Prezydent Miasta Rzeszowa

Rzeszów, dnia 23 listopada 2022 r.

ORA-O.1710.9.2022

Najwyższa Izba Kontroli
Delegatura w Rzeszowie
ul. Kraszewskiego 8
35-016 Rzeszów
23.11.2022 Wiesław Motyka

Pan
Wiesław MOTYKA
Dyrektor
Najwyższa Izba Kontroli
Delegatura w Rzeszowie

W odpowiedzi na wystąpienie pokontrolne z dnia 28 października 2022 r., znak: LRZ.410.020.02.2022 przedstawiam informację o sposobie wykonania wniosków pokontrolnych oraz o podjętych działaniach:

Wniosek 1: *Ustanowienie dodatkowych mechanizmów kontrolnych oraz uzupełnienie wewnętrznych procedur i zasad dotyczących zarządzania licencjami/oprogramowaniem komputerowym.*

W ramach trwających prac nad modyfikacją wykorzystywanej obecnie Polityki Bezpieczeństwa Informacyjnego Urzędu Miasta Rzeszowa zostaną rozbudowane wewnętrzne procedury dotyczące zarządzania licencjami/oprogramowaniem komputerowym oraz zostaną ustanowione mechanizmy kontrolne umożliwiające skuteczną weryfikację procesu zarządzania licencjami/oprogramowaniem komputerowym.

SZBI będzie uzupełniony między innymi o odpowiednie zapisy tak, aby procedury odnoszące się do cyklu życia licencji i oprogramowania obejmowały także:

1) zakres koniecznej weryfikacji pod kątem wymagań bezpieczeństwa w ramach nabywania licencji;
2) ustanowienie zasad przechowywania i zabezpieczania dostępu do nośników instalacyjnych, kluczy licencyjnych i innych dokumentów licencyjnych (w tym utrzymywanych w środowiskach chmurowych);
3) ewidencjonowanie wszystkich posiadanych i używanych licencji, w tym oprogramowania nabywanego w modelu SAAS dystrybucji i redystrybucji licencji;
4) permanentne monitorowanie stanu użycia i legalności licencji oraz zasad wykonywania ich okresowych przeglądów (określenie cyklu, monitorowania poziomu wykorzystania i daty ważności - szczególnie w przypadkach czasowych subskrypcji, wymagany sposób i elementy raportowania), na wszystkich wykorzystywanych w Urzędzie Miasta Rzeszowa urządzeniach (serwery, stacje robocze, laptopy, smartfony/tablety) ze szczególnym nadzorem jednostek użytkowników posiadających uprawnienia administracyjne;
5) dokonywanie cyklicznego skanowania środowiska IT (stacje robocze, serwery, urządzenia mobilne) pod kątem identyfikacji nieautoryzowanego oprogramowania, a w przypadku jego identyfikacji przedstawiania w raportach pokontrolnych przyczyn takich sytuacji oraz (jeśli konieczne) wskazywania rekomendacji systemowych;
6) dokonywanie przeglądów lokalnych i serwerowych zasobów plikowych pod kątem przechowywania danych multimedialnych i innych plików, których magazynowanie prowadzi do naruszenia praw własności intelektualnej oraz innych treści nielegalnych.

Jednocześnie mechanizmy kontrolne umożliwiające skuteczną weryfikację procesu zarządzania licencjami/oprogramowaniem komputerowym zostaną wzmocnione przy wykorzystaniu dostępnych funkcjonalności posiadanego narzędzia *Inventory tool* zwiększając jego efektywność.

Wniosek 2: *Zapoznanie pracowników (użytkowników) z regulacjami wynikającymi z przepisów określonych w SZBI Urzędu Miasta Rzeszowa.*

W celu usunięcia powyższej nieprawidłowości zostały podjęte kompleksowe działania, których celem jest znaczne poszerzenie wiedzy pracowników z obszaru bezpieczeństwa informacyjnego. Działanie skoncentrowane są na następujących obszarach:

1) udoskonalenie wykorzystywanej obecnie Polityki Bezpieczeństwa Informacyjnego poprzez zmianę jej struktury na bardziej przejrzystą dla użytkownika końcowego;
2) modyfikację szkoleń okresowych poprzez poszerzenie w nich części dotyczącej zawartości dokumentów SZBI Urzędu Miasta Rzeszowa wraz z przeprowadzeniem szkoleń w nowej formule. Szkolenia zostaną przeprowadzone bezpośrednio po zakończeniu procedur modyfikacji dokumentów SZBI, tj. w grudniu 2022 r. Obowiązywać będą przy tym następujące zasady:

   a)szkolenie zostanie przeprowadzone w formie hybrydowej przez osobę posiadającą stosowne uprawnienia. Forma hybrydowa oznacza, że dostępne będą następujące formy udziału w szkoleniu:

   - bezpośredni udział w szkoleniu prowadzonym w sali przez wykładowcę;
   - zdalny udział w szkoleniu na stanowisku pracy za pośrednictwem transmisji sieciowej w czasie rzeczywistym;
   - odtworzenie zapisu multimedialnego szkolenia w czasie zarezerwowanym na szkolenia pracowników;

   b) każdy z pracowników Urzędu i osób współpracujących mających dostęp do zasobów systemu informacyjnego Urzędu ma obowiązek odbycia szkolenia w jednej z dostępnych form;
   c) szkolenia będą odbywać się cyklicznie;
   d) każdorazowo przygotowywane będę dodatkowe materiały szkoleniowe poszerzające wiedzę pracowników w zakresie bezpieczeństwa informacyjnego.

3) planowane jest uruchomienie platformy informatycznej do przeprowadzania szkoleń z zakresu podnoszenia świadomości bezpieczeństwa pracowników oraz symulacji ataków w celu nabycia przez pracowników praktycznych umiejętności unikania cyber-zagrożeń;

4) po przeprowadzonych szkoleniach pracowników dotyczących zapisów SZBI odebranie elektronicznych oświadczeń potwierdzających zapoznanie się pracowników z zapisami SZBI.

Wniosek 3: *Wdrożenie skutecznego nadzoru nad oprogramowaniem instalowanym na wszystkich pracujących w Urzędzie urządzeniach końcowych, przy efektywnym wykorzystaniu dostępnych narzędzi Inventory tool.*

W ramach zaawansowanych prac nad modyfikacją wykorzystywanej obecnie Polityki Bezpieczeństwa Informacji Urzędu Miasta Rzeszowa uzupełnione zostały wewnętrzne procedury dotyczące nadzoru nad oprogramowaniem instalowanym na wszystkich pracujących w Urzędzie urządzeniach (serwery, stacje robocze, laptopy, smartfony/tablety). Procedury te zostały zebrane w jeden dokument pt. *Polityka zarządzania oprogramowaniem i licencjami*. W dokumencie założono, że podstawą dbałości

o oprogramowanie instalowane zarówno na stacjonarnych jak i mobilnych komponentach systemu informacyjnego Urzędu Miasta Rzeszowa będą funkcje oferowane przez eksploatowany obecnie zestaw narzędzi *Inventory tool*. Dokument ten definiuje m. in.: obowiązek permanentnego określania ilościowego i jakościowego zakresu wykorzystania oprogramowania (ilość zainstalowanych programów wg typów, liczbę wykorzystanych licencji itp.), prawa i obowiązki użytkowników oprogramowania, zasady nadzoru nad oprogramowaniem i działaniami użytkowników oraz sposoby egzekwowania zapisów Polityki. Za zapewnienie w jednostce realizacji wymagań opisanych w przywołanej Polityce odpowiedzialny będzie wyznaczony pracownik Biura Obsługi Informatycznej i Telekomunikacyjnej (OI).

Wniosek 4: *Modyfikacja wewnętrznej procedury akceptacyjnej dopuszczającej oprogramowanie rozprowadzane na zasadach darmowych, umożliwiająca jej stosowanie w praktyce.*

W ramach trwających prac nad modyfikacją wykorzystywanej obecnie Polityki Bezpieczeństwa Informacji Urzędu Miasta Rzeszowa zostanie zmodyfikowana wewnętrzna *procedura akceptacyjna dopuszczająca oprogramowanie rozprowadzane na zasadach darmowych.*

Lista dopuszczonego darmowego oprogramowania do użytku w Urzędzie będzie utrzymywana przez Dyrektora OI i ewentualnie wyznaczonego przez niego pracownika OI, z zastosowaniem następujących zasad:

1) po zgłoszeniu przez użytkownika potrzeby wykorzystania darmowego oprogramowania. Dyrektor OI weryfikuje prawa autorskie, którymi objęty jest program, czy pozwalają one na wykorzystywanie oprogramowania darmowego do celów komercyjnych i czy zapisy umowy licencyjnej nie budzą żadnych wątpliwości;
2) w przypadku jakichkolwiek wątpliwości dotyczących strony prawnej wykorzystania programu, Dyrektor OI zwraca się o pomoc do służb prawnych Urzędu;
3) Dyrektor OI, zgodnie z dobrymi praktykami w tym zakresie, dokonuje przetestowania funkcjonalności oprogramowania, w szczególności czy realizuje ono funkcje niedostępne w eksploatowanych aktualnie programach lub przyczynia się do znaczącego obniżenia kosztów funkcjonowania systemu informacyjnego Urzędu Miasta Rzeszowa oraz sprawdzenia bezpieczeństwa instalacji i funkcjonowania programu w systemie informacyjnym Urzędu;
4) jeżeli wszystkie sprawdzenia, o których mowa powyżej, zostaną pomyślnie zakończone, oprogramowanie zostaje wpisane na listę dopuszczonego darmowego oprogramowania do użytku w Urzędzie. Dyrektor OI może również odmówić wpisania produktu na listę, co jest równoznaczne z zakazem wykorzystania go w systemie informacyjnym Urzędu Miasta Rzeszowa.

Z poważaniem,

Prezydent Miasta Rzeszowa

Konrad FIJOŁEK

Otrzymują:

1. Adresat
2. A/a

DYREKTOR BIURA OBSŁUGI INFORMATYCZNEJ I TELEKOMUNIKACYJNEJ URZĘDU MIASTA RZESZOWA
mgr inż. Lesław Bandur

SEKRETARZ MIASTA RZESZOWA
Marcin Stopa