Białystok, dnia 23 lipca 2019 r.

PODLASKI URZĄD WOJEWÓDZKI
w BIAŁYMSTOKU
15-213 Białystok, ul. Mickiewicza 3

RE-IV.431.2.4.2019.PS

Pan
Jarosław Borowski
Burmistrz Miasta
Bielsk Podlaski

WYSTĄPIENIE POKONTROLNE

Na podstawie art. 25 ust. 1 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne w dniach 12 - 14 czerwca 2019 roku pracownicy Wydziału Programów Rządowych i Funduszy Europejskich Podlaskiego Urzędu Wojewódzkiego w Białymstoku:
1) Agata Maciuka, kierownik oddziału - upoważnienie do przeprowadzenia kontroli nr 9 znak: RE-IV.431.2.4.2019 z dnia 24 maja 2019 roku wydane z upoważnienia Wojewody Podlaskiego przez Zastępcę Dyrektora Wydziału Programów Rządowych i Funduszy Europejskich,
2) Piotr Suchocki, starszy inspektor wojewódzki - upoważnienie do przeprowadzenia kontroli nr 10 znak: RE-IV.431.2.4.2019 z dnia 24 maja 2019 wydane z upoważnienia Wojewody Podlaskiego przez Zastępcę Dyrektora Wydziału Programów Rządowych i Funduszy Europejskich, przeprowadzili kontrolę w Urzędzie Miasta Bielsk Podlaski, przy ul. M. Kopernika 1.

Przedmiot kontroli i okres objęty kontrolą:

Ocena działania i bezpieczeństwa systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych za okres od 01.01.2017 roku do dnia kontroli.

Wykonywanie zadań w kontrolowanym zakresie ocenia się pozytywnie z uchybieniami.

Podstawą powyższej oceny są dokumenty, które jednostka kontrolowana przekazała w odpowiedzi na zawiadomienie o kontroli (uzupełniony Wykaz systemów teleinformatycznych oraz uzupełniony Kwestionariusz do kontroli) oraz ustalenia szczegółowe podjęte podczas czynności kontrolnych.

Słownik:

baza konfiguracji CMDB — baza danych zarządzania konfiguracją (Configuration Management DataBase), centralny rejestr zasobów informatycznych ich konfiguracji i relacji pomiędzy elementami konfiguracji,
BI — bezpieczeństwo informacji,
dostępność — właściwość bycia dostępnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot,
integralność — zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,
KRI — Krajowe Ramy Interoperacyjności stanowią zbiór zasad i sposobów postępowania podmiotów w celu zapewnienia systemom informatycznym interoperacyjności działania, rozumianej jako zdolność tych systemów oraz wspieranych przez nie procesów do wymiany danych oraz do dzielenia się informacjami i wiedzą,
polityka bezpieczeństwa informacji, polityka BI, PBI — zestaw praw, reguł i praktycznych doświadczeń, regulujących sposób zarządzania, ochrony i dystrybucji informacji wewnątrz określonej organizacji,
poufność — zapewnienie, że informacja jest dostępna tylko dla osób do tego upoważnionych;
rozporządzenie KRI — rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247),
SZBI – system zarządzania bezpieczeństwa informacji - część całościowego systemu zarządzania oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji,
ustawa o informatyzacji — ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2019 r. poz. 700, 730).

W okresie objętym kontrolą Urząd Miasta Bielsk Podlaski wykorzystywał 6 systemów teleinformatycznych do realizacji zadań zleconych z zakresu administracji rządowej, w tym 4 systemy centralne:

1. Źródło,
2. Centralna Ewidencja i Informacja o Działalności Gospodarczej,
3. System teleinformatyczny Karty Dużej Rodziny (SI KDR),
4. System Informatyczny Wsparcia Organów Wyborczych.

Pozostałe systemy zostały pozyskane samodzielnie przez Urząd Miasta Bielsk Podlaski, są to:

1. SELWIN,
2. PB_USC.

Systemy centralne podlegały kontroli w ograniczonym zakresie.

1. Projektowanie, wdrażanie i eksploatowanie systemów teleinformatycznych:

Z uwagi na fakt, iż w jednostce nie projektuje się dedykowanych systemów teleinformatycznych, a jedynie zakupywane są gotowe już rozwiązania, kontrolerom zostały przedstawione funkcjonujące w Urzędzie Miasta Bielsk Podlaski zasady, zgodnie z którymi przygotowywane są wymagania odnośnie zamawianych systemów teleinformatycznych w zakresie: architektury systemu, sposobu licencjonowania i wykorzystania praw autorskich, zgodności z obowiązującym prawem, sposobu i poziomu zabezpieczeń, zastosowania norm i standardów przemysłowych, wydajności, poziomu niezawodności, mechanizmów kontroli i audytu, sposobu dostarczenia i instalacji systemu teleinformatycznego, wymagań sprzętowych i środowiskowych dla systemu, sposobu i zakresu testów odbiorowych, a także

warunków i kryteriów odbioru. Źródłem powyższych wymagań jest zbiór dobrych praktyk, dotychczas wypracowanych przez informatyka urzędu. Nie zostały one jednak sprecyzowane w funkcjonujących regulacjach wewnętrznych, co byłoby w pełni zgodne z uznanymi standardami.
W ramach wykonywanych czynności kontrolnych, kontrolerom przedstawiono obowiązujące w jednostce procesy ciągłego monitorowania systemów teleinformatycznych i środowiska ich pracy pod kątem wydajności i pojemności w celu zapobieżenia ewentualnym problemom z tym związanym. Działania te stanowią uzupełnienie czynności do wykonania których zobowiązuje Administratora Systemu Informatycznego w §4 *Instrukcja Zarządzania Systemem Informatycznym,* nie mają one jednak odzwierciedlenia w obowiązujących w podmiocie politykach i instrukcjach.
Z informacji uzyskanych od przedstawiciela Urzędu Miasta samodzielnie pozyskane systemy spełniają wymagania Urzędu w zakresie funkcjonalności, używalności, niezawodności i wydajności.
Z przedstawionych kontrolerom dowodów wynika, iż w kontrolowanym okresie nie odnotowano żadnych incydentów związanych z wydajnością, niezawodnością lub funkcjonalnością tych systemów. Podczas kontroli również użytkownicy przedmiotowych systemów nie sygnalizowali problemów z ich działaniem.
Z samodzielnie zakupionych przez Urząd Miasta Bielsk Podlaski systemów będących przedmiotem kontroli, system SELWIN, jest rozwijany i dostosowywany do obowiązujących przepisów prawa. Na to oprogramowanie świadczone jest wsparcie techniczne, jednostce udostępniona została najnowsza wersja oprogramowania. System PB_USC jest systemem, który został zastąpiony przez system centralny Źródło, użytkowany jest w ograniczonym zakresie (traktowany jest jako archiwum) – z tego powodu nie jest już rozwijany.
W Urzędzie Miasta Bielsk Podlaski, pomimo braku odrębnych formalnych regulacji wewnętrznych, zapewniono warunki dla uzyskania odpowiedniej funkcjonalności, niezawodności, używalności, wydajności, przenaszalności i pielęgnowalności systemów informatycznych w fazie ich projektowania (specyfikowania), wdrażania i eksploatacji, co spełnia wymagania § 15 ust. 1 rozporządzenia KRI.

Badany obszar oceniono pozytywnie.

2. Zarządzanie usługami realizowanymi przez systemy teleinformatyczne:

Poziom dostępności usług systemów objętych kontrolą (SELWIN, PB_USC), a samodzielnie zakupionych przez Urząd, w sposób szczegółowy został ustalony w umowach serwisowych: nr 2017-2003011-0069 zawartej z Technika IT S.A. oraz 133/GA/2018 zawartej z Centrum Informatyki ZETO S.A (oraz późniejszych aneksach). Zawarte umowy na serwis oprogramowania zawierają postanowienia określające poziom świadczenia tych usług np. poprzez wskazanie maksymalnych czasów reakcji, usunięcia błędów oraz zdefiniowanie grup błędów.
Według uzyskanych wyjaśnień od przedstawiciela jednostki, do chwili obecnej reakcja wykonawców na zgłaszane problemy była zgodna z oczekiwaniami i nie budziła zastrzeżeń.

Badany obszar oceniono pozytywnie.

3. Wymogi WCAG 2.0:

Systemy informatyczne wspomagające realizację zadań zleconych z zakresu administracji rządowej w Urzędzie Miasta Bielsk Podlaski nie są objęte wymogami WCAG 2.0 ze względu na brak interakcji z klientami za pośrednictwem sieci publicznej.

4. System zarządzania bezpieczeństwem informacji:

W Urzędzie ustanowiono i wdrożono *Politykę Bezpieczeństwa Informacji dla Urzędu Miasta Bielsk Podlaski* Zarządzeniem nr 81/19 Burmistrza Miasta Bielsk Podlaski z dnia 7 czerwca 2019 r. zawierającą opis struktury dokumentacji stanowiącej SZBI funkcjonującego w Urzędzie (która zastąpiła *Polityki Bezpieczeństwa Informacji dla Urzędu Miasta Bielsk Podlaski* ustanowione Zarządzeniami nr 482/18 z 12 stycznia 2018 oraz nr 589/18 Burmistrza Miasta Bielsk Podlaski z dnia 4 października 2018 r.).
Celem wprowadzonej PBI jest określenie kierunków działań oraz zapewnienie bezpieczeństwa przetwarzania i przechowywania informacji w tym zapewnienie poufności, dostępności oraz integralności informacji w komórkach organizacyjnych oraz w systemach informatycznych służących do przetwarzania informacji w Urzędzie Miasta Bielsk Podlaski.
Ustanowiony SZBI, zgodnie z Zarządzeniem, jest systemem zarządzania odnoszącym się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji.
Przedmiotowy SZBI składa się z następujących dokumentów:
1. Polityka bezpieczeństwa danych osobowych w Urzędzie Miasta Bielsk Podlaski,
2. Instrukcja zarządzania systemem informatycznym,
3. Procedura nadawania, zarządzania i użytkowania uprawnieniami do systemów teleinformatycznych,
4. Procedura oceny i zarządzania ryzykiem w obszarze ochrony informacji,
5. Zasada czystego biurka – zasady związane z zapewnieniem bezpieczeństwa informacji podczas wykonywania obowiązków służbowych,
6. Procedura postępowania z kluczami i alarmami,
7. Standard stacji roboczej,
8. Procedura testowania i wymiany akumulatorów w urządzeniach UPS,
9. Regulamin korzystania z pamięci zewnętrznych i urządzeń mobilnych,
10. Procedura szyfrowania i deszyfrowania danych osobowych przesyłanych pocztą elektroniczną,
11. Plan ciągłości działania Urzędu,
12. Procedura zarządzania incydentem,
13. Procedura postępowania w przypadku podejrzenia lub naruszenia ochrony danych osobowych,
14. Procedura tworzenia, przechowywania i niszczenia kopii bezpieczeństwa,
15. Regulamin korzystania z Internetu.
Zakres ustanowionej PBI obejmuje:
- wszystkie systemy informatyczne Urzędu,
- wszystkie pomieszczenia Urzędu, w których są przetwarzane informacje,
- wszystkich pracowników Urzędu oraz inne osoby mające dostęp do informacji przetwarzanych w Urzędzie,
- wszystkie informacje, niezależnie od formy w jakiej są przechowywane.

Funkcjonująca w Urzędzie *Polityka Bezpieczeństwa Informacji* jest poddawana okresowym przeglądom oraz doskonalona zgodnie z rozporządzeniem KRI. Jednostka dokonuje analizy dokumentacji SZBI podczas okresowych przeglądów, wykonywanych co najmniej raz w

roku, nie później niż do końca marca. Wyniki ostatniego przeglądu przedstawiono i zaakceptowano w dokumencie z 4 kwietnia 2019r. Następnie podjęto działania wynikające z przeprowadzonych analiz.
Ponadto należy zauważyć, iż w kontrolowanym okresie, w Urzędzie Miasta Bielsk Podlaski, kwestie związane z zapewnieniem BI znajdowały odzwierciedlenie w corocznych Planach Audytu:
- 2017 rok – Czynności sprawdzające zadania audytowe AU.1720.2.2015 – „Sanowanie i weryfikacja bezpieczeństwa sieci komputerowej Urzędu przy pomocy narzędzi informatycznych pod kątem ochrony danych osobowych zgodnie z rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych,
- 2018 rok - Audyt bezpieczeństwa informacji w zakresie dostosowanie zabezpieczeń i regulacji wewnętrznych wynikających z Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych – RODO)
- 2019 rok – Bezpieczeństwo informacji – sprawdzenie wymagań par. 20 ust. 2 KRI.

W jednostce dokonano inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji. Prowadzony jest rejestr zasobów teleinformatycznych (baza konfiguracji CMDB) zawierający informacje o wszystkich zidentyfikowanych aktywach informatycznych, w tym: szczegółowe dane o urządzeniach technicznych, oprogramowaniu, ich rodzaju, parametrach, aktualnej konfiguracji i relacjach między elementami konfiguracji oraz użytkowniku. Ponadto w celu optymalizacji kosztów zakupu i utrzymania oraz wdrożenia efektywnych mechanizmów kontroli i monitorowania środowiska stacji roboczych, w Urzędzie opracowano standardy stacji roboczych, których opisy stanowią Dokument nr 7 SZBI.
Badaniem, w ramach kontroli, objęto 12 stacji roboczych oraz 1 serwer. Dane dotyczące badanych stacji roboczych zawierały m.in. informacje o pokoju, w którym znajduje się urządzenie, osobie, która obsługuje komputer, okresie gwarancji i terminie jej upływu, zainstalowanym oprogramowaniu, systemie operacyjnym, parametrach technicznych (m.in. ilość pamięci, rodzaj i wielkość dysku twardego, typie procesora). Dane badanego serwera zawierały m.in. informacje o pomieszczeniu, w którym znajduje się serwer, zainstalowanych aplikacjach (data instalacji, wersja), systemie operacyjnym, parametrach technicznych. Zmiany w wykazie sprzętu, oprogramowania i konfiguracji są nanoszone na bieżąco.

W Urzędzie Miasta Bielsk Podlaski, w okresie objętym badaniem kontrolnym, zarządzano ryzykiem bezpieczeństwa informacji w oparciu analizę ryzyka w ramach funkcjonującej w Urzędzie Miasta kontroli zarządczej oraz w oparciu o *Procedurę oceny i zarządzania ryzykiem w obszarze ochrony informacji* W ramach dokonanej analizy ryzyka zidentyfikowano kluczowe zasoby informatyczne, podatności, zagrożenia, skutki tych zagrożeń, prawdopodobieństwo ich wystąpienia oraz określono sposoby postępowania z ryzykiem – w tym stosowanie zabezpieczeń je minimalizujących. Kontrolującym przedstawiono Sprawozdanie podsumowujące wyniki oceny ryzyka za 2018 rok przeprowadzonej w oparciu o *Procedurę oceny i zarządzania ryzykiem w obszarze ochrony informacji*. Jednocześnie, zgodnie z zapisami *Procedury oceny i zarządzania ryzykiem w obszarze ochrony informacji,* dodatkowym źródłem danych do monitorowania ryzyka jest proces zarządzania incydentami związanymi z bezpieczeństwem informacji. Ponadto przygotowano też stosowne procedury w celu zapewnienia ciągłości działania w przypadku awarii krytycznych zasobów.

Dodatkowo aspekty bezpieczeństwa informacji, wzięto pod uwagę również przy analizie ryzyka w kontekście bezpieczeństwa danych osobowych, dokonanej w listopadzie 2018 roku.

Pracownicy Urzędu Miasta Bielsk Podlaski, przetwarzający dane osobowe w systemach używanych do realizacji zadań z zakresu administracji rządowej, posiadają stosowne upoważnienia do przetwarzania danych osobowych.
Zakres uprawnień pracowników do przetwarzania danych w badanych systemach jest adekwatny do powierzonych im zadań i obowiązków, określonych w imiennych zakresach czynności. W czasie kontroli ustalono, iż zakres uprawnień osób zaangażowanych w przetwarzanie danych jest zmieniany, w przypadku zmiany zadań tych osób lub zakończenia pracy.

Z przedstawionych dokumentów wynika, iż Funkcjonująca w Urzędzie Miasta Bielsk Podlaski *Polityka Bezpieczeństwa Informacji,* w § 12, jako istotne dla utrzymania odpowiedniego poziomu bezpieczeństwa, wskazuje systematyczne szkolenia oraz podnoszenie kwalifikacji zawodowych pracowników. W dokumencie tym nie umieszczono jednak szczegółowych regulacji odnośnie częstotliwości i trybu prowadzenia szkoleń z zakresu bezpieczeństwa informacji. Ponadto § 11 obowiązującej w Urzędzie *Polityki* zobowiązuje odpowiednie komórki organizacyjne do zapoznania każdego nowego pracownika z obowiązującą dokumentacją SZBI. Każdy z pracowników podpisuje oświadczenie o stosowaniu się do zasad określonych w SZBI.
Jednostka przedstawiła podczas kontroli dokumentację z przeprowadzonych w okresie objętym kontrolą szkoleń z zakresu ochrony danych osobowych i bezpieczeństwa informacji. Zakres przeprowadzonych dla pracowników szkoleń nie był w całości zgodny z wymaganiami w tym zakresie zawartymi w rozporządzeniu Rady Ministrów z dnia 13 kwietnia 2012r. w sprawie KRI – ich tematyka skupiała się głównie na zagadnieniach związanych z ochroną danych osobowych. Cykl szkoleń z zakresu ochrony bezpieczeństwa danych osobowych i bezpieczeństwa informacji odbyło tylko kilka osób z kadry zarządczej. Zapowiedzią zmian w powyższym zakresie jest uwzględnienie w planie szkoleń pracowników Urzędu Miasta Bielsk Podlaski na rok 2019 szkoleń z zakresu bezpieczeństwa danych oraz cyberbezpieczeństwa dla większej grupy pracowników Urzędu.

Przetwarzane informacje w ramach badanych systemów teleinformatycznych są chronione przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, poprzez:
- monitorowanie dostępu do informacji,
- czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
- środki uniemożliwiające nieautoryzowany dostęp na poziomie: systemów operacyjnych, usług sieciowych i aplikacji, m.in. poprzez następujące zabezpieczenia:
- stosowanie urządzenia typu firewall, które stanowi jedyne połączenie z siecią zewnętrzną,
- podział fizyczny sieci – wydzielenie sieci dedykowanej obsłudze systemu Źródło,
- blokowanie prób nieupoważnionego dostępu,
- inspekcja ruchu sieciowego,
- wdrożenie oprogramowania antywirusowego i systematyczne kontrole stacji roboczych i serwerów, zgodnie z § 4 *Instrukcji zarządzania systemem informatycznym*.
- stosowanie zasilaczy awaryjnych UPS, których celem jest zapobieganie minimalizowania ryzyk związanych z awarią zasilania lub zakłóceniami w sieci zasilającej. W celu zapewnienia odpowiedniej sprawności urządzeń podtrzymujących zasilanie, została wdrożona *Procedura testowania i wymiany akumulatorów w urządzeniach UPS.*

Wchodzące w skład SZBI dokumenty (m.in. *Instrukcja zarządzania systemem informatycznym, Procedura nadawania, zarządzania i użytkowania uprawnieniami do systemów teleinformatycznych, Zasada czystego biurka – zasady związane z zapewnieniem bezpieczeństwa informacji podczas wykonywania obowiązków służbowych, Procedura postępowania z kluczami i alarmami, Regulamin korzystania z pamięci zewnętrznych i urządzeń mobilnych, Procedura szyfrowania i deszyfrowania danych osobowych przesyłanych pocztą elektroniczną, Procedura zarządzania incydentem, Procedura postępowania w przypadku podejrzenia lub naruszenia ochrony danych osobowych, Regulamin korzystania z Internetu*), uwzględniają regulacje wewnętrzne, w których ustalono zasady postępowania z informacjami zapewniając minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji oraz zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami.
Przedstawione zostały czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji m.in. poprzez kontrolę logów systemów, oraz bieżący monitoring stacji roboczych przy użyciu dedykowanego oprogramowania. Oprogramowanie to pozwala na bieżący monitoring i analizę statystyczną działań użytkowników, wykorzystywanych przez nich aplikacji, zarządzanie (blokowanie) nośnikami wymiennymi, monitorowanie wydruków, w tym zbieranie szczegółowych informacji o drukowanych dokumentach. Monitorowana jest także aktywność pracowników w Internecie.

W jednostce stosowane są mechanizmy kontroli dostępu do badanych systemów w postaci identyfikatorów i haseł dla każdego użytkownika, a w przypadku Systemu Źródło, imienne karty dostępu. W funkcjonującej w Urzędzie Procedurze, stanowiącej Dokument nr 3 SZBI, szczegółowo opisano zasady przyznawania i używania kont oraz zmiany haseł stosowanych do uwierzytelniania użytkowników. Zasady te wdrożono zarówno w odniesieniu do aplikacji jak i systemów operacyjnych. Urząd posiada wdrożoną usługę katalogową opartą o SAMBA. Usługa ta pozwalała na kontrolę i zarządzanie tożsamościami i relacjami (z wyjątkiem komputerów pracujących w wydzielonej sieci, dedykowanej systemowi Źródło). W ramach czynności kontrolnych dokonano również sprawdzenia ważności kont użytkowników, których stosunek pracy wygasł w trakcie okresu objętego kontrolą i ustalono, iż przydzielone konta zostały zdezaktywowane.

Zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość w Urzędzie Miasta Bielsk Podlaski ustanowione zostały *Regulaminie korzystania z pamięci zewnętrznych na stacjach roboczych i z urządzeń mobilnych*. Z przekazanej dokumentacji wynika, iż pracownicy Urzędu nie wykorzystują zdalnych połączeń do wykonywania czynności służbowych. Kwestie dot. zdalnego serwisowania oprogramowania przez podmioty zewnętrzne zostały uregulowane w funkcjonującej w podmiocie *Procedurze zdalnego serwisu oprogramowania*. Umowy serwisowe podpisane przez Urząd ze stronami trzecimi zawierają klauzule dotyczące bezpieczeństwa informacji, w tym zapisy regulujące powierzenie przetwarzania danych osobowych.

W celu przedstawienia procedur związanych z fizyczną utylizacją nośników danych, kontrolerom przedstawiony został dokument *Potwierdzenie przetworzenia sprzętu elektronicznego*, w którym podmiot zewnętrzny, 6 lipca 2018 roku, potwierdza odebranie i utylizację 41 dysków twardych. Ponadto przedłożono także umowę z dostawcą sprzętu, w której zawarto klauzule dot. zasad przekazywania sprzętu informatycznego do naprawy, w tym pozostawienia nośników danych w urzędzie na czas naprawy w serwisie. Przedstawione

powyżej procedury związane z przechowywaniem i utylizacją sprzętu informatycznego nie zostały sformalizowane.

Jednym ze środków minimalizujących ryzyko utraty informacji w wyniku awarii, w Urzędzie Miasta Bielsk Podlaski, jest będąca elementem SZBI, *Procedura tworzenia, przechowywania i niszczenia kopii bezpieczeństwa*. Faktyczny sposób wykonywania kopii, testowania i przechowywania jest zgodny z zapisami tej polityki.

Stanowiska komputerowe wykorzystywane przy pracy z badanymi systemami są skonfigurowane w sposób zapewniający bezpieczeństwo plików systemowych. Wszyscy użytkownicy posiadają indywidualne konta o określonych prawach podstępu. Istnieją wydzielone konta administratorów. Dostęp do serwerów z bazami danych mają wyłącznie pracownicy obsługi teleinformatycznej. W trakcie czynności kontrolnych wykazano, iż badane systemy oraz systemy operacyjne, w których one funkcjonują, są na bieżąco aktualizowane. Również systemy antywirusowe oraz inne aplikacje wspierające realizację zadań (np. przeglądarka internetowa) posiadały aktualne wersje.

W ramach kontroli zweryfikowane zostały mechanizmy wymiany danych z systemem Źródło oraz zweryfikowane mechanizmy zabezpieczające sieć Urzędu Miasta Bielsk Podlaski przed nieautoryzowanym dostępem z zewnątrz.

W ramach kontroli ustalono, iż w przypadku dostrzeżenia problemów z działaniem systemów użytkownicy niezwłocznie zgłaszają problem do Informatyka Urzędu, który podejmuje niezbędne działania.
W urzędzie na wypadek naruszenia bezpieczeństwa informacji, wdrożono *Procedurę zarządzania incydentem* i jak wynika z przekazanych informacji, prowadzony jest dedykowany rejestr. Ponadto wyodrębniono specjalną *Procedurę postępowania w przypadku podejrzenia naruszenia lub naruszenia ochrony danych osobowych* wraz z dedykowanym Dziennikiem naruszeń ochrony danych osobowych.

Mając powyższe na uwadze stwierdzono następujące uchybienie:

1) niezapewnienie regularnych szkoleń, osobom zaangażowanym w proces przetwarzania informacji, uwzględniających takie zagadnienia jak:
- zagrożenia bezpieczeństwa informacji,
- skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
- stosowanie środków zapewniających bezpieczeństwo informacji.

Badany obszar oceniono pozytywnie z uchybieniem

5. Rozliczalność:

W wyniku badania stwierdzono, że w dziennikach systemów podlegających kontroli (z wyłączeniem systemów centralnych) rejestrowane są zdarzenia zgodnie z § 21 ust. rozporządzenia KRI. W dziennikach systemowych (oraz dziennikach tworzonych za pomocą dedykowanego oprogramowania) odnotowywane są działania wszystkich użytkowników zarejestrowanych w systemach, także tych z uprawnieniami administracyjnymi. Dzienniki systemów zawarte są w bazach danych i gromadzone są od momentu pierwszej instalacji systemów. Kopie zapasowe dzienników są wykonywane w ramach kopii bezpieczeństwa systemów i są składowane wraz z pozostałymi kopiami. Zapisy we wszystkich dziennikach

przechowywane są, przez co najmniej 2 lata. Podczas kontroli nie stwierdzono prowadzenia dzienników systemowych na nośniku papierowym.
Opisane powyżej zasady gromadzenia i przechowywania zapisów z dzienników systemów teleinformatycznych, w kontrolowanej jednostce, nie zostały ujęte w regulacjach wewnętrznych i opierają się na nieformalnych procedurach.

Mając powyższe na uwadze stwierdzono następujące uchybienie:
1) brak sformalizowanej procedury tworzenia kopii zapasowych dzienników systemowych.

Badany obszar oceniono pozytywnie z uchybieniem.

6. Bezpieczeństwo fizyczne:

Zasady bezpieczeństwa fizycznego przetwarzania danych w Urzędzie Miasta Bielsk Podlaski ustanowiono w ramach obowiązującego SZBI.
Kontrolowana jednostka zapewnia fizyczne bezpieczeństwo przetwarzanych informacji m.in. poprzez:
- zabezpieczenie okien budynku kratami i folią antywłamaniową,
- zabezpieczenie korytarzy na poszczególnych piętrach drzwiami przeciwpożarowymi,
- zamontowanie w kluczowych pomieszczeniach czujek dymu,
- zainstalowanie elektronicznego systemu alarmowego wewnątrz budynku oraz zawarcie umowy z firmą zewnętrzną na monitorowanie sygnałów z tego systemu,
- objęcie budynku Urzędu monitoringiem wizyjnym,
- składowanie dokumentów oraz nośników danych w szafach zamykanych na klucz, w przypadku dokumentów o szczególnym znaczeniu, przechowywanie w szafach metalowych, zamykanych na klucz
- kontrolę dysponowania kluczami do pomieszczeń (*zgodnie z Procedurą postępowania z kluczami i alarmami*),
- zamykanie pokoi na klucz, każdorazowo przy opuszczeniu przez pracownika stanowiska pracy i inne czynności do których zobowiązani są pracownicy zgodnie z funkcjonującym w Urzędzie *Dokumentem nr 5 Systemu Zarządzania Bezpieczeństwem Informacji - Zasada czystego biurka – zasady związane z zapewnieniem bezpieczeństwa informacji podczas wykonywania obowiązków służbowych*.

Podczas kontroli dokonano także oględzin pomieszczenia pełniącego rolę serwerowni. Pomieszczenie posiada klimatyzację, wyposażone jest także w czujnik ruchu i dymu. jednakże stwierdzono w nim brak systemów monitorujących parametry środowiskowe, co może mieć negatywny wpływ na znajdujące się w nim urządzenia komputerowe. Mając na uwadze umiejscowienie pomieszczenia serwerowni, należy też rozważyć wymianę znajdujących się w tym pomieszczeni drzwi na gwarantujące odpowiedni poziom bezpieczeństwa i ogniotrwałości oraz zamontowanie systemu kontroli dostępu.
Mając powyższe na uwadze stwierdzono następujące uchybienie:
1) brak bieżącego monitorowania parametrów środowiskowych pomieszczenia pełniącego funkcję serwerowni.

Badany obszar oceniono pozytywnie z uchybieniem.

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

1. Należy zapewnić szkolenia osobom zaangażowanym w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień jak:
   - zagrożenia bezpieczeństwa informacji,
   - skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
   - stosowanie środków zapewniających bezpieczeństwo informacji.
2. Należy sformalizować procedury tworzenia kopii zapasowych dzienników systemowych,
3. Należy zapewnić monitoring warunków środowiskowych (min. temperatury) w pomieszczeniu pełniącym funkcję serwerowni.

Jednocześnie proszę poinformować Wojewodę Podlaskiego, w terminie 30 dni od daty otrzymania niniejszego wystąpienia pokontrolnego o sposobie wykonania zaleceń lub wykorzystania wniosków, a także o podjętych działaniach lub przyczynach ich niepodjęcia.

Z up. WOJEWODY PODLASKIEGO
(-)
Jarosław Cezary Worobiej
Dyrektor Wydziału
Certyfikacji i Funduszy Europejskich