NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie

LSZ – 411.002.01.2016
K/16/002

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie
ul. Jacka Odrowąża 1, 71-420 Szczecin
T +48 91 831 39 00, F +48 91 831 39 66
lsz@nik.gov.pl

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli

K/16/002 - Ocena postępu wdrożenia wybranych wymagań nałożonych na systemy informatyczne przez rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności – realizacja wniosków pokontrolnych z kontroli nr P/14/004.

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli
Delegatura w Szczecinie

Kontroler

Artur Matejko, st. inspektor k.p., upoważnienie do kontroli nr LSZ/2/2016 z dnia 7.04.2016 r. (dowód: akta kontroli str. 1-2)

Jednostka kontrolowana

Urząd Miasta w Szczecinku, Plac Wolności 13, 78-400 Szczecinek (dalej Urząd).

Kierownik jednostki kontrolowanej

Jerzy Hardie - Douglas, Burmistrz Miasta Szczecinek.

(dowód: akta kontroli str. 3-5)

II. Ocena kontrolowanej działalności[1]

Ocena ogólna

Burmistrz Miasta Szczecinek zrealizował wnioski zawarte w wystąpieniu pokontrolnym z dnia 3 października 2014 r., z kontroli nr 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*.[2] W Urzędzie zrealizowano zadania określone 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[3], tj.:

- dostosowano system pn. FK-2 do minimalnych wymogów interoperacyjności (stosownie do wymogu § 5 ust. 3 pkt 3 rozporządzenia KRI);
- przeprowadzano w odstępach półrocznych przeglądy postanowień Polityki bezpieczeństwa informacji;
- uniemożliwiono instalowania oprogramowania przez użytkowników niebędących pracownikami służb informatycznych (zgodnie z § 20 ust. 2 pkt 4 oraz pkt 7 lit. c rozporządzenia KRI);
- przeszkolono pracowników zaangażowanych w proces przetwarzania informacji (zgodnie z wymogiem § 20 ust. 2 pkt 6 rozporządzenia KRI).

Natomiast przy realizacji zadań określonych w rozporządzeniu KRI nie przeprowadzono w Urzędzie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, co stanowiło naruszenie § 20 ust. 2 pkt 14 rozporządzenia KRI.

[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] Wystąpienie pokontrolne z dnia 3.10.2014 r., znak LSZ-4101-011-01/2014; P/14/004.

[3] Dz.U. z 2016 r. poz. 113; zwane dalej: rozporządzeniem KRI.

III. Opis ustalonego stanu faktycznego

1. Realizacja wniosków pokontrolnych[4].

Opis stanu faktycznego

1.1. W wyniku przeprowadzonych w dniu 13.04.2016 r. oględzin ustalono, że użytkowany w Urzędzie system, służący do rejestracji mandatów pn. FK-2[5], spełniał minimalne wymogi interoperacyjności w zakresie współpracy z innymi systemami informatycznymi funkcjonującymi w Urzędzie, tj. wymogi określone w § 5 ust. 3 pkt 3 rozporządzenia KRI. Ustalono m.in., że system FK-2 komunikował się jednostronnie z systemem Besti@ służącym do zarządzania finansami w Urzędzie, poprzez funkcjonalność wyprowadzania danych w formacie xml[6].

Ponadto system FK-2 posiadał funkcjonalność (w formie komunikacji jednostronnej) zaczytywania pliku z danymi (opcja programu *Zaczytaj przypisy z programu e-mandat*). Operator systemu po otrzymaniu za pośrednictwem poczty elektronicznej zaszyfrowanego pliku od Straży Miejskiej w Szczecinku, uruchamiał ww. opcję zaczytującą automatycznie plik.

Zapis danych wyjściowych, po wygenerowaniu pliku z systemu FK-2, spełniał warunek określony w załączniku nr 2 do rozporządzenia KRI, dotyczący możliwości zapisywania danych w jednym z formatów wymienionych w tym załączniku, zgodnie z przepisem § 18 ust. 1 rozporządzenia KRI.

(dowód: akta kontroli str. 76-78)

1.2. W badanym okresie, tj. od 1 listopada 2014 r. do 18 kwietnia 2016 r., w Urzędzie obowiązywała, zatwierdzona przez Burmistrza, Polityka Bezpieczeństwa Informacji[7]. Jako administrator danych w PBI wyznaczony został Burmistrz Miasta Szczecinek. Administratorem Bezpieczeństwa Informacji wyznaczona została Joanna Gawrych, Dyrektor Wydziału Organizacyjnego[8]. Administrator Bezpieczeństwa Informacji (ABI) odpowiadał również za przegląd PBI wykonywany nie rzadziej niż raz na sześć miesięcy.

Przeglądy postanowień PBI zostały przeprowadzone przez ABI w dniach: 29-30.12.2014 r.; 6-7.07.2015 r. i 27.11.2015 r. Ustalono, że nie występowała konieczność przeprowadzenia aktualizacji PBI.

(dowód: akta kontroli str. 29-56, 60a-60b)

1.3. W wyniku przeprowadzonych w dniu 11.04.2016 r. oględzin losowo wybranych 5 z 86 stanowisk komputerowych, użytkowanych przez pracowników nienależących do służb informatycznych Urzędu, ustalono, że użytkownicy ci nie posiadali uprawnień administratora systemu na używanych przez nich komputerach. Konto „Gość" na stanowiskach komputerowych objętych oględzinami było wyłączone.[9] Osoby te nie posiadały uprawnień do zainstalowania oprogramowania, stosownie do wymogu § 20 ust. 2 pkt 4 oraz pkt 7 lit. c rozporządzenia KRI.

(dowód: akta kontroli str. 74-75)

---

[4] Kontrola nr P/14/004 przeprowadzona w III i IV kwartale 2014 r. przez Delegaturę NIK w Szczecinie w Urzędzie Miasta w Szczecinku w ramach tematu: *„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"*, w wyniku której sformułowano 4 wnioski pokontrolne.

[5] Wersja programu 1.1.9a z dnia 21.04.2015 r.

[6] W opcjach programu: *Eksport w formacie XML/Sprawozdanie o dochodach Rb-27s*; *„Eksport w formacie XML/Sprawozdanie o wydatkach Rb-28s"*.

[7] Załącznik nr 2 do zarządzenia Burmistrza Nr 65/2014 z dnia 24 czerwca 2014 r., dalej PBI.

[8] Zarządzeniem Nr 83/2015 Burmistrza Miasta Szczecinek z 30.06.2015 r. powołano Administratora Bezpieczeństwa Informacji (ABI) w Urzędzie. Uprzednio obowiązywało zarządzenie Nr 66/2014 r. z 24.06.2014 r. w sprawie wyznaczenia ABI.

[9] Zalecenia zawarte w załączniku A do normy PN-ISO/EC 27001:2013 w punkcie A.12.6.2. stanowią, ze należy ograniczyć i kontrolować przyznawanie i korzystanie z przywilejów w systemach informatycznych.

1.4. W Urzędzie przeprowadzono szkolenie dla pracowników zaangażowanych w proces przetwarzania informacji[10] w dniach 23.10. i 20.11.2014 r. Szkolenie z zakresu polityki bezpieczeństwa informacji, ochrony danych osobowych przeprowadzone zostało 23 i 24.02.2015 r.
Nowo zatrudnieni pracownicy w 2016 r. (2 osoby) zostali przeszkoleni przez ABI w zakresie szyfrowania dysków, szyfrowania kluczy USB, dostępu do systemów IT po podaniu hasła.

(dowód: akta kontroli str. 63-71)

1.5. W badanym okresie przeprowadzono trzy analizy ryzyka bezpieczeństwa informacji[11], co było zgodne z § 20 ust. 2 pkt 3 rozporządzania KRI. W ich wyniku Urząd nie stwierdził utraty poufności, dostępności oraz integralności informacji.

W latach 2015 – 2016 (do dnia zakończenia kontroli -18.04.) w Urzędzie nie przeprowadzono okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji (wymóg § 20 ust. 2 pkt 14 rozporządzenia KRI). Ostatni okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji został przeprowadzony 30.07.2014 r.

(dowód: akta kontroli str. 57-60, 84)

Ustalone nieprawidłowości

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

W okresie 2015 – 2016 (do dnia zakończenia kontroli - 18.04.) nie przeprowadzono okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, co stanowiło naruszenie § 20 ust. 2 pkt 14 rozporządzenia KRI. Zgodnie z tym przepisem, zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji nie rzadziej niż raz w roku.

(dowód: akta kontroli str. 57-60, 84)

Burmistrz Miasta Szczecinek wyjaśnił, że osobą przeprowadzającą audyt w zakresie bezpieczeństwa informacji jest Audytor wewnętrzny. W 2015 r. Pani Audytor nie przeprowadziła ww. zadania, ponieważ przebywała na zwolnieniu lekarskim, a następnie na urlopie macierzyńskim. Powyższe zadanie audytowe nie zostało ujęte w planie audytu na 2015 r. i planie audytu na 2016 r., ale zadanie audytowe w zakresie bezpieczeństwa informacji zostanie przeprowadzone w tym roku, po powrocie Pani Audytor do pracy.

(dowód: akta kontroli str. 82)

Ocena cząstkowa

Urząd zrealizował wnioski sformułowane w wystąpieniu pokontrolnym z dnia 3 października 2014 r. w związku z kontrolą nr 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.*

Ustalenia kontroli wykazały jednak nieprawidłowość przy realizacji, w badanym okresie, zadań określonych w rozporządzeniu KRI, tj. nie przeprowadzono w Urzędzie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, co stanowiło naruszenie § 20 ust. 2 pkt 14 rozporządzenia KRI.

[10] Szkolenie przeprowadzone w Urzędzie na podstawie umowy OR.2403.62.2014 r. z dnia 26.1.0.2014 r. w ramach tematu: „Ochrona danych osobowych w jednostkach samorządu terytorialnego".
[11] Analizy przeprowadzono w dniach: 30.12.2014 r., 7.07.2015 r. i 27.11.2015 r.

IV. Wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny i uwagi wynikające z ustaleń kontroli, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[12], wnosi o wykonywanie okresowych audytów wewnętrznych w zakresie bezpieczeństwa informacji.

V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ust. 1 i 2 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 Szczecinie.

Obowiązek poinformowania NIK o sposobie wykonania wniosku

Zgodnie z art. 62 ustawy o NIK proszę o poinformowanie Najwyższej Izby Kontroli, w terminie 21 dni od dnia otrzymania wystąpienia pokontrolnego, o sposobie wykonania wniosku pokontrolnego 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.

Szczecin, dnia 19 maja 2016 r.

Najwyższa Izba Kontroli
Delegatura w Szczecinie

Kontroler
Artur Matejko
st. inspektor k.p.

Dyrektor

..... *Podpis*

..... *Podpis*

[12] Dz.U. z 2015 r. poz. 1096; dalej: ustawa o NIK.