NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie

LSZ – 411.002.02.2016
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/12/2016 z dnia 20.04.2016 r. (dowód: akta kontroli str. 1-2)

Jednostka kontrolowana

Urząd Miasta w Świnoujściu, ul. Wojska Polskiego 1/5, 72-600 Świnoujście[1].

Kierownik jednostki kontrolowanej

Janusz Żmurkiewicz, Prezydent Miasta Świnoujście[2].

(dowód: akta kontroli str. 3-9)

II. Ocena kontrolowanej działalności[3]

Ocena ogólna

Prezydent Miasta zrealizował wnioski zawarte w wystąpieniu pokontrolnym z dnia 24 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*.[4] Realizując w Urzędzie 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[5]:

- wdrożono całościowo Politykę Bezpieczeństwa Informacji w zakresie określonym w § 20 ust. 1, ust. 2 pkt 1 i ust. 3 rozporządzenia KRI;
- zaprowadzono kompletną i aktualną inwentaryzację sprzętu informatycznego, obejmującą jego rodzaj i konfigurację, zgodnie z wymogiem § 20 ust. 2 pkt 2 rozporządzenia KRI;
- uniemożliwiono instalowanie oprogramowania przez użytkowników niebędących pracownikami służb informatycznych, zgodnie z § 20 ust. 2 pkt 4 oraz pkt 7 lit. c rozporządzenia KRI;
- opracowano i wdrożono procedury gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracę na odległość, stosownie do § 20 ust. 2 pkt 8 rozporządzenia KRI;

[1] Dalej Urząd.
[2] Dalej Prezydent Miasta.
[3] 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.
[4] Wystąpienie pokontrolne z dnia 24.10.2014 r., znak LSZ-4101-011-03/2014; P/14/004.
[5] Dz.U. z 2016 r. poz. 113, zwane dalej „rozporządzeniem KRI".

- w umowach serwisowych systemów EOD eKancelaria i Geo-Info zawarto zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji, zgodnie z § 20 ust. 2 pkt 10 rozporządzenia KRI;
- przeprowadzano okresowe audyty wewnętrzne w zakresie bezpieczeństwa informacji, stosownie do wymogu § 20 ust. 2 pkt 14 rozporządzenia KRI;
- dostosowano procedury tworzenia kopii zapasowych do wprowadzonych w Urzędzie rozwiązań organizacyjnych i technologicznych.

Natomiast przy realizacji zadań określonych w rozporządzeniu KRI, nieprzeprowadzono szkoleń w zakresie zachowania bezpieczeństwa informacji dla 5 pracowników Urzędu (zatrudnionych od grudnia 2015 r.), uczestniczących w procesie przetwarzania informacji, co stanowiło naruszenie § 20 ust. 2 pkt 6 rozporządzenia KRI.

III. Opis ustalonego stanu faktycznego

1. Realizacja wniosków pokontrolnych.

Opis stanu faktycznego

Realizacja 8 wniosków pokontrolnych, zawartych w wystąpieniu pokontrolnym z dnia 24.10.2014 r., miała charakter systemowy, planowy.
W Urzędzie określony został harmonogram prac dotyczących realizacji wniosków pokontrolnych oraz osoby odpowiedzialne za realizacją poszczególnych zadań. W ramach cotygodniowych narad u Sekretarza Miasta zdawana była relacja przez pracowników z realizacji zadań ujętych w harmonogramie[6].

(dowód: akta kontroli str. 222-226)

1.1. Zarządzeniem Nr 395/2015 Prezydenta Miasta z dnia 27.07.2015 r. wdrożono Politykę Bezpieczeństwa przetwarzania danych osobowych oraz Instrukcję Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie, będącą elementem systemu zarządzania bezpieczeństwem informacji w zakresie określonym w § 20 ust. 1, ust 2 pkt 1 i ust. 3 rozporządzenia KRI.

(dowód: akta kontroli str. 48-108, 211-213)

1.2. W Urzędzie przeprowadzono kompletną inwentaryzację sprzętu komputerowego, obejmującą jego rodzaj i konfigurację, przy użyciu programu komputerowego pn. Statlook[7], stosownie do wymogu § 20 ust. 2 pkt 2 rozporządzenia KRI.

(dowód: akta kontroli str. 178-180, 198-203)

W wyniku przeprowadzonych oględzin w zakresie danych sprzętowych i konfiguracji oprogramowania:
- w dniu 26.04.2016 r. dla 5 stanowisk komputerowych,
- w dniu 28.04.2016 r. obejmujących jeden serwer,

ustalono, że ujęte w prowadzonej przy użyciu oprogramowania pn. Statlook dane dotyczące rodzaju sprzętu, jego konfiguracji i oprogramowanie były aktualne i zgodne ze stanem faktycznym występującym na urządzeniach poddanych oględzinom.

(dowód: akta kontroli str. 193-197, 206-208)

1.3. W wyniku przeprowadzonych w dniu 26.04.2016 r. oględzin losowo wybranych 5 stanowisk komputerowych, nienależących do służb informatycznych Urzędu, ustalono, że użytkownicy nie posiadali uprawnień administratora systemu na używanych przez nich komputerach. Konto „Gość" na stanowiskach komputerowych

[6] W związku z realizacją zadań harmonogram był aktualizowany, ostatnią aktualizację wykonano 4.08.2015 r.
[7] Nr wersja oprogramowania 10.3.1.

objętych oględzinami było wyłączone.[8] 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. 193-197)

Objętych badaniem 5 osób (pracujących m.in. z systemami EOD eKancelaria i Geo-Info) posiadało uprawnienia do systemów odpowiadające zakresowi zadań określonych w Karcie obowiązków, uprawnień i odpowiedzialności, co było zgodne z wymogiem określonym w § 20 ust. 2 pkt 4 rozporządzenia KRI.

(dowód: akta kontroli str. 221)

1.4. Zgodnie z wymogiem § 20 ust. 2 pkt 6 rozporządzenia KRI w Urzędzie przeprowadzono szkolenia w zakresie bezpieczeństwa przetwarzania informacji oraz wymogów wynikających z wprowadzonej zarządzeniem Prezydenta Miasta z 27.07.2015 r. Polityki Bezpieczeństwa przetwarzania danych osobowych i Instrukcji Zarządzenia Systemami Informatycznymi Urzędu[9]. Szkolenie wewnętrzne w tym zakresie przeprowadzone zostało przez Administratora Bezpieczeństwa Informacji Urzędu[10]. Każdorazowo szkolenie kończone było testem sprawdzającym.

Dodatkowo z zakresu polityki bezpieczeństwa informacji i ochrony danych osobowych przeprowadzone zostało szkolenie 13.03.2015 r. przez Fundację Rozwoju Demokracji Lokalnej[11].

(dowód: akta kontroli str. 114-117, 217-219)

1.5. W Urzędzie opracowano i wdrożono procedury gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość[12], stosownie do § 20 ust. 2 pkt 8 rozporządzenia KRI, co potwierdzono przeprowadzonymi 26.04.2016 r. oględzinami dotyczącymi trybu i sposobu realizacji połączenia zdalnego z Urzędem.

(dowód: akta kontroli str. 190-192, 211-213)

Małgorzata Bielenis – Główny Specjalista, Administrator Bezpieczeństwa Informacji wyjaśniła: *W Urzędzie nie ma zastosowania praca przy przetwarzaniu danych w formie mobilnej i pracy na odległość przez pracowników Urzędu, pracowników służb informatycznych i kadry zarządzającej. Praca na odległość – przetwarzanie mobilne ma miejsce jedynie w przypadkach, gdy firmy informatyczne (autorzy oprogramowania użytkowanego w Urzędzie) łączą się zdalnie z wyznaczonym stanowiskiem komputerowym. (…) Aby możliwe było połączenie ze stanowiskiem komputerowym w Urzędzie muszą użyć specjalnie wygenerowanego hasła. Dostęp do niego uzyskują telefonicznie. Przebieg całego połączenia nadzorowany jest przez pracownika służb informatycznych.*

(dowód: akta kontroli str. 228)

1.6. W obowiązujących w badanym okresie[13] umowach serwisowych dotyczących serwisowania oprogramowania eKancelaria (system EOD eKancelaria)[14] oraz oprogramowania Geo-Info[15] zawarto zapisy gwarantujące odpowiedni poziom

[8] 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.

[9] Szkolenia przeprowadzono w dniach: 11.09.2015 r.; 18.09.2015 r.; 25.09.2015 r.; 8.10.2015 r.; 16.10.2015 r.; 30.10.2015 r.; 6.11.2015 r. i 13.11.2015 r. dla ogółem 202 osób.

[10] Zarządzeniem Nr 177/2014 Prezydenta Miasta z 18.03.2014 r. powołano Administratora Bezpieczeństwa Informacji w Urzędzie. Do jego zadań należało m.in. prowadzenie szkolenia wstępnego dla pracowników oraz okresowego dla poszczególnych wydziałów Urzędu.

[11] Szkolenie obejmowało m.in. bezpieczeństwo systemów komputerowych, sposób chronienia i udostępniania - szyfrowania danych informatycznych. W szkoleniu wzięło udział 40 pracowników Urzędu.

[12] Rozdział 22 i 23 wprowadzonej zarządzeniem Nr 395/2015 Prezydenta Miasta z dnia 27.07.2015 r. Polityki Bezpieczeństwa przetwarzania danych osobowych.

[13] Okres objęty kontrolą: od 1 listopada 2014 r. do dnia zakończenia czynności kontrolnych – 29.04.2016 r.

[14] Umowy z dnia 2.01.2015 r. i 20.01.2016 r.

[15] Umowy z dnia 14.01.2015 r. i 4.01.2016 r.

bezpieczeństwa informacji, stosownie do wymogu § 20 ust. 1 pkt 10 rozporządzenia KRI.

(dowód: akta kontroli str. 165-177, 214)

1.7. Za przeprowadzanie okresowych audytów stanu bezpieczeństwa i sporządzanie raportów wraz z zaleceniami oraz nadzór nad działem IT w realizacji obowiązków związanych z zabezpieczeniem danych w systemach informatycznych odpowiedzialny był Administrator Bezpieczeństwa Informacji (ABI)[16].

(dowód: akta kontroli str. 142-143)

W Urzędzie obowiązywał zaakceptowany przez Prezydenta Miasta, przedłożony przez ABI 1.12.2015 r., plan wykonania okresowych audytów w zakresie bezpieczeństwa informacji.[17]

(dowód: akta kontroli str. 146-150)

ABI sporządziła sprawozdania – raporty (w okresie grudzień 2015 r. – marzec 2016 r.), w zakresie bezpieczeństwa informacji, zgodnie z wymogiem § 20 ust. 2 pkt 14 rozporządzenia KRI, dla wydziałów i biur Urzędu[18].
Audyt w Biurze Technologii Informacyjnych Urzędu został zaplanowany przez ABI na listopad 2016 r.

(dowód: akta kontroli str. 151-164)

Małgorzata Bielenis – ABI, odpowiadając na pytanie, dlaczego pierwsze sprawozdanie z wykonania badania audytowego w Urzędzie w zakresie bezpieczeństwa informacji, było sporządzone w grudniu 2015 r., wyjaśniła: *W lipcu 2015 roku została wprowadzona nowa Polityka Bezpieczeństwa i Instrukcja Zarządzania Systemami Informatycznymi, następnie pracownicy Urzędu zostali przeszkoleni przez ABI w zakresie bezpieczeństwa przetwarzania informacji. Szkolenia trwały od września do listopada.*

(dowód: akta kontroli str. 228)

1.8. W „Instrukcji Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie”[19] wskazano w rozdziale 5 i 6 zasady tworzenia i przechowywania kopii zapasowych.

(dowód: akta kontroli str. 91-92)

Przeprowadzone 26.04.2016 r. oględziny sposobu wykonywania kopii zapasowych i ich przechowywania potwierdziły, że w Urzędzie dostosowano procedury ich tworzenia i przechowywania do istniejących rozwiązań technicznych.

(dowód: akta kontroli str. 184-189, 215-216)

Ustalone nieprawidłowości

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

W okresie 2015-2016 (do dnia zakończenia kontroli – 29.04.) Prezydent Miasta nie zapewnił przeprowadzenia szkoleń dla 5 użytkowników[20] systemów informatycznych wykorzystywanych przez Urząd, w zakresie bezpieczeństwa informacji, co stanowiło naruszenie § 20 ust. 2 pkt 6 rozporządzenia KRI. Zgodnie z tym przepisem,

[16] Zarządzeniem Nr 177/2014 Prezydenta Miasta z 18.03.2014 r. na ABI wyznaczono Małgorzatę Bielenis.
[17] Pismo znak BTI-142-1/2015 z 1.12.2015 r.
[18] Tj.: Biura Kadr, Miejskiego Rzecznika Konsumentów, Straży Miejskiej, Biura Budżetu, Biura Informacji i Konsultacji Społecznych, Samodzielnego Stanowiska ds. Gospodarki Morskiej, Biura Geodety, Biura Prawne, Biura Rady Miasta, Samodzielnego Stanowisko ds. BHP i ppoż, Biura ds. Egzekucji, Samodzielnego Stanowiska ds. Ochrony Informacji Niejawnej oraz Wydziału Komunikacji.
[19] Stanowiącej załącznik Nr 2 do wprowadzonej zarządzeniem Nr 395/2015 Prezydenta Miasta z dnia 27.07.2015 r. Polityki Bezpieczeństwa przetwarzania danych osobowych oraz Instrukcji Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie.
[20] Osoby zatrudnione w Urzędzie od dnia 1.12.2015 r.

zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. działań zapewniających szkolenie osób zaangażowanych w procesie przetwarzania informacji, ze szczególnym uwzględnieniem takich zagadnień jak: zagrożenie bezpieczeństwa informacji, skutki naruszania zasad bezpieczeństwa informacji, stosowanie środków zapewniających bezpieczeństwo informacji.

(dowód: akta kontroli str. 217, 219)

Prezydent Miasta wyjaśnił, że w dniach 2-4.05.2016 r. ABI przeprowadziła szkolenia z zakresu bezpieczeństwa informacji dla wskazanych 5 użytkowników systemów informatycznych. Jako przyczynę opóźnienia w szkoleniach Prezydent wskazał zakup i instalację sprzętu informatycznego oraz przeprowadzaną w tym czasie kompleksową jego inwentaryzację.
W dalszej części złożonych wyjaśnieniach Prezydent Miasta poinformował o podjętych działaniach organizacyjnych poprawiających standard komunikacji między Biurem Technologii Informacyjnych a Biurem Kadr, polegający na informowaniu o nowo zatrudnianych pracownikach, zmianie stanowisk lub ustaniu stosunku pracy. Od maja 2016 r. osoba przystępująca do pracy będzie zobligowana przez Biuro Kadr do zapoznania się z Polityką Bezpieczeństwa jak również będzie w tym zakresie przeszkolona przez ABI. W wyniku powyższych zmian zostanie zmodyfikowany proces dopuszczania pracowników do pracy przy stanowiskach komputerowych, wykluczający możliwość pracy bez odbycia szkolenia wymaganego § 20 ust. 2 pkt 6 rozporządzenia KRI.

(dowód: akta kontroli str. 233)

Uwagi dotyczące badanej działalności

ABI nie brała udziału w szkoleniach dotyczących przeprowadzania audytów w zakresie bezpieczeństwa systemów informatycznych; uczestniczyła w szkoleniach dotyczących przetwarzania i ochrony danych osobowych, w szkoleniach o innym zakresie problemowym.

Zarządzeniem Nr 177/2014 Prezydenta Miasta z dnia 18.03.2014 r. powołano na ABI w Urzędzie Małgorzatę Bielenis – Głównego Specjalistę w Biurze Technologii Informacyjnych. Zgodnie z ww. zarządzeniem do zadań ABI należało m.in. prowadzenie okresowych audytów stanu bezpieczeństwa informacji i sporządzanie raportów wraz z zaleceniami zmian a także nadzór nad działem IT w realizacji obowiązków związanych z zabezpieczeniem danych w systemach informatycznych.

(dowód: akta kontroli str. 142-143)

Prezydent Miasta wyjaśnił, że ABI do września 2016 r. zostanie oddelegowana na szkolenie dotyczące przeprowadzania audytów wewnętrznych.

(dowód: akta kontroli str. 233)

Ocena cząstkowa

Urząd zrealizował wnioski pokontrolne sformułowane w wystąpieniu pokontrolnym z dnia 24 października 2014 r.

Ustalenia kontroli wykazały natomiast nieprawidłowość przy realizacji, w badanym okresie, zadań określonych w rozporządzeniu KRI polegającą na nieprzeszkoleniu w zakresie bezpieczeństwa informacji 5 osób.

IV. 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 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[21] 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.

Szczecin, dnia 19 maja 2016 r.

Najwyższa Izba Kontroli
Delegatura w Szczecinie

Kontroler
Artur Matejko
st. inspektor k.p.

Dyrektor

..... *podpis*

..... *Podpis*

[21] Dz.U. z 2015 r. poz. 1096.