W przypadku zgłaszania przez pracowników problemów z działaniem sprzętu lub oprogramowania

Administrator Systemu Informatycznego rozwiązywał problem, aktualizował na bieżąco zarówno systemy operacyjne jak również oprogramowanie antywirusowe. Na bieżąco aktualizowane było także oprogramowanie wspomagające realizację zadań w Urzędzie Miasta i Gminy Nowa Dęba. Aktualizację wykonywał osobiście Administrator Systemu Informatycznego lub Wykonawca, z którym podpisana była umowa na obsługę serwisową ww. oprogramowania.

i. Pracownicy Urzędu Miasta i Gminy Nowa Dęba przetwarzający dane osobowe posiadali upoważnienia do przetwarzania danych osobowych. Wyniki badania włączono do akt kontroli (wraz z listą badanych pracowników oraz z listą sprawdzającą). W wyniku badania stwierdzono, iż wszyscy pracownicy Urzędu Miasta i Gminy Nowa Dęba pracujący w badanych systemach teleinformatycznych posiadali stosowne uprawnienia, które wynikały z indywidualnych upoważnień do przetwarzania danych osobowych. Upoważnienia określały m.in. formę przetwarzania danych, zakres uprawnień pracownika oraz wykorzystywany system teleinformatyczny.

   Badane upoważnienia podpisał Administrator Danych.

   Załącznikiem do upoważnienia było oświadczenie o zapoznaniu się z regulacjami dotyczącymi ochrony danych osobowych oraz świadomości ciążących na pracowniku obowiązków.

   W umowie zawartej z Wykonawcą o asystę techniczną systemu informatycznego wspomagającego realizację zadań Urzędu Miasta i Gminy Nowa Dęba w zakresie USC w § 8 określone zostały zasady powierzenia przetwarzania danych osobowych Wykonawcy.

   Również z Wykonawcą zintegrowanego systemu informatycznego wspomagającego realizację zadań Urzędu Miasta i Gminy Nowa Dęba w zakresie m.in. ewidencji ludności i dopłat paliwowych, świadczeń rodzinnych została zawarta Umowa o powierzeniu przetwarzania danych osobowych.

j. Zakres uprawnień pracowników do przetwarzania danych w badanych systemach był adekwatny do powierzonych im zadań i obowiązków, określonych w imiennych zakresach czynności. Z uzyskanych wyjaśnień wynika, że w badanym okresie, w sprawdzanych systemach wystąpiła zmiana powierzonych zadań i obowiązków. Zakres uprawnień był zmieniony, w przypadku zmiany zadania pracownika.

   Równocześnie podczas badania ustalono, że w przypadku ustania upoważnienia dla pracownika w 2015 r. nie została dokonana blokada konta użytkownika w systemie centralnym CEIDG. W wydrukowanym raporcie CEIDG pracownik nadal był na liście użytkowników niezablokowanych oraz nieusuniętych z organizacji.
   W dniu 22 marca 2016 r. mailowo była przekazana informacja z Urzędu Miasta i Gminy Nowa Dęba o podjętych działaniach w celu usunięcia z listy niezablokowanych oraz nieusuniętych z organizacji użytkownika, który nie miał upoważnienia do pracy w systemie CEIDG. Należy pamiętać, aby podejmować niezwłocznie działania wyrejestrowujące użytkownika z systemu informatycznego w takich przypadkach jak: rozwiązanie umowy, utrata upoważnienia do przetwarzania danych osobowych, zmiana zakresu obowiązków.

k. Pracownikom przetwarzającym dane w badanych systemach zapewniono szkolenia z zakresu bezpieczeństwa informacji. System szkoleń obejmował:

- zapoznanie z przepisami dotyczącymi ochrony danych osobowych przed przystąpieniem do przetwarzania danych oraz pracy w systemie; zapoznanie dokumentowały oświadczenia podpisane i opatrzone datą przez pracownika;

- okresowe szkolenie z "podstawowych zasad i podstaw prawnych przetwarzania danych osobowych z uwzględnieniem zmian w przepisach prawa z zakresu ochrony danych osobowych" w Urzędzie Miasta i Gminy Nowa Dęba przeprowadził w dniu 2 marca 2016 r. Pan Piotr Glen - specjalista ds. ochrony danych osobowych, Audytor Systemu Zarządzania Bezpieczeństwem Informacji wg PN-ISO/IEC 27001. Ogółem przeszkolono 48 pracowników. Program szkoleń obejmował m.in. zakres ochrony danych osobowych oraz obowiązujących wymagań formalno-prawnych, wymagania obowiązujące w procesie bezpiecznego przetwarzania i przechowywania danych osobowych, zagrożenia i metody wykradania danych oraz zasady ich ochrony, zabezpieczenia systemów informatycznych oraz uświadomienie o zakresie odpowiedzialności.

  Specjalista ds. ochrony danych osobowych poinformował również, że wszystkie dokumenty dotyczące Polityki Bezpieczeństwa Informacji umieszczone zostały na zasobie wewnętrznym Urzędu Miasta i Gminy Nowa Dęba dostępnym dla każdego pracownika.

a. Przetwarzane informacje w ramach badanych systemów teleinformatycznych były chronione przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
- monitorowanie dostępu do informacji,
- czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
- zastosowanie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji w sposób wystarczający z jedną uwagą.

  Komputery pracujące w sieci publicznej Urzędu Miasta i Gminy Nowa Dęba były zabezpieczone przed zagrożeniami pochodzącymi z sieci publicznej Internet za pomocą dedykowanego urządzenia typu firewall. Należy rozważyć możliwość podniesienia kwalifikacji ASI w zakresie konfiguracji i monitorowania używanych w Urzędzie urządzeń sieciowych za pomocą specjalistycznych szkoleń celem pełnego wykorzystania możliwości urządzeń aktywnych sieci.
  Jako dobrą praktykę, której wprowadzenie należy rozważyć jest system monitorujący otwarcia drzwi do serwerowni. O każdym wejściu do pomieszczenia, Administrator Systemu Informatycznego byłby informowany za pomocą SMS-a. Ponadto system może informować o innych parametrach środowiskowych serwerowni.

b. W *Polityce bezpieczeństwa informacji ze szczególnym uwzględnieniem ochrony danych osobowych* i *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych* zostały określone podstawowe zasady gwarantujące bezpieczną pracę na odległość. Jednak w Urzędzie nie wykonywało się pracy na odległość z wyjątkiem prac serwisowych. Zasady prac serwisowych zostały opisane w umowach z firmami zewnętrznymi.

c. Przetwarzane informacje w badanych systemach były zabezpieczone w sposób uniemożliwiający nieuprawnionym osobom ich ujawnienie, modyfikacje, usunięcie, zniszczenie lub wprowadzenie błędnych informacji poprzez zastosowanie mechanizmów kontroli dostępu do badanych systemów – identyfikatory i hasła dla każdego użytkownika, a w przypadku systemu Źródło imienne karty dostępu.

d. Badane systemy centralne posiadały własne polityki bezpieczeństwa i wobec tego badana jednostka musiała je realizować. Umowy zawarte z dostawcami aplikacji alternatywnych wspierających pracę w Urzędzie Miasta i Gminy Nowa Dęba zawierały zapisy dotyczące powierzenia przetwarzania danych osobowych, które musi przestrzegać Wykonawca w celu zachowania odpowiedniego poziomu bezpieczeństwa informacji. Umowa zawarta o świadczenie usług hostingowych

zawierała zapisy zobowiązujące Wykonawcę do zachowania tajemnicy wszystkich danych, informacji uzyskanych w związku ze świadczeniem usług. Ponadto w przypadku awarii dysku twardego będącego na gwarancji dysk nie był przekazywany do serwisu, lecz naprawiany na miejscu lub wymieniany na nowy. Stare, nieużywane dyski twarde magazynowane były przez Administratora Systemu Informatycznego w celu ich późniejszego zniszczenia.

e. Ogólne zasady postępowania z informacjami, zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych zostały ustalone w *Polityce bezpieczeństwa informacji ze szczególnym uwzględnieniem ochrony danych osobowych* oraz w *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych*.

f. Systemy operacyjne zainstalowane na stanowiskach komputerowych, gdzie wykorzystywane były badane systemy posiadały bieżące aktualizacje. Również systemy antywirusowe, java i zintegrowane systemy informatyczne wspomagające realizację zadań Urzędu Miasta i Gminy Nowa Dęba były w aktualnej wersji. Na dzień kontroli w Urzędzie Miasta i Gminy Nowa Dęba były wykorzystywane 3 licencje na system operacyjny Windows XP. Z uwagi na brak wsparcia dla systemu operacyjnego Windows XP od 8 kwietnia 2014 r. przez firmę Microsoft należy dążyć do tego, aby w pierwszej kolejności zaktualizować ww. system operacyjny, szczególnie wtedy, gdy jest jeszcze wykorzystywany przez pracowników podczas codziennej pracy.

g. W *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych* została zawarta informacja o procedurze tworzenia kopii zapasowych, ich przechowywania, testowania oraz likwidacji nośników zawierających stare, nieaktualne kopie bezpieczeństwa. Za przestrzeganie zasad wymienionych w procedurze odpowiadał Administrator Systemów Informatycznych, który przedstawił Notatkę służbową z dnia 14.03.2016 r. dotyczącą sposobu wykonywania i przechowywania kopii bezpieczeństwa w Urzędzie Miasta i Gminy Nowa Dęba oraz nowy rejestr kopii zapasowych baz danych Urzędu Miasta i Gminy Nowa Dęba. Należy wyraźnie podkreślić, że ASI odpowiedzialny jest za wykonywanie lub nadzór nad wykonywaniem kopii bezpieczeństwa, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszych przydatności. Warto zwrócić szczególną uwagę na sprawowanie tego nadzoru w przypadku, gdy ww. czynności zlecane są Wykonawcom umów na obsługę serwisową.

h. Dostęp do serwerów z bazami danych aplikacji alternatywnych wspierających realizację zadań Urzędu Miasta i Gminy Nowa Dęba mieli wyłącznie Administrator Systemu Informatycznego oraz Wykonawcy umowy serwisowej. Takie rozwiązanie zapewnia ochronę przed błędami, utratą lub nieuprawnioną modyfikacją danych przedmiotowego systemu.

i. W ramach kontroli sprawdzone zostały mechanizmy wymiany danych pomiędzy systemami alternatywnymi wspierającymi realizację zadań Urzędu Miasta i Gminy Nowa Dęba, a Systemami Rejestrów Państwowych (SRP). Dostęp do sieci SRP dla systemów wspierających pracę Urzędu nie był skonfigurowany. Pracownicy korzystający z pakietu systemów wspomagających realizację zadań Urzędu w zakresie m.in. ewidencji ludności w celu wymiany danych z centralnym systemem SRP korzystali z odpowiedniego modułu, który umożliwiał taką wymianę za pomocą odpowiednich subskrypcji, przenoszonych między stacjami roboczymi na urządzeniu typu Pendrive. Pracownicy USC pozbawieni byli podobnego rozwiązania, wszystkie

zmiany, w centralnym systemie SRP jak i w aplikacji wspomagającej pracę Urzędu w zakresie USC, nanoszone były ręcznie. Takie rozwiązanie jest bezpieczne.

Jako dobrą praktykę, której wprowadzenie należy rozważyć jest możliwość przeprowadzenia odpowiedniej konfiguracji systemów wspomagających realizację zadań Urzędu Miasta i Gminy Nowa Dęba, sieci publicznej, sieci Systemów Rejestrów Państwowych w celu zautomatyzowania wymiany informacji pomiędzy systemami stosowanymi w Urzędzie a centralnym systemem SRP. Pomocne w tym może być ww. szkolenie dla ASI oraz wytyczne dostępne na stronie plid.obywatel.gov.pl.

j. Stanowiska komputerowe wykorzystywane do pracy z badanymi systemami były skonfigurowane w sposób zapewniający bezpieczeństwo plików systemowych, a także zapewniono redukcję ryzyk wynikających z opublikowanych podatności poprzez wykonywanie aktualizacji, z dwiema uwagami:

   Na dzień kontroli większość z użytkowników pracowała na swoim komputerze na koncie nazwanym "użytkownik". Należy każdemu użytkownikowi utworzyć imienne konta na stacjach roboczych, z odpowiednimi uprawnieniami.

   Warto rozważyć możliwość wdrożenia usługi Active Directory. Z informacji uzyskanych podczas kontroli Urząd Miasta i Gminy Nowa Dęba posiadał odpowiednie licencje na wdrożenie ww. usługi.

k. W ramach kontroli ustalono, że w przypadku dostrzeżenia problemów z działaniem systemów użytkownik zgłaszał problem do Administratora Systemów Informatycznych. Jeżeli Administrator samodzielnie nie był w stanie rozwiązać problemu dokonywał zgłoszenia na serwisy help deskowe poszczególnych badanych systemów. Z informacji otrzymanych od Administratora Systemów Informatycznych nie były to zgłoszenia dot. możliwości naruszenia bezpieczeństwa informacji, ale dotyczyły błędnie działających systemów.

5. Rozliczalność:

a. W wyniku badania stwierdzono, że w dziennikach systemów alternatywnych wpierających realizację zadań Urzędu Miasta i Gminy Nowa Dęba rejestrowane były zdarzenia zgodnie z § 21 ust. 1 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 526, ze zm.) z dwiema uwagami:

   Zintegrowany system informatyczny wspierający realizację zadań Urzędu Miasta i Gminy Nowa Dęba w zakresie m.in. ewidencji ludności nie posiadał modułu umożliwiającego rejestr wykonanych czynności przez użytkowników. Rozliczalność nie była realizowana na poziomie systemu, lecz na poziomie bazy danych. Należy stworzyć funkcjonalność umożliwiającą przeglądanie ASI logów systemu.

   System wspierający realizację zadań Urzędu Miasta i Gminy Nowa Dęba w zakresie USC posiadał moduł umożliwiający rejestr wykonanych zdarzeń przez użytkowników lecz rozliczalność nie była w nim realizowana. Rozliczalność była realizowana na poziomie bazy danych. W systemie należy włączyć rejestrację czynności wykonywanych przez użytkowników w odpowiednim module.

b. W dziennikach systemowych, na poziomie baz danych, odnotowywane były działania wszystkich użytkowników zarejestrowanych w systemie, także tych z uprawnieniami administracyjnymi. W Urzędzie oprócz Administratora Systemów

Informatycznych dostęp administracyjny do systemów wspomagających pracę Urzędu mieli także pracownicy podmiotów zewnętrznych, z którymi podpisane były umowy na obsługę serwisową oprogramowania. Należy stworzyć osobne, imienne konta administracyjne dla każdego administratora w bazach danych badanych systemów w celu jednoznacznej identyfikacji wykonywanych zadań.

c. Dzienniki systemów zawarte były w bazach danych, z których korzystały aplikacje alternatywne wspierające realizację zadań Urzędu Miasta i Gminy Nowa Dęba i gromadzone były od momentu pierwszej instalacji systemów. W przypadku aplikacji wspomagającej realizację zadań w zakresie USC od 2014 roku, a w przypadku aplikacji wspomagających realizację zadań w zakresie m.in. ewidencji ludności i dopłat paliwowych także od 2014 roku.

Przedstawiając powyższe oceny i uwagi, w celu usunięcia stwierdzonych uchybień oraz usprawnienia badanej działalności – na podstawie art. 46 ust. 3 pkt 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej – przekazuję następujące wnioski i zalecenia pokontrolne:

1. Zgodnie z wymogami par. 20 ust. 1-3 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 526, ze zm.) należy kontynuować prace związane z kompletowaniem, wdrożeniem i eksploatacją wewnętrznych regulacji, które obejmowałyby system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji w Urzędzie Miasta i Gminy Nowa Dęba.
2. Ustanowić, wdrożyć i zapewnić funkcjonowanie lub podjąć prace związane z poprawieniem i uaktualnieniem istniejących w Urzędzie procedur wewnętrznych w zakresie: zarządzania ryzykiem bezpieczeństwa informacji, wykonywania corocznych audytów w zakresie bezpieczeństwa informacji.
3. W przypadkach takich jak: rozwiązanie umowy, utrata upoważnienia do przetwarzania danych osobowych, zmiana zakresu obowiązków - należy niezwłocznie podejmować działania wyrejestrowujące użytkownika z systemu informatycznego.
4. Należy rozważyć możliwość wykorzystania oprogramowania do automatycznego audytu sprzętu i oprogramowania.
5. Należy rozważyć możliwość podniesienia kwalifikacji Administratora Systemów Informatycznych w zakresie konfiguracji i monitorowania używanych w Urzędzie urządzeń sieciowych za pomocą specjalistycznych szkoleń celem pełnego wykorzystania możliwości urządzeń aktywnych sieci.
6. Należy rozważyć możliwość wprowadzenia systemu monitorującego otwieranie drzwi do serwerowni. O każdym wejściu do pomieszczenia, Administrator Systemu Informatycznego byłby informowany za pomocą SMS-a. Ponadto system może informować o innych parametrach środowiskowych serwerowni.
7. Z uwagi na niewspieranie systemu Windows XP należy w pierwszej kolejności wyeliminować ww. oprogramowanie. Na dzień kontroli w Urzędzie Miasta i Gminy Nowa Dęba wykorzystywane były 3 licencje na system Windows XP.
8. Należy zwiększyć nadzór nad wykonywaniem kopii bezpieczeństwa, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszych przydatności.
9. Należy rozważyć możliwość przeprowadzenia odpowiedniej konfiguracji systemów wspomagających realizację zadań Urzędu Miasta i Gminy Nowa Dęba, sieci publicznej, sieci Systemów Rejestrów Państwowych w celu

Informatycznych dostęp administracyjny do systemów wspomagających pracę Urzędu mieli także pracownicy podmiotów zewnętrznych, z którymi podpisane były umowy na obsługę serwisową oprogramowania. Należy stworzyć osobne, imienne konta administracyjne dla każdego administratora w bazach danych badanych systemów w celu jednoznacznej identyfikacji wykonywanych zadań.

c. Dzienniki systemów zawarte były w bazach danych, z których korzystały aplikacje alternatywne wspierające realizację zadań Urzędu Miasta i Gminy Nowa Dęba i gromadzone były od momentu pierwszej instalacji systemów. W przypadku aplikacji wspomagającej realizację zadań w zakresie USC od 2014 roku, a w przypadku aplikacji wspomagających realizację zadań w zakresie m.in. ewidencji ludności i dopłat paliwowych także od 2014 roku.

Przedstawiając powyższe oceny i uwagi, w celu usunięcia stwierdzonych uchybień oraz usprawnienia badanej działalności – na podstawie art. 46 ust. 3 pkt 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej – przekazuję następujące wnioski i zalecenia pokontrolne:

1. Zgodnie z wymogami par. 20 ust. 1-3 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 526, ze zm.) należy kontynuować prace związane z kompletowaniem, wdrożeniem i eksploatacją wewnętrznych regulacji, które obejmowałyby system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji w Urzędzie Miasta i Gminy Nowa Dęba.
2. Ustanowić, wdrożyć i zapewnić funkcjonowanie lub podjąć prace związane z poprawieniem i uaktualnieniem istniejących w Urzędzie procedur wewnętrznych w zakresie: zarządzania ryzykiem bezpieczeństwa informacji, wykonywania corocznych audytów w zakresie bezpieczeństwa informacji.
3. W przypadkach takich jak: rozwiązanie umowy, utrata upoważnienia do przetwarzania danych osobowych, zmiana zakresu obowiązków - należy niezwłocznie podejmować działania wyrejestrowujące użytkownika z systemu informatycznego.
4. Należy rozważyć możliwość wykorzystania oprogramowania do automatycznego audytu sprzętu i oprogramowania.
5. Należy rozważyć możliwość podniesienia kwalifikacji Administratora Systemów Informatycznych w zakresie konfiguracji i monitorowania używanych w Urzędzie urządzeń sieciowych za pomocą specjalistycznych szkoleń celem pełnego wykorzystania możliwości urządzeń aktywnych sieci.
6. Należy rozważyć możliwość wprowadzenia systemu monitorującego otwieranie drzwi do serwerowni. O każdym wejściu do pomieszczenia, Administrator Systemu Informatycznego byłby informowany za pomocą SMS-a. Ponadto system może informować o innych parametrach środowiskowych serwerowni.
7. Z uwagi na niewspieranie systemu Windows XP należy w pierwszej kolejności wyeliminować ww. oprogramowanie. Na dzień kontroli w Urzędzie Miasta i Gminy Nowa Dęba wykorzystywane były 3 licencje na system Windows XP.
8. Należy zwiększyć nadzór nad wykonywaniem kopii bezpieczeństwa, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszych przydatności.
9. Należy rozważyć możliwość przeprowadzenia odpowiedniej konfiguracji systemów wspomagających realizację zadań Urzędu Miasta i Gminy Nowa Dęba, sieci publicznej, sieci Systemów Rejestrów Państwowych w celu

zautomatyzowania wymiany informacji pomiędzy systemami stosowanymi w Urzędzie a centralnym systemem SRP. Pomocne w tym może być ww. szkolenie dla Administratora Systemów Informatycznych oraz wytyczne dostępne na stronie plid.obywatel.gov.pl.

10. Należy każdemu użytkownikowi utworzyć imienne konta na stacjach roboczych, z odpowiednimi uprawnieniami.
11. Należy rozważyć możliwość wdrożenia usługi Active Directory. Z informacji uzyskanych podczas kontroli Urząd Miasta i Gminy Nowa Dęba posiadał odpowiednie licencje na wdrożenie ww. usługi.
12. W zintegrowanym systemie informatycznym wspierającym realizację zadań Urzędu Miasta i Gminy Nowa Dęba w zakresie m.in. ewidencję ludności należy stworzyć funkcjonalność umożliwiającą przeglądanie przez Administratora Systemów Informatycznych logów systemu.
13. W systemie wspierającym realizację zadań Urzędu Miasta i Gminy Nowa Dęba w zakresie USC należy włączyć moduł odpowiedzialny za rejestrację czynności wykonywanych przez użytkowników.
14. Należy stworzyć osobne, imienne konta administratora w bazach danych systemów w celu jednoznacznej identyfikacji wykonywanych zadań.

O sposobie wykonania powyższych zaleceń, a także o podjętych działaniach lub przyczynach ich niepodjęcia – mając na względzie art. 46 ust. 3 pkt 3 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej – proszę poinformować na piśmie w terminie do dnia **30 czerwca 2016 r.**

WOJEWODA PODKARPACKI

(-)

Ewa Leniart

(Podpisane bezpiecznym podpisem elektronicznym)