NAJWYŻSZA IZBA KONTROLI
Delegatura w Krakowie

LKR – 4101-022-01/2014
P/14/004

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura w Krakowie
ul. Łobzowska 67, 30-038 Kraków
T +48 12 342 34 00, F +48 12 342 34 44
lkr@nik.gov.pl

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli

P/14/004 – Wdrażanie wybranych wymagań dotyczących systemów teleinformatycznych, wymiany informacji w postaci elektronicznej oraz Krajowych Ram Interoperacyjności na przykładzie niektórych urzędów gmin miejskich i miast na prawach powiatu

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli
Delegatura w Krakowie

Kontroler

Janusz Klimek, specjalista kontroli państwowej, upoważnienie do kontroli nr 92108 z 28 lipca 2014 r.

(dowód: akta kontroli str. 1-2)

Jednostka kontrolowana

Urząd Miasta Nowy Targ, ul. Krzywa 1, 34-400 Nowy Targ (dalej: Urząd)

Kierownik jednostki kontrolowanej

Marek Fryźlewicz, Burmistrz Miasta Nowy Targ (dalej: Burmistrz)

(dowód: akta kontroli str. 3)

II. Ocena kontrolowanej działalności

Ocena ogólna[1]

Urząd podjął działania dla zapewnienia minimalnych wymogów interoperacyjności systemów informatycznych. Dwa z trzech skontrolowanych systemów (Obsługa Urzędu Stanu Cywilnego oraz Obsługa Ewidencji Ludności) zapewniały wewnątrz Urzędu informacyjny poziom współpracy, natomiast system Odpady komunalne powiązany był z dwoma innymi systemami na poziomie jednostronnej komunikacji, a z jednym systemem na poziomie transakcyjnym, gdzie wymiana danych przebiegała bez pośrednictwa użytkowników systemu. Ponadto skontrolowane systemy udostępniały dane w formatach określonych w rozporządzeniu 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].

W Urzędzie obowiązuje tradycyjny obieg dokumentów, jednakże Urząd zamierza wdrożyć system elektronicznego zarządzania dokumentacją w ramach Programu Operacyjnego Kapitał Ludzki realizując projekt „Nowoczesna administracja samorządowa".

W badanym okresie, tj. od 31 maja 2012 r. do 19 sierpnia 2014 r., Urząd świadczył usługę elektroniczną polegającą na komunikacji klienta z Urzędem za pośrednictwem ePUAP[3]. W ramach tego klienci mogli składać wnioski, czy też formularze w 109 kategoriach spraw, których liczba została zwiększona w badanym okresie ponad czterokrotnie. Wzory dokumentów elektronicznych w zakresie świadczonych przez Urząd usług nie zostały jednak przekazane do centralnego repozytorium na ePUAP, co było niezgodne z art. 19b ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[4]

Wzajemna komunikacja pomiędzy Urzędem a Małopolskim Urzędem Wojewódzkim odbywała się w formie elektronicznej, jak i tradycyjnej. Ponadto Urzędy Skarbowe przekazywały Urzędowi sprawozdania Rb elektronicznie za pośrednictwem ePUAP.

[1] Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna. Jeżeli sformułowanie oceny ogólnej według proponowanej skali byłoby nadmiernie utrudnione, albo taka ocena nie dawałaby prawdziwego obrazu funkcjonowania kontrolowanej jednostki w zakresie objętym kontrolą, stosuje się ocenę opisową, bądź uzupełnia ocenę ogólną o dodatkowe objaśnienie.

[2] Dz. U. z 2012 r., poz. 526 – dalej: rozporządzenie KRI.

[3] Elektroniczna Platforma Usług Administracji Publicznej.

[4] Dz. U. z 2013 r. poz. 235 - dalej: ustawa o informatyzacji.

Urząd w podstawowym stopniu wspierał model usługowy w zakresie świadczenia usług elektronicznych. W usługach dostępnych elektronicznie można było zidentyfikować właściciela tych usług, istniały karty opisu usługi i były aktualizowane. W stosunku do ww. usług w żadnym dokumencie nie wskazano jednak maksymalnego czasu niedostępności usługi, sposobu zgłaszania awarii, podmiotów zobowiązanych do jej usunięcia, czy technicznego właściciela usługi.

Sprawowanie nadzoru nad tworzeniem i monitorowaniem systemu zarządzania bezpieczeństwem systemów informatycznych, w tym zapewnienie bezpieczeństwa danych przetwarzanych w Urzędzie Najwyższa Izba Kontroli ocenia negatywnie, bowiem kontrola wykazała następujące nieprawidłowości naruszające unormowania § 20 ust. 2 rozporządzenia KRI w powiązaniu z normami PN-ISO/IEC 17799:2007 i PN-ISO/IEC 27001:2007:

- brak aktualizacji i doskonalenia uregulowań wewnętrznych Urzędu w zakresie systemu zarządzania bezpieczeństwem informacji, co nie zapewniło zarządzania bezpieczeństwem informacji w zakresie zmieniającego się otoczenia;
- nieprzeprowadzanie inwentaryzacji składników sprzętu komputerowego i zainstalowanego na nim oprogramowania;
- pozostawienie możliwości instalacji nieautoryzowanego oprogramowania na dziesięciu komputerach, poddanych oględzinom;
- nieprzeszkolenie w badanym okresie wszystkich pracowników zaangażowanych w proces przetwarzania informacji;
- brak procedur gwarantujących bezpieczną pracę przy przetwarzaniu danych na urządzeniach mobilnych;
- niewprowadzenie do stosowania w Urzędzie procedur zgłaszania incydentów naruszenia bezpieczeństwa informacji;
- nietestowanie kopii zapasowych danych Urzędu w pełnym zakresie tych danych;
- przechowywanie kopii zapasowych danych Urzędu w sposób nie gwarantujący zabezpieczenia przed ich utratą w sytuacji wypadków losowych, takich jak pożar czy zalanie.

III. Opis ustalonego stanu faktycznego

1. Dostosowanie systemów teleinformatycznych do współpracy z innymi systemami informatycznymi

1.1. Elektroniczne świadczenie usług w dokumentach strategicznych miasta

Opis stanu faktycznego

W Strategii Rozwoju Miasta Nowy Targ na lata 2012-2020[5] wyszczególniono kierunki rozwoju, podzielone na cele strategiczne, uszczegółowione celami operacyjnymi i wreszcie konkretnymi zadaniami. W ramach tychże zadań wymieniono m.in. rozbudowę infrastruktury teleinformatycznej i interoperacyjnych platform cyfrowych dla instytucji publicznych i samorządów[6] oraz podnoszenie jakości świadczonych usług publicznych[7]. Ramy czasowe realizacji pierwszego z tych zadań określono na lata 2012-2013. Sformułowano także mierniki dla tego zadania, takie jak: liczba osób korzystających z elektronicznych narzędzi obsługi administracyjnej, zmiany liczby klientów obsługiwanych przy pomocy narzędzi elektronicznych w stosunku do ogółu klientów obsługiwanych przez administrację

[5] Strategię Rozwoju wprowadzono uchwałą Rady Miasta nr XX/153/2012 z 31 maja 2012 r.

[6] Kierunek I „Gospodarka lokalna", cel strategiczny II „Rozwój infrastruktury technicznej zwiększającej atrakcyjność inwestycyjną miasta Nowy Targ", cel operacyjny II.2 „Rozwój infrastruktury społeczeństwa informacyjnego", zadanie II.2.3.

[7] Kierunek III „Kapitał społeczny", cel strategiczny I „Rozwój kapitału społecznego", cel operacyjny I.6 „Podnoszenie jakości świadczonych usług publicznych", zadanie I.6.1)

samorządową. Drugie zadanie zostało skrótowo opisane jako „doskonalenie jakości usług publicznych w administracji samorządowej przy zastosowaniu nowoczesnych systemów zarządzania oraz platform elektronicznych (e-urząd)". Ramy czasowe jego realizacji to lata 2012-2020, a miernikami były: liczba działań wdrożeniowych z zakresu podnoszenia zdolności zarządczych administracji samorządowej oraz działań doskonalących funkcjonowanie administracji, ocena skuteczności funkcji i jakości obsługi Urzędu mierzona poziomem satysfakcji petentów, wskaźnik procentowy wszystkich obsługiwanych do zadowolonych i wnoszących uwagi. W przypadku obu powyższych zadań nie określono wskaźników stopnia ich realizacji. Jak wyjaśnił Burmistrz brak określenia tych wskaźników wynikał z braku wprowadzenia stosownego zapisu podczas aktualizacji Strategii przez Małopolski Instytut Samorządu Terytorialnego, który moderował jej opracowanie, jak i uczestników warsztatów opracowujących poszczególne zadania do celów operacyjnych. W swoich wyjaśnieniach Burmistrz wskazał, iż Urząd zwróci uwagę na powyższy brak podczas procesu ewaluacji zapisów strategicznych.

Zagadnienia dotyczące dostosowania Urzędu do elektronicznego świadczenia usług poruszone zostały także we wprowadzonym z datą 24 maja 2013 r. IV wydaniu polityki jakości określającym cele strategiczne, poprzez które polityka ta będzie realizowana. Wśród celów tych zapisano usprawnienie obsługi klientów poprzez doskonalenie jakości i terminowości świadczonych usług oraz wdrażanie i stosowanie nowoczesnych systemów informatycznych, wspomagających pracę Urzędu oraz kontakt z klientem.

Zadanie polegające na rozbudowie infrastruktury teleinformacyjnej i interoperacyjnych platform cyfrowych nie zostało wykonane. Jako przyczynę, w sprawozdaniu z realizacji Strategii Rozwoju, wskazano bariery prawne i techniczne na rynku teleinformatycznym oraz wygaszenie funduszy MRPO 2007-2013. Z kolei podnoszenie jakości świadczonych usług publicznych zrealizowano poprzez działania w obszarze wyposażenia infrastrukturalnego (m.in. zakupy sprzętu informatycznego i oprogramowania, remont serwerowni, uzupełnienie podpisów elektronicznych dla kluczowych pracowników Urzędu) oraz modernizację procesów zarządzania (opisanie i uszczegółowienie procesów pracy w Urzędzie zgodnie z normą ISO 9001:2008, w tym zidentyfikowanie i opisanie procedur usług świadczonych przez Urząd).

(dowód: akta kontroli str. 8-21, 109, 144, 249)

1.2. Promowanie komunikacji elektronicznej

Opis stanu faktycznego

Burmistrz wyjaśnił, że Urząd nie promował komunikacji elektronicznej, natomiast tego rodzaju działania zostały zaplanowane w ramach projektu „Nowoczesna administracja samorządowa" w Programie Operacyjnym Kapitał Ludzki. Realizacja tego projektu odbędzie się w okresie od 1 lipca 2014 r. do 30 września 2015 r. W projekcie uwzględniono takie działania jak: promocja elektronicznych usług publicznych, uruchomienie punktu potwierdzenia Profilu Zaufanego, instalacja i uruchomienie usług elektronicznych dostępnych na platformie ePUAP, wdrożenie systemu elektronicznego zarządzania dokumentami, a także szkolenia dla pracowników. Urząd otrzymał informację, iż powyższy projekt zostanie dofinansowany w ramach ww. Programu.

(dowód: akta kontroli str. 110, 333-338)

1.3. Ankiety lub inne formy poznania potrzeb mieszkańców gminy odnośnie elektronicznej formy komunikacji

Opis stanu faktycznego

Urząd dokonywał corocznego badania satysfakcji mieszkańców Nowego Targu w zakresie świadczonych im usług. Pytania jakie zadawano w ankietach dotyczyły m.in. oceny zapewnienia i dostępności informacji oraz terminowości wykonania usługi. Powyższe badania nie uwzględniały kwestii potrzeb mieszkańców w zakresie komunikacji elektronicznej z Urzędem.

(dowód: akta kontroli str. 111)

Uwagi dotyczące badanej działalności

Zdaniem NIK jakiekolwiek działania związane z rozwojem elektronicznych form komunikacji między klientem a Urzędem powinny być poprzedzone identyfikacją potrzeb mieszkańców miasta oraz wnikliwą ich analizą. Rozszerzenie przez Urząd badań satysfakcji klientów

Urzędu o temat ich potrzeb w zakresie komunikacji elektronicznej z Urzędem zapewni prawidłowe i precyzyjne wytyczenie celów oraz w następstwie tego gospodarne wydatkowanie środków publicznych.

1.4. Korespondencja z Ministrem Administracji i Cyfryzacji

Opis stanu faktycznego

Po wejściu w życie rozporządzenia KRI, Urząd nie zwracał się do Ministra Administracji i Cyfryzacji z problemami lub z prośbą o pomoc w zakresie dostosowania swoich systemów/rejestrów informatycznych do wymogów KRI.

(dowód: akta kontroli str. 111)

1.5. Procedury regulujące komunikację elektroniczną w Urzędzie

Opis stanu faktycznego

Burmistrz zarządzeniem Nr 120.Z.10.2011 z 11 marca 2011 r. w sprawie określenia systemu kancelaryjnego oraz wytycznych dotyczących zasad i trybu wykonywania czynności kancelaryjnych w Urzędzie ustanowił system tradycyjny (papierowy) jako podstawowy sposób dokumentowania przebiegu załatwiania i rozstrzygania spraw. W rozdziale II § 4 ww. zarządzenia zapisano m.in., że korespondencję wpływającą do urzędu przyjmuje Biuro Obsługi Mieszkańców, które prowadzi rejestr kancelaryjny korespondencji wpływającej: od klientów, z poczty, od kurierów, przesłanej e-mailem na konto umnt@um.nowytarg.pl. Ponadto Sekretariat zobowiązany został do przyjmowania korespondencji przesyłanej faksem lub pocztą elektroniczną. W zarządzeniu tym określono także sposób postępowania przy wysyłaniu korespondencji faksem. Nie sprecyzowano procedur elektronicznego obiegu dokumentów w Urzędzie, ani komunikacji za pośrednictwem ePUAP. W regulaminie organizacyjnym Urzędu nie określono sposobu załatwiania spraw drogą elektroniczną.

(dowód: akta kontroli str. 120-121, 145)

Burmistrz Miasta Nowy Targ Urząd wyjaśnił, że nie opracował procedur obiegu dokumentów regulujących komunikację elektroniczną w Urzędzie, ponieważ nie wdrożono jeszcze systemu do elektronicznego obiegu dokumentów. System taki będzie wdrożony w ramach projektu „Nowoczesna administracja samorządowa", który zgodnie z informacjami przekazanymi Urzędowi otrzyma unijne dofinansowanie. Nie tworzono również odrębnych procedur odnośnie komunikacji za pośrednictwem ePUAP, traktując korzystanie z tej platformy analogicznie jak korespondencję e-mail. Zasady postępowania z pocztą elektroniczną opisane zostały w § 44, § 45 i § 60 ogólnie obowiązującej Instrukcji kancelaryjnej, stanowiącej załącznik nr 1 do rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych[8].

Pracownicy Biura Obsługi Mieszkańców mieli w swoich zakresach czynności obowiązek „obsługi Elektronicznej Platformy Usług Administracji Publicznej – ePUAP oraz skrzynki mailowej Urzędu Miasta Nowy Targ".

(dowód: akta kontroli str. 111, 146, 158-159, 161, 164, 167, 170)

1.6. Liczba złożonych dokumentów / wniosków / podań

Opis stanu faktycznego

W okresie od 31 maja 2012 r. do 31 maja 2014 r. do Urzędu wpłynęło 52.367 dokumentów w tym 1.176 w formie elektronicznej (obywatele złożyli 26.940 dokumentów w wersji tradycyjnej i 17 w wersji elektronicznej, osoby prawne złożyły w Urzędzie 12.801 dokumentów papierowych i 9 elektronicznych, natomiast inne urzędy przekazały 11.450 dokumentów tradycyjnych i 1.150 elektronicznych).

(dowód: akta kontroli str. 114)

1.7. Zgodność opisu usług elektronicznych z usługami Urzędu

Opis stanu faktycznego

W badanym okresie Urząd realizował usługę elektroniczną umożliwiającą komunikację z klientem za pośrednictwem platformy ePUAP. Według stanu na 31 maja 2012 r. (wejście w życie rozporządzenia KRI) klienci Urzędu mieli możliwość zdalnego załatwienia spraw

[8] Dz. U. Nr 14, poz. 67 ze zm.

w 20 kategoriach. Natomiast na dzień 19 sierpnia 2014 r. kategorii takich było 109. Wśród dziesięciu usług najczęściej odwiedzanych na stronie internetowej Urzędu znalazły się sprawy dotyczące: dofinansowania kosztów kształcenia młodocianych pracowników (21,4 tys. odsłon), udostępnienia informacji publicznej (18,8 tys.), nadania stopnia awansu zawodowego nauczyciela mianowanego (14 tys.), odpisu aktu stanu cywilnego (12,7 tys.), transportu niepełnosprawnych uczniów w celu spełniania obowiązku szkolnego i obowiązku nauki (12,1 tys.), transportu niepełnosprawnych uczniów w celu spełniania obowiązku rocznego przygotowania przedszkolnego (11,8 tys.), wydawania dowodów osobistych po raz pierwszy (11,2 tys.), składania formularzy podatkowych do podatku od nieruchomości, podatku rolnego i podatku leśnego przez osoby prawne (11,1 tys.), zapłaty opłaty skarbowej (10,9 tys.) oraz zawarcia małżeństwa w Urzędzie stanu cywilnego (9,9 tys.). Do 19 sierpnia 2014 r. odnotowano łącznie 551.823 odsłony na stronie internetowej Urzędu w zakresie usług świadczonych elektronicznie.

(dowód: akta kontroli str. 150-155)

Usługa świadczona przez Urząd elektronicznie polegała na możliwości: uzyskania informacji na temat danej sprawy, pobrania wzoru określonego dokumentu oraz przesłania go za pośrednictwem ePUAP do Urzędu.

Informacje na temat usługi świadczonej przez Urząd elektronicznie, jak również wzory dokumentów związanych z tą usługą znajdowały się na stronie internetowej Urzędu. Na dzień 18 sierpnia 2014 r. w samym ePUAP znajdowały się informacje o dwunastu kategoriach spraw możliwych do załatwienia. Powyższy sposób prezentacji nie ograniczał klientowi możliwości załatwienia pozostałych (niewymienionych w ePUAP) spraw, jednakże mógł wprowadzić w błąd, co do dostępności tych niewymienionych.

(dowód: akta kontroli str. 150-156, 175-176)

Szczegółową kontrolą objęto pięć spośród dwunastu usług, które pojawiły się w wyszukiwarce spraw w platformie ePUAP jako właściwe dla Urzędu Miasta Nowy Targ. Były to: decyzja o środowiskowych uwarunkowaniach dla planowanego przedsięwzięcia mogącego potencjalnie znacząco oddziaływać na środowisko, deklaracja na podatek leśny, deklaracja na podatek od nieruchomości, odpisy i zaświadczenia z ksiąg stanu cywilnego oraz udostępnianie informacji publicznej na wniosek. Stwierdzono zgodność opisu usługi elektronicznie świadczonej za pośrednictwem ePUAP z faktycznie świadczonymi usługami.

(dowód: akta kontroli str. 175-176)

1.8. Opisy procedur elektronicznego załatwiania spraw w BIP

Opis stanu faktycznego

Biuletyn Informacji Publicznej Urzędu prowadzony był w ramach jego strony internetowej (www.nowytarg.pl). Wszystkie odnośniki zawarte w BIP prowadziły do informacji publikowanych na stronie Urzędu, w tym również informacji na temat sposobu elektronicznego załatwiania spraw. Instrukcja tam zamieszczona zawierała: podstawę prawną usługi, nazwę usługi i jej cel, kategorię i odbiorców, a także umiejscowienie usługodawcy wg podziału administracyjnego kraju.

(dowód: akta kontroli str. 157, 175-176)

1.9. Przekazanie wzorów dokumentów elektronicznych do centralnego repozytorium ePUAP

Opis stanu faktycznego

Wg stanu na dzień 22 sierpnia 2014 r. w Centralnym Repozytorium Wzorów Dokumentów zarejestrowano 1564 wzory dokumentów z lat 2008-2014. Żaden z dostępnych tam wzorów nie był wzorem zarejestrowanym przez Urząd. Wymóg przekazywania przez organ administracji publicznej wzorów dokumentów elektronicznych do centralnego repozytorium na ePUAP wynikał z art. 19b ust. 3 ustawy o informatyzacji.

W ramach świadczonej przez Urząd usługi elektronicznej nie posługiwano się wzorami dokumentów elektronicznych pobranych z Centralnego Repozytorium.

(dowód: akta kontroli str. 175-176, 280)

Ustalone nieprawidłowości

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

Urząd do dnia kontroli NIK nie umieścił wzorów dokumentów elektronicznych w centralnym repozytorium ePUAP, co było niezgodne z art. 19 b ust. 3 ustawy informatyzacji, w myśl której, organy administracji publicznej przekazują do centralnego repozytorium wzory dokumentów dotyczących świadczonych przez jednostkę usług elektronicznych.

Jak wyjaśnił Starszy informatyk Urzędu w związku z wykonywaniem bieżących podstawowych czynności przypisanych do stanowiska informatyka w Urzędzie nie był on w stanie sporządzić wzorów zgodnych z wymaganiami centralnego repozytorium. W okresie od maja 2012 r. do sierpnia 2014 r. priorytetem było opracowanie dokumentów wykorzystywanych na potrzeby usług opisanych na stronie internetowej Urzędu. Ponieważ karty usług ulegały ciągłym zmianom i modyfikacjom w jego ocenie nie było sensu w przekazywaniu do repozytorium wzorów dokumentów, których kształt nie był ostateczny. Ponadto, jak wyjaśnił Burmistrz Miasta, formalne powierzenie obowiązków w powyższym zakresie miało miejsce dopiero 25 lipca 2014 r.

(dowód: akta kontroli str. 175-176, 280, 355-360)

1.10. Wspieranie modelu usługowego w zakresie świadczenia usług elektronicznych

Opis stanu faktycznego

Urząd w podstawowym stopniu wspierał model usługowy w zakresie świadczenia usług elektronicznych. W zakresie tych usług można było zidentyfikować ich właściciela. Tworzono i aktualizowano karty opisu usług. Natomiast w żadnym dokumencie nie określono maksymalnego czasu niedostępności usługi, sposobu zgłaszania awarii, podmiotów zobowiązanych do jej usunięcia, czy technicznego właściciela usługi.

(dowód: akta kontroli str. 175-176, 250, 281, 362)

1.11. Zakres i sposób współpracy systemów IT

Opis stanu faktycznego

Badaniem objęto trzy wybrane systemy działające w Urzędzie: Obsługa Urzędu Stanu Cywilnego, Obsługa Ewidencji Ludności oraz Odpady komunalne.

Z systemu do obsługi Urzędu Stanu Cywilnego raz w miesiącu generowany był raport ewidencyjny ludności (ilość urodzeń, małżeństw i zgonów) poprzez otwarte łącze baz danych (ODBC) do serwera Głównego Urzędu Statystycznego. System wymagał ręcznego uruchamiania tej funkcji przez pracownika, tzn. komunikacja była jednostronna. System umożliwiał zapis rejestrów do pliku w formacie XML oraz każdego generowanego wydruku do postaci pliku pdf, nie był powiązany z innymi systemami Urzędu, tym samym wewnątrz Urzędu gwarantował informacyjny poziom współpracy.

Dane osobowe z systemu Obsługa Ewidencji Ludności (OE) były przekazywane do Terenowego Banku Danych poprzez ePUAP. Dane osobowe z systemu OE do Centralnego Banku Danych (CBD) przekazywane były poprzez Portal Informacyjny Administracji (PIA). System nie był bezpośrednio skomunikowany z żadnym systemem poza Urzędem. Komunikacja zwrotna do Urzędu przychodziła z CBD i obejmowała informacje z numerami PESEL (w pliku txt) również za pośrednictwem PIA. Wszelkie czynności wymagały aktywności pracownika w systemie. Ponadto system umożliwiał zapis danych w postaci pliku txt. Stwierdzono, że dane z systemu Urzędu Stanu Cywilnego nie mogły być importowane do systemu Ewidencji ludności. Pracownik Urzędu musiał wprowadzać je ręcznie, a współpraca między systemami była na poziomie informacyjnym.

W systemie Odpady komunalne dokonywano wymiaru opłat i przypisu deklaracji. System był powiązany poprzez pliki XML z systemem Finansowo Księgowym Urzędu (jednostronna komunikacja) oraz systemem KASA w zakresie podglądu wpłat (transakcyjny poziom współpracy). System był przygotowany do eksportu danych w postaci pliku csv dla firm wywożących odpady. Ponadto system był powiązany z aplikacją Masowe płatności (jednostronna komunikacja).

(dowód: akta kontroli str. 195-231)

Badane systemy informatyczne spełniały minimalne wymogi interoperacyjności[9] w zakresie współpracy z innymi systemami Urzędu, określone w § 5 ust. 3 pkt 3 rozporządzenia w sprawie KRI.

1.12. Procedury i praktyki postępowania stosowane we współpracy z innymi jednostkami administracji publicznej

Opis stanu faktycznego

Burmistrz wyjaśnił, że Urząd prowadził komunikację elektroniczną z innymi jednostkami administracji publicznej za pomocą:

- portali internetowych (Portal Informacyjny Administracji, Centralna Ewidencja Pojazdów i Kierowców - CEPiK, Portal Zamówień Publicznych Wspólnoty Europejskiej SIMAP, Ekoportal),
- rejestru dowodów osobistych,
- platformy internetowej ePUAP,
- programów służących do wymiany informacji (Płatnik, Besti@, Quicksoft),
- systemów informacyjnych, sprawozdawczych (PFRON, GUS, SIO),
- poczty elektronicznej.

(dowód: akta kontroli str. 112-113, 181-183)

Ponadto jak wyjaśnił Burmistrz, z wnioskiem do Urzędu o prowadzenie wzajemnej komunikacji elektronicznej zwracał się Małopolski Urząd Wojewódzki. Komunikacja ta funkcjonuje, przy czym oprócz formy elektronicznej prowadzona jest również w formie tradycyjnej. Urzędy Skarbowe zwracały się do Urzędu z prośbą o podanie adresu na platformie ePUAP w celu przekazywania sprawozdań budżetowych. Urząd nie występował do innych podmiotów administracji publicznej z inicjatywą komunikacji elektronicznej.

(dowód: akta kontroli str. 180, 355)

Zgodnie z wyjaśnieniami Burmistrza, Urząd prowadził elektroniczną komunikację z innymi instytucjami poprzez przekazywanie danych obejmujących:

- informacje związane z aktami stanu cywilnego,
- formularze zgłoszeniowe takie jak ZUA, ZZA, ZCNA, ZIUA, ZWUA, IWA, formularze rozliczeniowe jak DRA, RCA, RZA, RSA,
- deklaracje DEK-a i DEK-I-a, informacje o ilości zatrudnionych osób i kwocie do zapłaty dla PFRON
- sprawozdania budżetowe, m.in. Rb-27S, Rb-28S, Rb-N, Rb-Z, Rb-30, Rb-34S, Rb-50,
- dane identyfikacyjne podmiotów gospodarczych,
- dane wnioskodawców i członków ich rodzin w zakresie Karty Dużej Rodziny,
- akty prawne podlegające publikacji w Małopolskim Dzienniku Urzędowym Województwa Małopolskiego,
- dane do Systemu Informacji Oświatowej obejmujące m.in. ilość uczniów, nauczycieli, majątku szkoły i jej wydatków,
- informacje o liczbie placówek świadczących usługi opieki nad dziećmi do lat 3,
- wnioski o wydanie dowodów osobistych,
- wysyłanie i odbieranie przelewów (w tym Masowe płatności),
- informacje o zamówieniach publicznych,
- informacje o decyzjach środowiskowych, zawierające dane wnioskodawcy, oznaczenie nieruchomości,
- dane o numerach rejestracyjnych i markach pojazdów, informacja zwrotna obejmowała dane właściciela pojazdu,
- informacje o zmianie danych osobowych, takich jak miejsce zamieszkania, zameldowanie/wymeldowanie osoby, informacje o osobie w celu nadania numeru PESEL,

[9] Rozumianej jako zdolność różnych podmiotów oraz używanych przez nie systemów teleinformatycznych i rejestrów publicznych do współdziałania na rzecz osiągnięcia wzajemnie korzystnych i uzgodnionych celów, z uwzględnieniem współdzielenia informacji i wiedzy przez wspierane przez nie procesy biznesowe realizowane za pomocą wymiany danych za pośrednictwem wykorzystywanych przez te podmioty systemów teleinformatycznych.

- sprawozdania statystyczne, np.: AO-01, G-02b, K-09, KFT-OB/a, M-01, M-03, PP-1, SG-01-1, SG-01-2/M, SG-01-3/M, SG-01-3BZ/M, SG-01-4, SG-01-4/ZOS, Z-02, Z-03, Z-05, Z-06a, Z-14, Z-KW.

(dowód: akta kontroli str. 181-183)

Żaden z trzech badanych systemów IT działających w Urzędzie nie posiadał bezpośrednich odwołań[10] do rejestrów centralnych, zewnętrznych lub systemów informatycznych innych organów administracji publicznej. Systemy te korzystały jedynie ze zbiorów danych Urzędu. Z tego powodu, zdaniem NIK, poziom współpracy badanych systemów IT Urzędu z systemami innych urzędów administracji publicznej, należy sklasyfikować jako brak interoperacyjności, o której mowa w § 5 ust. 3 pkt 3 rozporządzenia KRI[11].

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działalność kontrolowanej jednostki w zakresie dostosowania systemów teleinformatycznych do współpracy z innymi systemami. Urząd zapewnił minimalne wymogi interoperacyjności skontrolowanych systemów informatycznych w zakresie ich współpracy wewnątrz Urzędu. W dokumentach strategicznych miasta zawarto zapisy dotyczące rozwoju usług elektronicznych, a Urząd podjął działania zmierzające do realizacji projektu „Nowoczesna administracja samorządowa". W ciągu dwóch lat od wejścia w życie rozporządzenia KRI Urząd nie zwiększył liczby usług świadczonych elektronicznie (gwarantuje jedynie kontakt za pomocą ePUAP), jednakże ponad czterokrotnie wzrosła liczba spraw, jakie klient może załatwić zdalnie za pośrednictwem ePUAP. Opisy tych usług są dla klientów dostępne w internecie i prezentują aktualne informacje zgodne ze stanem faktycznym. Nieprawidłowym było nieprzekazanie wzorów dokumentów elektronicznych do centralnego repozytorium.

2. Zarządzanie bezpieczeństwem systemów informatycznych

2.1. Aktualizacja regulacji dotyczących zmieniającego się otoczenia

Opis stanu faktycznego

Zarządzeniem Burmistrza Miasta Nowy Targ nr 0151-60/07 z 15 czerwca 2007 r. wprowadzono do stosowania w Urzędzie Politykę bezpieczeństwa i Instrukcję Zarządzania Systemem Informatycznym. Zarządzeniem nr 0151-27/10 z 1 lutego 2010 r. Burmistrz dokonał zmiany treści Polityki bezpieczeństwa. Do 22 sierpnia 2014 r. nie dokonywano żadnych zmian powyższych uregulowań.

Zgodnie z treścią Polityki bezpieczeństwa osobami odpowiedzialnymi za jej tworzenie i aktualizowanie byli: Administrator Danych Osobowych, Administrator Systemu Informatycznego, Administrator Bezpieczeństwa Informacji (ABI) oraz Sekretarz Miasta. Przyjęta w Urzędzie praktyka i podział zadań wskazywały na to, iż jedyną osoba odpowiedzialną w Urzędzie za tworzenie i aktualizację polityki bezpieczeństwa był starszy informatyk Urzędu, któremu Burmistrz powierzył funkcję Administratora Bezpieczeństwa Informacji.

(dowód: akta kontroli str. 26-43, 58-99, 141, 245, 355)

Ustalone nieprawidłowości

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

W okresie od 31 maja 2012 r. do dnia 22 sierpnia 2014 r. nie dokonano aktualizacji regulacji wewnętrznych dotyczących bezpieczeństwa informacji w zakresie zmieniającego się otoczenia. Działanie takie było niezgodne z § 20 ust. 2 pkt 1 rozporządzenia KRI.

ABI wyjaśnił, że brak powyższej aktualizacji wynikał z nadmiaru jego obowiązków. Jednakże wypełniając rekomendacje po przeprowadzonym w 2013 r. audycie bezpieczeństwa

[10] Systemy nie pobierały automatycznie danych z zewnętrznych systemów informatycznych.

[11] Przepis stanowi, że interoperacyjność na poziomie semantycznym osiągana jest m.in. poprzez stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań.

informacji do końca 2014 r. zostanie zaktualizowana polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym.

(dowód: akta kontroli str. 26-43, 58-99, 141, 245)

Zdaniem NIK, przy obecnym postępie technologicznym oraz mając na względzie zapewnienie systemowi zarządzania bezpieczeństwem informacji przydatności, adekwatności i skuteczności, uregulowania wewnętrzne w zakresie bezpieczeństwa informacji, zgodnie z zapisami pkt. 5.1.2. normy PN-ISO/IEC 17799:2007 powinny być poddawane regularnym przeglądom w zaplanowanych odstępach czasu lub w przypadku np. poważnego naruszenia bezpieczeństwa informacji, pojawienia się nowych i istotnych rodzajów ryzyka, czy też zmian regulacji prawnych dotyczących bezpieczeństwa informacji. Zgodnie z dobrymi praktykami zaleca się aktualizowanie polityki bezpieczeństwa informacji nie rzadziej niż raz na sześć miesięcy.

2.2. Sprzęt informatyczny

Opis stanu faktycznego

Urząd nie przeprowadzał inwentaryzacji zasobów informatycznych w rozumieniu ustalenia poszczególnych komponentów sprzętowych komputerów i zainstalowanego na nich oprogramowania. Przeprowadzano natomiast inwentaryzację w oparciu o art. 26 ustawy z dnia 29 września 1994 r. o rachunkowości[12].

(dowód: akta kontroli str. 172-174, 195-231, 251-263, 364-380)

Ustalone nieprawidłowości

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

Brak inwentaryzacji zasobów informatycznych Urzędu naruszał wymóg (§ 20 ust. 2 pkt 2 rozporządzenia KRI) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. Prowadzona w Urzędzie forma inwentaryzacji nie dostarczała powyższych informacji przez co nie zapewniono możliwości szybkiego odtworzenia informatycznego środowiska pracy po nagłym zdarzeniu losowym (np. pożar).
Jak wyjaśnił ABI Urząd dysponował aplikacją do inwentaryzacji sprzętu i oprogramowania. W momencie zakupu tej aplikacji klient programu został zainstalowany na wszystkich komputerach Urzędu. Jednakże z biegiem czasu klient programu został stopniowo deinstalowany ze stacji roboczych, ponieważ w miarę upływu lat bieżące aktualizacje systemów operacyjnych na stacjach roboczych w połączeniu z powyższym oprogramowaniem powodowały duże spowolnienie pracy komputerów. Co najmniej połowa komputerów Urzędu jest przestarzałych technologicznie i posiadają systemem Windows XP, który nie jest wspomagany od kwietnia 2014 r. Cykl wymiany tych urządzeń trwa w Urzędzie około 8 lat.

(dowód: akta kontroli str. 195-233, 364-380)

2.3. Analizy utraty integralności, poufności lub dostępności informacji

Opis stanu faktycznego

W załączniku nr 3 do Instrukcji Zarządzania Systemem Informatycznym (wprowadzonej w Urzędzie w 2007 r.) wymieniono 30 hipotetycznych zagrożeń informatycznych. Analiza ta obejmowała skutki zagrożenia, ewentualnie podejmowane czynności zmierzające do wyeliminowania tych skutków, koszty działania i czas przywrócenia do stanu pierwotnego oraz określenie poziomu zagrożenia.

Jak wyjaśnił ABI wszyscy pracownicy zostali zaznajomieni z powyższą instrukcją i przedmiotowym załącznikiem. Po wprowadzeniu tej Instrukcji wszystkie zdarzenia były na bieżąco monitorowane przez informatyków. Monitoring polegał na sprawdzaniu raportów na serwerach oraz podejmowaniu czynności w przypadku zgłaszania przez użytkowników nieprawidłowości w działaniu programów lub sprzętu komputerowego. Powyższych

[12] Dz. U. z 2013 r. poz. 330 ze zm.

czynności nie dokumentowano. Ponadto w badanym okresie nie wystąpił przypadek utraty integralności, poufności lub dostępności informacji.

W okresie od 31 maja 2012 r. w Urzędzie nie przeprowadzano okresowych analiz utraty integralności, poufności lub dostępności informacji.

Stosownie do wyjaśnień ABI, w oparciu o rekomendacje audytu z 2013 r. do końca 2014 roku przeprowadzona zostanie nowa analiza utraty integralności, poufności lub dostępności informacji oraz ustalone zostaną zasady dokonywania i dokumentowania takich analiz. Brak cyklicznych analiz tego rodzaju w okresie od 31 maja 2012 r. wynikał z dużej ilości obowiązków ABI. W Urzędzie zatrudnionych na pełny etat było dwóch informatyków (w tym ABI). Obsługa informatyczna sprzętu wraz z jego użytkownikami pochłaniała dużo czasu. Dodatkowe obowiązki z zakresu administracji bezpieczeństwem informacji nie pokrywały się z zakresem czynności przypisanych do stanowiska informatyka. Ponadto informatycy prowadzili również nadzór na stroną internetową Urzędu i BIP, w tym ich aktualizację.

(dowód: akta kontroli str. 233, 282-290)

Uwagi dotyczące badanej działalności

W ocenie NIK koniecznym jest przeprowadzenie ponownej analizy ryzyka utraty integralności, dostępności lub poufności informacji. Postanowienia § 20 ust. 2 pkt 3 rozporządzenia KRI nie wskazują w jakich okresach należy przeprowadzać takie analizy, jednakże należy przyjąć, iż ustalenia poczynione przez Urząd w tym zakresie w roku 2007 mogą być zdezaktualizowane ze względu na szybki postęp technologiczny w środowisku informatycznym.

2.4. Zarządzanie uprawnieniami użytkowników

Opis stanu faktycznego

Instrukcja zarządzania systemem informatycznym w Urzędzie określała m.in. zasady uzyskiwania przez pracowników dostępu do systemów informatycznych oraz zasady wyrejestrowania użytkownika z systemu informatycznego. Procedura nadawania uprawnień obejmowała przekazanie administratorowi systemu przez komórkę do spraw osobowych wniosku w postaci karty obiegowej. Jednakże powyższa instrukcja nie wskazywała zasad postępowania w sytuacji, gdy pracownik Urzędu zostaje przeniesiony na inne stanowisko pracy (wtedy w Urzędzie nie sporządza się nowej karty obiegowej). W związku z powyższym w przypadku, gdy taka zmiana pociąga za sobą konieczność pracy w innym systemie informatycznym niż dotychczas, brak jest sformalizowanych procedur postępowania. W takim przypadku administrator systemu informatycznego aktualizuje uprawnienia użytkownika w oparciu o ustne informacje przekazywane mu przez kierowników komórek organizacyjnych Urzędu.

Jak wyjaśnił ABI przyczyną braku szczegółowych procedur, dotyczących powyższego zagadnienia, jest założenie, że w przypadku zmiany stanowiska pracy osoby już zatrudnionej zmianie ulegają jedynie dostęp do dysku wydziałowego i dostęp do systemów dziedzinowych z danego wydziału.

(dowód: akta kontroli str. 32-33, 321, 361)

Kontrola uprawnień do systemów informatycznych Urzędu nadanych 15 pracownikom wykazała, że uprawnienia te odpowiadały czynnościom służbowym, jakie pracownicy wykonywali. Powyższe wypełniało wymogi § 20 ust. 2 pkt 4 rozporządzenia KRI.

Ponadto kontrolą objęto konta dziesięciu użytkowników systemów informatycznych Urzędu, którzy w badanym okresie zakończyli zatrudnienie w Urzędzie. Ich konta zostały usunięte lub zablokowane z chwilą ustania zatrudnienia, co było zgodne z § 20 ust. 2 pkt 5 rozporządzenia w sprawie KRI.
Uprawnienia były nadawane i odbierane w oparciu o sformalizowane wnioski lub karty obiegowe.
W przypadku dziesięciu poddanych oględzinom komputerów, na których realizowane były przez pracowników Urzędu zadania związane z: ewidencją ludności, obsługą Urzędu Stanu Cywilnego i gospodarowaniem odpadami komunalnymi, ich użytkownicy posiadali uprawnienia administratora, co dawało im możliwość instalowania nieautoryzowanego oprogramowania. Wśród ww. dziesięciu urządzeń sześć komputerów było przekazanych do użytkowania przez Ministerstwo Spraw Wewnętrznych i Administracji. Urząd dysponował

zgodą Ministerstwa na wykorzystanie tego sprzętu do bieżącej pracy w zakresie ewidencji ludności i Urzędu Stanu Cywilnego.

(dowód: akta kontroli str. 26-40, 148, 177-179, 322-329)

Ustalone nieprawidłowości

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

Użytkownicy systemów informatycznych niebędący pracownikami służb informatycznych posiadali uprawnienia administracyjne w związku z czym mogli samodzielnie instalować oprogramowanie na komputerach służbowych[13]. Zgodnie z zapisami normy PN-ISO/IEC 27001:2007, załącznik A, punkt A.11.2.2 pkt b) należy ograniczyć i kontrolować przyznawanie oraz korzystanie z przywilejów w systemach informatycznych według minimalnych wymagań wynikających z przydzielonych pracownikom zadań służbowych.
Jak wyjaśnił Starszy informatyk Urzędu przyjęte zasady postępowania, dające użytkownikom służbowych komputerów prawa administratora wynikały z upowszechnienia stosowania plików w formacie pdf oraz stosowania aplikacji wykorzystujących Javę. Powyższe wymusiło instalowanie na komputerach oprogramowania Adobe Reader i Java Runtime Environment. Początkowo zainstalowane oprogramowanie nie wymagało częstych modyfikacji, jednak od 2011 r. powszechnie odnotowano gwałtowny wzrost ataków na komputery użytkowników z wykorzystaniem luk w zabezpieczeniach plików pdf oraz aplikacjach Java. Jednym ze sposobów zabezpieczania się przed takimi atakami jest szybka aktualizacja programów. Jednakże mechanizmy zastosowane przez producentów oprogramowania wymagały interakcji użytkownika oraz uprawnień administracyjnych. Przy użytkowanej w Urzędzie liczbie komputerów nie był możliwy każdorazowy obchód wszystkich stanowisk i własnoręczna instalacja aktualizacji. Natomiast zdalna instalacja aktualizacji z wykorzystaniem usługi Active Directory była możliwa, ale wymagała stałego śledzenia raportów zabezpieczeń i własnoręcznego przygotowania plików poprawek w formacie msi, co nie zawsze dawało pewność funkcjonowania. W kwestii posiadanych przez użytkowników uprawnień administratora Starszy informatyk Urzędu wyjaśnił, iż konta pracowników z takimi uprawnieniami odnoszą się tylko lokalnie do danego komputera. System zabezpieczeń stosowany w Urzędzie opiera się na kontroli na poziomie Active Directory, gdzie wszyscy pracownicy mają status użytkowników domeny czyli uprawnienia ograniczone.
Burmistrz Miasta w swoich wyjaśnieniach podtrzymał powyższe stanowisko, wskazując, że przyjęty system zabezpieczeń gwarantował spełnienie wymogu § 20 ust. 2 pkt 7c rozporządzenia KRI, polegającego na zapewnieniu środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji.

(dowód: akta kontroli str. 172-174, 195-231, 239-241, 318-319)

Zdaniem NIK potrzeba ograniczenia uprawnień związana jest m.in. z ryzykiem polegającym na możliwości nieświadomego zainstalowania przez użytkowania złośliwego oprogramowania dokonanego w trakcie przeglądania stron internetowych. Oprogramowanie antywirusowe nie zawsze jest gwarancją bezpiecznej pracy w systemie informatycznym.

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę na fakt, iż zgodnie z pkt A.11.2.1. załącznika A normy PN-ISO/IEC 27001:2007 przyznawanie i odbieranie dostępu do wszystkich systemów i usług informacyjnych powinno być realizowane w oparciu o formalną procedurę rejestrowania i wyrejestrowania użytkowników.

2.5. Szkolenia pracowników przetwarzających informacje

Opis stanu faktycznego

Według stanu na 29 sierpień 2014 r. 117 pracowników Urzędu było użytkownikami komputerów stacjonarnych lub przenośnych. W latach 2012-2013 nie przeprowadzano szkoleń dla pracowników Urzędu z zakresu bezpieczeństwa informacji. Uzyskując dostęp do systemu informatycznego Urzędu, pracownicy składali oświadczenia o tym, że zostali zaznajomieni z polityką bezpieczeństwa oraz instrukcją zarządzania systemem informatycznym. Jednakże ustalenia audytu wewnętrznego przeprowadzonego w 2013 r. wskazywały na niedostateczną wiedzę pracowników Urzędu z zakresu bezpieczeństwa

[13] Sprawdzono na próbie 10 komputerów.

informacji. Zgodnie z rekomendacją audytora w planie szkoleń na 2014 r. zawarto szkolenie (w II kwartale) dla wszystkich pracowników z zakresu bezpieczeństwa informacji. W lipcu i sierpniu 2014 r. przeszkolono 48 pracowników. Szkolenia te przeprowadzał ABI.

Jak wyjaśnił ABI nadmiar obowiązków nie pozwolił mu na realizację w II kwartale 2014 r. przyjętego planu szkoleniowego. Ostatnia tura szkoleń ma odbyć się we wrześniu 2014 r. i objąć wszystkich pozostałych pracowników.

(dowód: akta kontroli str. 58-99, 184-194, 233, 310)

Ustalone nieprawidłowości

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

W okresie od 31 maja 2012 r. do czerwca 2014 r. pracownikom Urzędu, zaangażowanym w proces przetwarzania informacji, nie zapewniono szkoleń z zakresu zagrożenia bezpieczeństwa informacji, skutków naruszenia zasad bezpieczeństwa informacji oraz stosowania środków zapewniających bezpieczeństwo informacji. Było to niezgodne z § 20 ust. 2 pkt 6 rozporządzenia KRI.

(dowód: akta kontroli str. 58-99, 184-194, 233)

Burmistrz wyjaśnił, że pracownicy zaangażowani w proces przetwarzania informacji przy użyciu systemów informatycznych zostali zaznajomieni z polityką bezpieczeństwa i instrukcją zarządzania systemem informatycznym w momencie nadania uprawnień do systemu informatycznego i udzielenia upoważnienia do przetwarzania danych osobowych. Równocześnie pracownicy zostali pouczeni o konsekwencjach jakie wynikają z nieprzestrzegania przepisów z zakresu ochrony danych osobowych.

(dowód: akta kontroli str. 312)

Ustalenia audytu wewnętrznego przeprowadzonego w temacie bezpieczeństwa informacji w 2013 r. wykazały, że wśród pracowników brak było wystarczającej świadomości wagi ochrony informacji, w tym danych osobowych oraz odpowiedzialności za dane osobowe. Ponadto pracownicy wskazywali, że nie pamiętają, czy byli przeszkoleni z zakresu ochrony danych osobowych oraz czy zapoznano ich z treścią polityki bezpieczeństwa i instrukcją zarządzania systemem informatycznym.

(dowód: akta kontroli str. 80)

Zdaniem NIK powyższe wskazuje na niedostateczne działania w zakresie szkoleń dla pracowników w temacie bezpieczeństwa informacji w okresie od wejścia w życie rozporządzenia KRI do czerwca 2014 r., kiedy to rozpoczęto szkolenie pracowników.

2.6. Procedury bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość

Opis stanu faktycznego

Administrator Bezpieczeństwa Informacji wyjaśnił, że w Urzędzie nie było technicznej możliwości pracy na odległość. Użytkownik dysponujący służbowym urządzeniem przenośnym nie był w stanie pracować na serwerach Urzędu łącząc się z nimi zdalnie, jednak użytkownik taki może pracować na danych z pamięci urządzenia mobilnego. Wewnętrzne uregulowania Urzędu nie uwzględniały zasad przetwarzania danych na urządzeniach przenośnych.

W kwietniu 2014 r. w Urzędzie wprowadzono do stosowania oświadczenia pracowników o odpowiedzialności za przetwarzanie danych na urządzeniach mobilnych. W oświadczeniach tych pracownicy wskazywali, czy przetwarzają dane osobowe na takich urządzeniach oraz czy po zakończeniu pracy zabierają te Urządzenia do domu i w jaki sposób zabezpieczają je poza miejscem pracy. Treść tych oświadczeń nie regulowała zasad gwarantujących bezpieczną pracę przy mobilnym przetwarzaniu informacji.

Stosownie do złożonych oświadczeń na 34 urządzenia mobilne udostępnione pracownikom pięciu użytkowników przetwarzało dane osobowe na takich urządzeniach, a po skończonej pracy zabierało je ze sobą do domu.

(dowód: akta kontroli str. 58-99, 233-234)

Ustalone nieprawidłowości

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

Nie dochowano wymogu § 20 ust. 2 pkt 8 rozporządzenia KRI i nie ustanowiono podstawowych zasad gwarantujących bezpieczną pracę przy mobilnym przetwarzaniu informacji.

Brak takich uregulowań w obowiązującej wersji Polityki bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym wynikał (jak wyjaśnił Administrator Bezpieczeństwa Informacji) z nadmiaru jego obowiązków. Po audycie z 2013 roku trwają prace nad modyfikacją tych uregulowań. ABI nie informował pracodawcy o problemach związanych z nadmiarem obowiązków.

(dowód: akta kontroli str. 58-99, 233-234, 311)

2.7. Umowy serwisowe

Opis stanu faktycznego

W badanym okresie Miasto Nowy Targ zawarło pięć umów o sprawowanie nadzoru autorskiego lub asystę techniczną nad zakupionymi systemami do obsługi ewidencji ludności, Urzędu Stanu Cywilnego oraz odpadów komunalnych. Ponadto zawarło umowę ws. zakupu jednego z systemów. W dwóch z łącznie sześciu takich umów nie zawarto postanowień w zakresie zachowania poufności informacji przez usługodawcę. Wymóg zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji wynikał z § 20 ust. 2 pkt 10 rozporządzenia KRI.

Ponadto Miasto zawarło sześć umów, na podstawie których zakupiono komputery. W umowach tych nie wskazywano zasad zabezpieczenia informacji gromadzonych w komputerach w przypadku serwisowania takiego sprzętu. Zasady te opisano w § 14 Instrukcji zarządzania systemem informatycznym. Zgodnie z powyższym przed przekazaniem sprzętu do naprawy urządzenia informatyczne pozbawia się zapisu danych, a jeśli nie jest to możliwe, naprawy można dokonać wyłącznie pod nadzorem osoby upoważnionej przez ABI.

(dowód: akta kontroli str. 36, 264-279, 291-300, 320)

Ustalone nieprawidłowości

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

W umowach opieki autorskiej nr 240/OA/13 z 9 października 2012 r. oraz nr 253/OA/14 z 8 października 2013 r., które obejmowały koszty licencji na 2013 r. i 2014 r. m.in. systemu do obsługi ewidencji ludności oraz koszty sprawowania opieki autorskiej nad programem, nie zawarto postanowień odnośnie zachowania poufności informacji przez usługodawcę. Opieka autorska zdefiniowana została w umowie jako wsparcie merytoryczne w postaci konsultacji telefonicznych, doradztwa, szkolenia oraz usług zdalnych lub w siedzibie Urzędu.

Brak w umowach z wykonawcą zobowiązania do zachowania przez niego tajemnicy informacji był niezgodny z § 20 ust. 2 pkt 10 rozporządzenia KRI.

ABI wyjaśnił, że usługodawca nie ma dostępu do danych osobowych przetwarzanych w ewidencji ludności. Dostarcza on tylko program, który wgrany jest na serwer przez informatyków. Wsparcie merytoryczne odbywało się wyłącznie telefonicznie. Z tego powodu w przedmiotowych umowach nie zawarto postanowień odnośnie zachowania poufności informacji przez usługodawcę, a brak takiej klauzuli nie wpływa na bezpieczeństwo przetwarzania danych osobowych.

(dowód: akta kontroli str. 264-265, 296-297, 301-302, 312-313)

Zdaniem NIK okoliczności przytoczone w powyższych wyjaśnieniach nie zwalniają Urzędu z obowiązku zawierania w umowach zobowiązania do zachowania tajemnicy informacji.

2.8. Zgłaszanie incydentów naruszenia bezpieczeństwa informacji

Opis stanu faktycznego

W Urzędzie nie wprowadzono do stosowania procedur zgłaszania incydentów naruszenia bezpieczeństwa informacji. Potwierdzają to ustalenia audytu wewnętrznego przeprowadzonego w Urzędzie w 2013 r.

Zgodnie z wyjaśnieniami ABI w okresie od 31 maja 2012 r. do 25 sierpnia 2014 r. nie wystąpiły przypadki zgłaszania incydentów naruszenia bezpieczeństwa informacji.

(dowód: akta kontroli str. 26-43, 58-99, 234)

Ustalone nieprawidłowości

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

Mimo wymogu § 20 ust. 2 pkt 13 rozporządzenia KRI, obowiązującego od 31 maja 2012 r., w Urzędzie do 25 sierpnia 2014 r. nie wprowadzono do stosowania procedur zgłaszania incydentów naruszenia bezpieczeństwa informacji.

Jak wyjaśnił ABI brak sformalizowanych zapisów w powyższym zakresie wynikał z nadmiaru jego obowiązków. Jednakże prace nad aktualizacją polityki bezpieczeństwa trwają i zgodnie z planem mają zakończyć się w 2014 roku.

(dowód: akta kontroli str. 26-43, 58-99, 234)

2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

Opis stanu faktycznego

W listopadzie 2012 roku audytorzy ISO przeprowadzili w Urzędzie audyt w zakresie: rejestracji zbiorów danych osobowych wraz ze zgłaszaniem zmian, rejestru udostępnień danych osobowych, dostępu do pomieszczeń, w których przechowywane są dokumenty zawierające dane osobowe, procedur nadawania uprawnień do przetwarzania danych osobowych, tworzenia kopii zapasowych zbiorów danych, przechowywania danych na sprzęcie przenośnym, realizacji obowiązków administratora bezpieczeństwa informacji. W ramach powyższego audytu nie stwierdzono niezgodności.

W 2013 r. przeprowadzono audyt wewnętrzny z zakresu bezpieczeństwa informacji. Czynności audytu przeprowadzane były od września do listopada 2013 r., a sprawozdanie końcowe z przeprowadzenia zadania zapewniającego pn. „Bezpieczeństwo informacji w zakresie ochrony danych osobowych w Urzędzie Miasta Nowy Targ" datowane było na 31 grudnia 2013 r. Po przeprowadzeniu zadania zapewniającego audytor sformułował 24 rekomendacje. Dotyczyły one w szczególności:

1) dokonywania corocznych przeglądów Polityki Bezpieczeństwa w zakresie jej aktualizacji do zmieniającego się otoczenia,

2) uzupełnienia Polityki Bezpieczeństwa o brakujące informacje i dane,

3) dokonania szeregu zmian w Instrukcji zarządzania systemem informatycznym.

Skierowane do wykonania rekomendacje zostały zrealizowane z wyjątkiem polegających na opracowaniu lub zaktualizowaniu stosownych regulacji wewnętrznych z zakresu bezpieczeństwa informacji. Posiadały one termin wykonania do końca 2014 r. i do dnia kontroli tego zagadnienia były w trakcie realizacji.

W planie audytu wewnętrznego na 2014 r. zatwierdzonym przez Burmistrza nie przewidziano audytu bezpieczeństwa informacji dla systemu informatycznego Urzędu, natomiast zawarto w nim czynności sprawdzające w tym zakresie, dotyczące realizacji rekomendacji wydanych po przeprowadzeniu audytu w 2013 r.

Audyt ten został zaplanowany do wykonania w IV kwartale 2014 r. przez audytorów wewnętrznych ISO, co zostało ujęte w „Programie auditów w Urzędzie Miasta Nowy Targ na 2014 rok".

(dowód: akta kontroli str. 58-103, 122-140, 330-332, 339-354)

2.10. Tworzenie i testowanie kopii zapasowych danych i oprogramowania aplikacyjnego

Opis stanu faktycznego

W Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta[14] (Instrukcja) określono obowiązek codziennego tworzenia i przechowywania kopii zapasowych. Sporządzane zgodnie z przyjętą procedurą kopie nie były testowane, natomiast nośniki, na których zostały sporządzone przechowywano w serwerowni oraz w pomieszczeniu innym niż serwerownia. Pomieszczenia, w których przechowywano kopie zapasowe były zabezpieczone przed dostępem osób nieuprawnionych. Ww. kopie obejmowały dane, takie jak aplikacje użytkowe i bieżąco tworzone przez urzędników dokumenty. Natomiast kopie zapasowe baz danych Urzędu wykonywane były codziennie na drugim serwerze znajdującym się w wydzielonym pomieszczeniu Urzędu, również zabezpieczonym przed nieuprawnionym dostępem.

(dowody: akta kontroli str. 26-40, 56, 104-106)

Ustalone nieprawidłowości

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

1. Bieżące kopie zapasowe (awaryjne) dokumentów tworzonych przez użytkowników systemów teleinformatycznych Urzędu i zapisywane na dyskach sieciowych, a także programów użytkowych (bez baz danych) przechowywane były w pomieszczeniu serwerowni. Oznaczało to, iż w przypadku wystąpienia pożaru w pomieszczeniu serwerowni utracie ulegną dane przechowywane na dyskach sieciowych oraz ich najbardziej aktualne kopie zapasowe.

   Powyższe działanie było niezgodne z § 10 ust. 3 Instrukcji, gdzie zapisano „Zabrania się przechowywania kopii awaryjnych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu".

   Ponadto kopie zapasowe gromadzone w pomieszczeniu innym niż serwerownia przechowywane były na podłodze w kartonowym pudle w sposób narażający je na czynniki takie jak ogień lub zalanie wodą. Powyższe oznaczało nierzetelne realizowanie obowiązku ABI w zakresie nadzoru nad wykonywaniem kopii awaryjnych i ich przechowywaniem[15], przy czym poza przytoczonym powyżej fragmentem instrukcji obowiązujące w Urzędzie procedury nie określały szczegółowo sposobu przechowywania kopii zapasowych.

   Jak wyjaśnił ABI, odpowiedzialny m.in. za nadzorowanie wykonywania kopii awaryjnych i ich przechowywanie, kopie przechowywane w serwerowni obejmowały dane tylko z ostatniego tygodnia i były wykorzystywane na bieżąco do odtwarzania danych dla pracowników Urzędu. Natomiast w jego ocenie sposób przechowywania kopii zapasowych w pomieszczeniu poza serwerownią nie zagrażał utracie danych.

   (dowody: akta kontroli str. 26-55, 234)

Zdaniem NIK, stosowane metody fizycznego zabezpieczenia kopii zapasowych narażały je na szereg zagrożeń, jak np. pożar, zalanie. Należy zauważyć, że zgodnie z pkt. 10.5.1 normy PN-ISO/IEC 17799:2007 kopie zapasowe powinny być odpowiednio zabezpieczone fizycznie.

2. Kopie zapasowe dokumentów tworzonych przez użytkowników systemów teleinformatycznych Urzędu i zapisywane na dyskach sieciowych, a także programów użytkowych (z wyłączeniem danych) nie były testowane co do ich przydatności do odtworzenia zasobów. Jedynymi czynnościami, które potwierdzały częściową prawidłowość wykonywanych kopii były operacje przywracania danych przeprowadzane w ramach bieżącej pracy Urzędu. W okresie od początku maja do końca lipca 2014 r.

[14] Instrukcja stanowiła załącznik nr 2 do zarządzenia Burmistrza Miasta Nowy Targ nr 0151-60/07 z 15 czerwca 2007 r. w sprawie Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym.

[15] Obowiązek ten Burmistrz Nowego Targu nadał Administratorowi w § 2 ust. 5 zakresu obowiązków stanowiącego załącznik do zarządzenia nr 0151-98/05 z dnia 31 grudnia 2005 r. ws. wyznaczenia Administratora Bezpieczeństwa Informacji w Urzędzie Miasta Nowy Targ.

wystąpiły dwa przypadki przywracania części danych. Łącznie przywrócono 1,19 GB danych, co w odniesieniu do 740 GB wszystkich danych (wg stanu na 4 sierpień 2014 r.) stanowiło 0,2%.

Powyższe było niezgodne z procedurą opisaną w § 10 ust. 5 Instrukcji, gdzie wskazano, że „administrator systemu przegląda okresowo kopie awaryjne i ocenia ich przydatność do odtworzenia zasobów systemu w przypadku jego awarii". Ponadto działanie takie nie spełniało wymagania określonego w § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI, tj. minimalizowania ryzyka utraty informacji w wyniku awarii.
Stosownie do wyjaśnień ABI, odpowiedzialnego za nadzór nad okresowym sprawdzaniem kopii awaryjnych pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu[16], testy takie nie miały miejsca, ponieważ Urząd nie dysponował warunkami technicznymi do ich przeprowadzenia. Zgodnie z wyjaśnieniami Starszego informatyka, zatrudnionego w Urzędzie, aby wykonać pełny test Urząd musiałby dysponować zapasowym serwerem, ponieważ przy obecnym wykorzystaniu serwera nie ma możliwości przetestowania przywracania całej kopii bezpieczeństwa.

(dowody: akta kontroli str. 26-55, 57, 234)

2.11. Format udostępniania zasobów informacyjnych badanych systemów informatycznych

Opis stanu faktycznego

Na przykładzie wybranych do badania systemów dziedzinowych (Odpady komunalne, Obsługa Urzędu Stanu Cywilnego, Obsługa Ewidencji ludności), stwierdzono, że systemy informatyczne udostępniały zasoby informacyjne m.in. w formatach xml, txt, csv, pdf, xls, rtf, odt, ods (po wygenerowaniu pliki można było zapisać w ww. formatach). Tym samym spełniony został warunek określony w załączniku nr 2 do rozporządzenia KRI o konieczności zapisywania danych w co najmniej w jednym z formatów wymienionych w KRI.

(dowód: akta kontroli str. 177-179)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie działalność Urzędu w zakresie wdrażania systemu zarządzania bezpieczeństwem systemów informatycznych, ponieważ nie spełniono szeregu istotnych wymogów przewidzianych w § 20 ust. 2 rozporządzenia KRI w powiązaniu z normami PN-ISO/IEC 17799:2007 i PN-ISO/IEC 27001:2007. I tak:

- w badanym okresie Urząd nie realizował obowiązku zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia,
- nie przeprowadzano inwentaryzacji składników sprzętu komputerowego i zainstalowanego na nim oprogramowania,
- użytkownikom dziesięciu komputerów (poddanych oględzinom) pozostawiono możliwość instalacji nieautoryzowanego oprogramowania,
- nie przeszkolono wszystkich pracowników zaangażowanych w proces przetwarzania informacji,
- nie ustalono zasad (procedur) gwarantujących bezpieczną pracę przy przetwarzaniu danych z wykorzystaniem urządzeń mobilnych,
- nie wprowadzono do stosowania procedur zgłaszania incydentów naruszenia bezpieczeństwa informacji,
- nie testowano kopii zapasowych danych Urzędu w pełnym zakresie tych danych,
- kopie zapasowe przechowywane były w sposób mogący zagrozić utratą danych Urzędu w sytuacji wypadków losowych, takich jak pożar czy zalanie.

[16] Obowiązek ten wynikał z § 2 ust. 5 zakresu obowiązków Administratora Bezpieczeństwa Informacji.

3. Dostosowanie sposobu prezentacji informacji przez systemy do potrzeb osób niepełnosprawnych

Opis stanu faktycznego

Strona internetowa Urzędu działa pod adresem www.nowytarg.pl, a administrowany przez Urząd Biuletyn Informacji Publicznej pod adresem www.bip.nowytarg.pl (przekierowanie pod adres http://www.nowytarg.pl/dane.php?cid=1712). Badanie powyższych stron internetowych przy użyciu narzędzi http://validator.w3.org oraz http://jigsaw.w3.org/css-validator dotyczących spełnienia wymagań określonych w standardzie WCAG 2.0[17] w zakresie zasady 4 - Kompatybilność wykazało błędy[18].
Należy zauważyć, iż termin realizacji powyższych wymogów został określony zgodnie z § 22 ww. rozporządzenia dopiero na dzień 1 czerwca 2015 r. i NIK nie ocenia realizacji tego obowiązku na tym etapie.

(dowód: akta kontroli str. 6, 363)

Jak wyjaśnił Z-ca Burmistrza Nowego Targu Urząd zaplanował realizację obowiązku dostosowania strony internetowej i Biuletynu Informacji Publicznej do potrzeb niepełnosprawnych na IV kwartał 2014 r. i I kwartał 2015 r. Zakres prac będzie obejmował dodanie możliwości zmiany rozmiaru czcionki wyświetlanego tekstu, możliwości poruszania się po menu strony przy pomocy klawiatury, zmiany kontrastu strony, punktowego powiększania obrazu bez utraty jakości jego wyświetlania oraz dodanie możliwości odsłuchania artykułów. Rozpoczęto procedurę szacowania kosztów wdrożenia tych zmian i ujęcia ich w planie budżetu na 2015 rok.

(dowód: akta kontroli str. 7, 25)

Ocena cząstkowa

Najwyższa Izba Kontroli nie formułuje oceny cząstkowej w tym obszarze.

IV. Uwagi i 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[19], wnosi o:

1) wprowadzenie rozwiązań systemowych zapewniających ograniczenie wśród pracowników Urzędu liczby użytkowników komputerów, posiadających uprawnienia administratora;
2) przechowywanie kopii zapasowych danych z systemów informatycznych w miejscu właściwie zabezpieczonym przed wypadkami losowymi, jak np. pożar lub zalanie;
3) przyjęcie rozwiązań umożliwiających przeprowadzanie testów wykonanych kopii bezpieczeństwa danych w pełnym zakresie tych danych;
4) opracowanie i wdrożenie zasad określających sposób zgłaszania incydentów naruszenia bezpieczeństwa informacji;
5) ustanowienia zasad gwarantujących bezpieczną pracę przy mobilnym przetwarzaniu danych;
6) prowadzenie aktualnej i kompletnej inwentaryzacji sprzętu informatycznego i oprogramowania służącego do przetwarzania informacji, obejmującej ich rodzaj i konfigurację.

[17] WCAG jest standardem służącym dostosowaniu wyświetlanej treści na stronie internetowej do potrzeb osób niedowidzących. Rozwiązanie to ma na celu zapewnienie prezentacji treści w sposób ułatwiający osobom niepełnosprawnym zapoznanie się z wiadomościami. Ułatwienia te koncentrują się na sposobie wyświetlania i komunikatach głosowych.

[18] Wykryto 32 błędy i 30 ostrzeżeń w zakresie adresu http://www.nowytarg.pl/ (narzędzie http://validator.w3.org) oraz 10 błędów i 14 ostrzeżeń (narzędzie http://jigsaw.w3.org/css-validator). W odniesieniu do adresu http://www.nowytarg.pl/dane.php?cid=1712 stwierdzono 85 błędów i 33 ostrzeżenia (narzędzie pierwsze) oraz 10 błędów i 14 ostrzeżeń (narzędzie drugie). W trakcie kontroli pracownik Urzędu dokonał zmian kodu strony internetowej Urzędu w wyniku czego liczba błędów wykazywanych przez oba narzędzia spadła poniżej dziesięciu.

[19] Dz. U. z 2012 r., poz.82 ze zm.

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 Krakowie.

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.

Kraków, dnia 16 września 2014 r.

Podpisał
Marcin Kopeć
Wicedyrektor

Kontroler
Janusz Klimek
Specjalista kontroli państwowej

.....
podpis