NAJWYŻSZA IZBA KONTROLI

Delegatura w Bydgoszczy

LBY.410.016.01.2022

Piotr Całbecki
Marszałek Województwa Kujawsko-Pomorskiego
Urząd Marszałkowski
Województwa Kujawsko-Pomorskiego
Plac Teatralny 2
87-100 Toruń

WYSTĄPIENIE POKONTROLNE

P/22/082 – Zarządzanie oprogramowaniem komputerowym przez administrację publiczną

NAJWYŻSZA IZBA KONTROLI
Delegatura w Bydgoszczy
ul. Wały Jagiellońskie 12, 85-950 Bydgoszcz
T +48 52 567 58 00, F +48 52 567 58 60
lby@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana

Urząd Marszałkowski Województwa Kujawsko-Pomorskiego[1], Plac Teatralny 2, 87-100 Toruń

Kierownik jednostki kontrolowanej

Piotr Całbecki, Marszałek Województwa Kujawsko-Pomorskiego[2]

Zakres przedmiotowy kontroli

1. Organizacja, użytkowanie i nadzór nad oprogramowaniem komputerowym.
2. Optymalizacja wykorzystania oprogramowania oraz wydatków związanych z jego nabyciem i użytkowaniem.

Okres objęty kontrolą

Lata 2019 – 2022 do dnia zakończenia kontroli[3], z wykorzystaniem dowodów wytworzonych przed i po tym okresie, jeżeli miały one istotny wpływ dla ustaleń i ocen kontroli.

Podstawa prawna podjęcia kontroli

Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[4].

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli
Delegatura w Bydgoszczy

Kontrolerzy

Maciej Gajdzik, doradca techniczny, upoważnienie do kontroli nr LBY/117/2022 z 1 lipca 2022 r.

(akta kontroli str. 1)

II. Ocena[5] kontrolowanej działalności

OCENA

W Urzędzie w ograniczonym zakresie sprawowano nadzór nad oprogramowaniem. Nie weryfikowano systematycznie wszystkich posiadanych zasobów pod kątem instalowania i korzystania przez pracowników z nielegalnego oprogramowania. Prawidłowo wykorzystywano natomiast udzielone licencje do używania oprogramowania.

W latach 2019-2020 oraz pierwszych trzech kwartałach 2022 r. dokonywane zakupy oprogramowania dotyczyły produktów niezbędnych i w związku z tym - wykorzystywanych w znaczącym stopniu. W 2021 r. zakupiono dwie, niewykorzystane jak dotąd, licencje oprogramowania do wsparcia pracy zdalnej 400 użytkowników, co Najwyższa Izba Kontroli ocenia jako niegospodarne. Izba zwraca również uwagę na fakt, że bieżące analizy funkcjonalności i efektywności posiadanego oprogramowania nie zapobiegły nieprawidłowemu działaniu - szczególnie istotnego z punktu widzenia niniejszej kontroli - narzędzia do prowadzenia ewidencji oprogramowania.

[1] Dalej także: „Urząd".
[2] Dalej także: „Marszałek".
[3] Tj. 7 października 2022 r.
[4] Dz. U. z 2022 r. poz. 623, dalej: „ustawa o NIK".
[5] Najwyższa Izba Kontroli formułuje ocenę jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

Stwierdzone nieprawidłowości dotyczyły ponadto braku: wdrożenia całościowych zasad zarządzaniem oprogramowaniem; zapewnienia kompletności danych o posiadanym oprogramowaniu prowadzenia bieżącej weryfikacji wykazu programów dopuszczonych do użytkowania przypadków; usunięcia z urządzeń oprogramowania mogącego stwarzać ryzyka dla bezpieczeństwa[6]; objęcia regularnym monitorowaniem całego oprogramowania; określenia szczegółowych zasad nabywania i wykorzystywania oprogramowania użytkowanego jako usługa.

III. Opis ustalonego stanu faktycznego

Przedmiotowy zakres kontroli

1. Organizacja, użytkowanie i nadzór nad oprogramowaniem komputerowym.

1.1. W Urzędzie Marszałkowskim Województwa Kujawsko-Pomorskiego uregulowania wewnętrzne, dotyczące niektórych elementów zarządzania oprogramowaniem komputerowym, w tym: w zakresie nabywania, wdrażania, użytkowania i sprawowania nadzoru nad działalnością związaną z posiadanym oprogramowaniem komputerowym, zawarte były w regulaminach organizacyjnych, Polityce Bezpieczeństwa Informatycznego Urzędu[7], procedurach eksploatacyjnych oraz zakresach obowiązków pracowników.

Właściwymi komórkami organizacyjnymi w zakresie realizacji zadań związanych z zarządzaniem oprogramowaniem był Departament Organizacyjny oraz wchodzący w jego skład Wydział Informatyzacji Urzędu:

- zgodnie z § 21 ust. 1 pkt 43 i 44 regulaminu organizacyjnego Urzędu[8] do zakresu działania Departamentu Organizacyjnego należało w szczególności planowanie i prowadzenie działań związanych z informatyzacją Urzędu oraz nadzorowanie prawidłowej pracy sprzętu komputerowego;
- zgodnie z postanowieniami regulaminu[9] Departamentu Organizacyjnego komórką organizacyjną odpowiedzialną za zarządzanie oprogramowaniem był Wydział Informatyzacji Urzędu[10]; jego zadania obejmowały w szczególności: wdrażanie systemów informatycznych i administrowanie nimi, zapewnienie ochrony oprogramowania przed dostępem osób nieupoważnionych, nadzór i utrzymanie aplikacji systemowych, prowadzenie ewidencji licencji[11], a także - współpracę z komórką właściwą w sprawach zamówień publicznych odnośnie przygotowania dostaw materiałów i wyposażenia.

Ponadto - w Polityce Bezpieczeństwa Informatycznego uregulowano m.in. następujące kwestie, związane z zarządzaniem oprogramowaniem:

- obowiązki i uprawnienia administratorów oraz użytkowników systemów;
- monitorowanie zagrożeń (WIU);

[6] Tj. – w nieaktualnych wersjach, z lukami bezpieczeństwa, nie wymagającego instalacji, nieznajdujących się w wykazie dopuszczonego oprogramowania.
[7] Załącznik nr 4 do zarządzeń Marszałka Województwa Kujawsko-Pomorskiego w sprawie wdrożenia dokumentacji systemu zarządzania bezpieczeństwem informacji w Urzędzie Marszałkowskim Województwa Kujawsko-Pomorskiego w Toruniu – z dnia 9 lipca 2018 r. oraz z dnia 1 października 2021 r. Dalej: „Polityka Bezpieczeństwa Informatycznego".
[8] Załącznik do uchwały 6/226/18 Zarządu Województwa Kujawsko-Pomorskiego z dnia 28 grudnia 2018 r. (ze zm.).
[9] Wprowadzany zarządzeniami Marszałka z dnia 16 grudnia 2019 r., 17 czerwca 2020 r. oraz 9 maja 2022 r.
[10] Dalej także: „WIU".
[11] Jak również - monitorowanie migracji wyposażenia oraz dokonywanie związanych z tym zmian w ewidencji majątkowej oraz udział w inwentaryzacji składników majątkowych.

- sposób zabezpieczenia stanowiska komputerowego, w tym - skierowany do użytkowników zakaz instalowania i usuwania oprogramowania;
- zasady projektowania, rozwoju i utrzymania systemów informatycznych;
- wdrażanie[12] i stosowanie pisemnych procedur eksploatacyjnych[13], jako elementu zarządzania systemem informatycznym;
- ewidencjonowanie oprogramowania, jako części infrastruktury informatycznej Urzędu, przy użyciu LogSystem;
- zasady przydzielania użytkownikom elementów infrastruktury informatycznej (na podstawie zapotrzebowania, ewidencja w LogSystem, monitorowanie przez pracowników WIU);
- sposób monitorowania zgodności działania systemów informatycznych z wymogami prawa;
- wymóg monitorowania prawidłowości działania zaewidencjonowanych elementów infrastruktury informatycznej (raz na kwartał);
- sposób usuwania danych z nośników i likwidacji sprzętu.

Ład informatyczny Urzędu określany był także przez:

- wzory formularzy wewnętrznych zamówień - zawierające opis zamówienia, uzasadnienie zakupu oraz potwierdzenie celowości zamówienia;
- wzór karty obiegowej rozwiązania stosunku pracy oraz formularz systemu Mdok „Modyfikacja konta pracownika” (zdanie urządzenia wraz z oprogramowaniem).

Ponadto Dyrektor Departamentu Organizacyjnego wyjaśnił, że Polityka Bezpieczeństwa Informatycznego Urzędu wprowadzała zakaz instalowania oprogramowania przez użytkowników, a konfiguracja domeny sieciowej Urzędu faktycznie to uniemożliwiała; stanowiło to samo w sobie działanie zapobiegawcze w odniesieniu do niezgodności dotyczących zarządzania oprogramowaniem oraz nie wymagało określania wymogu realizacji przeglądów oprogramowania i licencji[14] w zakresie bezpieczeństwa.

Naczelnik Wydziału Informatyzacji podał, że (w celu ułatwienia zarządzania licencjami) w ramach zakupów oprogramowania na potrzeby Urzędu preferowane było nabywanie licencji OEM oraz - w miarę możliwości - licencji wieczystych[15].

(akta kontroli str. 59-209, 239-275, 315-318, 346-364, 371-374, 409-514)

1.2. W Urzędzie zapewniono dostępność zasobów kadrowych, niezbędnych do realizacji poszczególnych zadań w zakresie zarządzania licencjami i oprogramowaniem komputerowym.

Według stanu na dzień 13 września 2022 r. w Urzędzie zatrudnionych było ośmiu administratorów systemów informatycznych oraz pracowników świadczących pomoc techniczną w tym zakresie. Siedmiu z tych pracowników wchodziło w skład Wydziału Informatyzacji Urzędu. Ponadto w Wydziale Księgowości Funduszy Unijnych zatrudniano administratora systemu finansowo-księgowego KSAT.

[12] WIU.

[13] Wprowadzone procedury obejmowały: przygotowanie komputera dla pracownika (w tym – wykazy programów do instalacji), niszczenie dysków twardych, trwałe usuwanie danych oraz zasady napraw sprzętu.

[14] W celu potwierdzenia, że spis oprogramowania jest aktualny, kompletny oraz, że Urząd posiada licencje na każde zainstalowane oprogramowanie.

[15] Na 106 pozycji licencji ujętych w ewidencji, 85 stanowiły licencje wieczyste.

Zakresy czynności, obowiązków, uprawnień i odpowiedzialności powyższych pracowników nie zawierały postanowień dotyczących wprost odpowiedzialności za skuteczność oraz efektywność zarządzaniem oprogramowaniem komputerowym. Dokumenty te zawierały jednak ogólny wymóg dbałości o środki publiczne.

W zakresach czynności, obowiązków, uprawnień i odpowiedzialności pracowników Wydziału Informatyzacji Urzędu nie określono odpowiedzialności za wycofywanie licencji oprogramowania, ponowne wykorzystanie licencji, inwentaryzację i przeglądy licencji, nośniki i klucze instalacyjne, monitorowanie stanu użycia, ważności i legalności licencji oraz działania naprawcze w zakresie zarządzania oprogramowaniem.

Dyrektor Departamentu Organizacyjnego podał w swoich wyjaśnieniach, że zakresy czynności powyższych pracowników zawierały obowiązek prowadzenia ewidencji oprogramowania, ale nie określają szczegółowo wszystkich aspektów składających się na ten proces, w tym w zakresie odpowiedzialności objętym zapytaniem; w przypadku wydania w powyższej sprawie zaleceń pokontrolnych, podjęta zostanie analiza w celu opracowania formalnych zasad zarządzania licencjami oprogramowania, a także odpowiednio zmienione zostaną zakresy obowiązków i odpowiedzialności pracowników.

W latach 2019-2022 pięciu z powyższych pracowników odbyło łącznie osiem szkoleń zewnętrznych. Szkolenia te dotyczyły administrowania systemami komputerowymi[16]. Ich przybliżony koszt wynosił 55,7 tys. zł. Dyrektor Departamentu Organizacyjnego wyjaśnił, że szkolenia te obejmowały obsługę systemów o największym stopniu skomplikowania, których zarządzanie i bieżące utrzymanie wymagało specjalistycznej wiedzy, w szczególności w obszarze rozwiązywania pojawiających się problemów.

(akta kontroli str. 239-276, 660-668)

1.3. Ewidencję zakupionych od 2018 r. licencji i oprogramowania prowadzono w Urzędzie przy pomocy narzędzia pn. *LogSystem*[17]. Według stanu na dzień 23 września 2022 r. do aplikacji tej wprowadzono dane dla pozycji 106 licencji oprogramowania używanego przez pracowników Urzędu (łącznie 613 sztuk licencji).

Koszt wsparcia serwisowego powyższego oprogramowania w badanym okresie wynosił 174,6 tys. zł. Ustalenia dotyczące kompletności ewidencji oraz działania powyższego narzędzia opisane zostały w dalszej części niniejszego wystąpienia pokontrolnego.

Na podstawie oględzin stwierdzono, że w przypadku wybranej próby 20 zakupów licencji oprogramowania[18] - posiadano dowody zakupu, dokumenty potwierdzające legalność posiadania licencji oraz przechowywano w folderze, udostępnionym jedynie administratorom systemów.

Według stanu na 14 września 2022 r. w Urzędzie nie zainstalowano następującego oprogramowania, zakupionego w okresie od 2019 r.:

– jednej licencji programu *Acronis True 2020 PL* – nabyto dwie licencje na łącznie osiem stanowisk; we wrześniu 2022 r. wykorzystywane sporadycznie na dwóch

[16] Były to jedyne szkolenia zewnętrzne o tematyce informatycznej, w jakich w badanym okresie powyżsi pracownicy brali udział.
[17] Według stanu na dzień 22 września 2022 r. – w wersji 6.8.81. Oprogramowanie zakupione 22 grudnia 2014 r.
[18] *Winmagic SES Enterprise FFE*, *HP IMC (JG749AAE)*, *Fortinet Fortiauthenticator* – dwie licencje, *Vmware Horizon*, *Cryoserver* – dwie licencje, *Fortinet Fortitoken Mobile*, *System Informacji Prawnej Lex* – 12 licencji.

stanowiskach administratorów przy pracach serwisowych dotyczących starszych komputerów[19];

- 25 sztuk licencji systemu *Securedoc* - z nabytych 250; przewidywane było sukcesywne wykorzystanie tych licencji do końca pierwszego kwartału 2023 r.;
- licencji *Fortinet Fortitoken Mobile FTM-ELIC-200* dla 400 użytkowników.

W badanym okresie[20] w Urzędzie zakończyło pracę łącznie 240 osób. O takim zdarzeniu Wydział Informatyzacji Urzędu uzyskiwał informację na podstawie kart obiegowych rozwiązania stosunku pracy oraz na podstawie formularza „Modyfikacja konta pracownika" w systemie Mdoc. Na podstawie próby 24 komputerów - zdanych przez osoby, które przestały być pracownikami Urzędu w okresie od 1 stycznia do września 2022 r.[21] - stwierdzono, że urządzenia te były wyposażone jedynie w zestaw oprogramowania, zapewniany przez producenta sprzętu[22].

Zgodnie z wyjaśnieniami Dyrektora Departamentu Organizacyjnego, jeśli zdawane urządzenie nie nadawało się do dalszej eksploatacji – ponadstandardowe oprogramowanie było odinstalowywane.

W Urzędzie nie posługiwano się programami tworzonymi przez własnych pracowników.

(akta kontroli str. 278-293, 346-364, 371-374, 418-512, 515-557)

1.4. W Urzędzie ustalono zasady akceptowalnego użycia służbowych zasobów informatycznych – w Polityce Bezpieczeństwa Informatycznego Urzędu oraz w procedurach eksploatacyjnych.

Z treścią powyższej polityki zapoznawano pracowników podczas szkoleń wewnętrznych oraz instruktażu stanowiskowego. Dokumentacja systemu zarządzania bezpieczeństwem informacji w Urzędzie była także udostępniona pracownikom w intranecie. Potwierdzenie zapoznania się z powyższymi uregulowaniami następowało poprzez złożenie oświadczenia o poufności, gdzie zawarto także zobowiązanie do przestrzegania powyższych wymogów.

W badanym okresie Samorząd Województwa Kujawsko-Pomorskiego nie ponosił kar lub dodatkowych opłat spowodowanych nielegalnym użytkowaniem oprogramowania (przy czym producenci nie prowadzili w Urzędzie audytów oprogramowania w tym okresie).

Polityka Bezpieczeństwa Informatycznego Urzędu nie przewidywała przekazywania osobom trzecim urządzeń wraz z oprogramowaniem. W 2020 r., w związku z pandemią, przekazano jednak cztery komputery przenośne na rzecz jednego ze szpitali wojewódzkich wraz z oprogramowaniem dostarczonym przez producenta.

Ustalenia dotyczące:

- braku prowadzenia przeglądów oprogramowania i licencji pod kątem kompletności i aktualności ewidencji oprogramowania;
- weryfikacji i monitorowania, czy poszczególni użytkownicy korzystali wyłącznie z oprogramowania zapewnianego przez Urząd;

[19] Oprogramowanie nie obsługiwało dysków SSD stosowanych w nabytych później urządzeniach.
[20] W okresie od 1 stycznia 2019 r. do 5 września 2022 r.
[21] Próba ta odpowiadała liczbie wszystkich wyposażonych w komputery osób, których stosunek pracy z Urzędem zakończył się we wskazanym okresie.
[22] W 20 przypadkach urządzenia zostały przekazane kolejnym użytkownikom, zaś w pozostałych czterech przypadkach – znajdowały one się w magazynie Biura Oprzyrządowania Technicznego.

– wycofania z użycia oprogramowania, którego licencje wygasły -

zostały opisane w dalszej części niniejszego wystąpienia pokontrolnego.

(akta kontroli str. 59-112, 239-275, 295, 315-318, 346-364, 409-417, 558)

1.5. Na podstawie opisanej wyżej wybranej próby 20 zakupów licencji do oprogramowania stwierdzono, że pracownicy Urzędu korzystali z oprogramowania zgodnie z warunkami nabycia lub wymogami określających sposób użytkowania - liczba użytkowników nie przekraczała liczby nabytych licencji, a licencje te były używane w terminach ich ważności.

(akta kontroli str. 293, 515, 559-560)

Stwierdzone nieprawidłowości

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

1. W Urzędzie, w latach 2019-2022[23], nie określono szczegółowych zasad zarządzania licencjami obejmujących wszystkie elementy i wymagane czynności niezbędne do zarządzania i nadzoru nad całym cyklem życia oprogramowania, mimo wyznaczenia komórki organizacyjnej odpowiedzialnej za obsługę oprogramowania[24]. Zasady zarządzania licencjami - w rozumieniu jednostki kontrolowanej - zawierały się w Polityce Bezpieczeństwa Informatycznego, procedurach eksploatacyjnych oraz zakresach obowiązków pracowników. Zasady te nie przewidywały jednak wszystkich istotnych elementów procesu, aby zarządzanie licencjami było skuteczne i efektywne. Nie określały bowiem szczegółowych odpowiedzialności i zadań w zakresie:

   – koniecznej weryfikacji pod kątem wymagań bezpieczeństwa w podczas nabywania licencji;

   – zasad przechowywania i zabezpieczania dostępu do nośników instalacyjnych, kluczy licencyjnych i innych dokumentów licencyjnych;

   – ewidencjonowania wszystkich posiadanych i używanych licencji, w tym oprogramowania udostępnionego w chmurze;

   – dystrybucji i redystrybucji licencji;

   – monitorowania (stanu użycia i legalności licencji) oraz zasad wykonywania cyklicznych przeglądów licencji (określenie cyklu, monitorowanie poziomu wykorzystania i daty ważności - szczególnie w przypadkach czasowych subskrypcji);

   – dokonywania przeglądów na wszystkich wykorzystywanych w Urzędzie urządzeniach (serwery, stacje robocze, laptopy, smartfonach i tabletach) oraz objęcia szczególnym nadzorem hostów użytkowników posiadających uprawnienia administracyjne;

   – dokonywania cyklicznego skanowania stacji roboczych, serwerów, urządzeń mobilnych) pod kątem identyfikacji nieautoryzowanego oprogramowania, a w przypadku jego identyfikacji przedstawiania w raportach pokontrolnych przyczyn takich sytuacji oraz (jeśli konieczne) wskazywania rekomendacji systemowych;

   – dokonywania przeglądów lokalnych i serwerowych zasobów plikowych pod kątem przechowywania danych multimedialnych i innych plików, których

[23] Do 7 października 2022 r.

[24] Por. - opinia biegłego zakresie audytu systemów informatycznych oraz systemów zarządzania bezpieczeństwem informacji s. 9-11.

przechowywanie prowadzi do naruszenia praw do własności intelektualnej oraz innych treści nielegalnych, odnoszących się do całego cyklu życia licencji i oprogramowania;

- mechanizmu kontrolnego, zapewniającego, że proces instalacji lub udostępniania oprogramowania uwzględni konieczność zapoznania się osoby odpowiedzialnej za instalację z warunkami umowy licencyjnej i w przypadku wystąpienia specyficznych warunków umowy licencyjnej zapewni z nimi zgodność.

Dyrektor Departamentu Organizacyjnego podał w swoich wyjaśnieniach m.in., że:

- w dokumentacji systemu zarządzania bezpieczeństwem informacji zdefiniowano podstawowe zasady dotyczące zarządzania licencjami na oprogramowanie w obszarze dostaw oraz wykorzystywania przez użytkowników końcowych; przyjęto, być może niesłusznie, że wdrożenie odrębnej polityki zarządzania licencjami oprogramowania komputerowego nie jest niezbędne, gdyż jest to kwestia techniczna; jednocześnie w przepisach prawa nie ma wprost odniesienia, iż w tym zakresie wymagane jest przyjęcie formalnych zasad w postaci aktu normatywnego własnego;
- w przypadku wydania w tym zakresie zaleceń pokontrolnych podjęta zostanie analiza w celu opracowania formalnych zasad zarządzania licencjami oprogramowania, należy jednak uwzględnić, iż będzie to wymagało dodatkowych nakładów pracy i kosztów związanych z wdrożeniem systemu.

(akta kontroli str. 59-209, 239-275, 315-318, 409-417, 641-658, 787-801)

NIK zauważa, że brak określenia procedur - wspierających efektywne zarządzanie oprogramowaniem w zakresie nabywania, wdrażania, użytkowania i bieżącego nadzoru - pogłębiał ryzyka, związane z brakiem skutecznej zautomatyzowanej bieżącej kontroli nad posiadanym oprogramowaniem oraz brakiem podsiadania skutecznych mechanizmów nadzoru, a także monitorowania instalowania i użycia oprogramowania w czasie rzeczywistym oraz w trybie ciągłym.

2. W monitorowanych urządzeniach, należących do Urzędu, zapisane były programy, nieuwzględnione w wykazie dopuszczonego w Urzędzie oprogramowania, oraz aplikacja, która powinna była być wycofana ze względu na luki w bezpieczeństwie[25].

   Dyrektor Departamentu Organizacyjnego wyjaśnił, że:

   - *Spotify* dostępny był jako widżet[26] i domyślnie aktywowany podczas instalacji systemu operacyjnego; ponieważ aplikacja ta nie była potrzebna do wykonywania pracy na stanowiskach urzędniczych - procedura przygotowywania nowych komputerów do pracy ma zostać odpowiednio skorygowana;
   - komunikator *Signal* używany był przez pracowników Wydziału Informatyzacji Urzędu jako narzędzie uzupełniające komunikację przy przekazywaniu chronionych danych[27]; ze względu na to, że wiele czynności

[25] Por. - opinia biegłego s. 12-16.
[26] Element graficznego interfejsu użytkownika (ang. *widget*).
[27] Np. fragmentów haseł lub konfiguracji.

administracyjnych i wdrożeniowych wykonywanych by przez kilku administratorów, bieżące dzielenie się informacjami znacznie ułatwiało pracę; używanie powyższej aplikacji umożliwiało przy tym zachowanie poufności;

- *PasswordTech* nie była aplikacją działającą stale w tle jako proces; podczas oględzin wykryta została jej nieużywana i nieaktualna wersja;
- aplikacje *Napiprojekt* i *Roblox* zostały zainstalowane incydentalnie do celów prywatnych użytkownika[28] a według stanu na dzień 7 października 2022 r. zostały one usunięte;
- aplikacja *Adobe Shockwave* została zinwentaryzowana na posiadanych urządzeniach - w efekcie czego mają zostać podjęte działania w celu usunięcia instalacji tego programu ze wszystkich stanowisk komputerowych;
- instalacje aplikacji *7-Zip* oraz *Zoom* zinwentaryzowano oraz podjęto działania w celu ich aktualizacji.

(akta kontroli str. 641-658, 662-668, 787-793)

3. W Urzędzie w latach 2019-2022[29] nie prowadzono okresowych audytów lub przeglądów (skanowania):
   - hostów[30], serwerów i urządzeń mobilnych - pod kątem obecności nieautoryzowanego oprogramowania,
   - hostów i serwerów - pod kątem potwierdzania, że liczba posiadanych licencji była odpowiednia dla wykorzystywanego oprogramowania.

   Dyrektor Departamentu Organizacyjnego podał w wyjaśnieniach, że:
   - zgodnie z postanowieniami (§ 18) Polityki Bezpieczeństwa Informatycznego – dozwolone było wykorzystywanie rozwiązań komercyjnych pozyskanych wyłącznie na podstawie umowy, której treść winna gwarantować odpowiednie warunki zakupu, dostawy, instalacji, konfiguracji i uruchomienia, wdrożenia do eksploatacji oraz licencjonowania;
   - w oświadczeniu o poufności, które składał każdy pracownik, zawarto zobowiązanie do wykorzystywania jedynie legalnego oprogramowania, będącego w dyspozycji Urzędu;
   - konfiguracja domeny sieciowej Urzędu uniemożliwiała użytkownikom nieautoryzowane instalowanie oprogramowania oraz zapewniała monitorowanie stanowisk pracy;
   - w związku z powyższym przeglądy oprogramowania i licencji były prowadzone na bieżąco a każde potwierdzenie użycia danego programu w sposób nieautoryzowany, w szczególności bez wymaganej licencji, było traktowane jako incydent bezpieczeństwa.

[28] Urządzenie oznaczone numerem 1/487/4816.
[29] W okresie do dnia 7 października 2022 r.
[30] Dowolne urządzenie posiadające własny adres IP, podłączone do sieci komputerowej i uczestniczące w przesyłaniu, udostępnianiu, wymianie danych za pomocą protokołu komunikacyjnego.

NIK zauważa, że pracownicy Urzędu posługiwali się opisanymi w poprzednim punkcie niezaakceptowanymi aplikacjami[31] (w tym – nie wymagającymi instalacji przez administratora) i zdarzenia te nie były traktowane jako incydenty bezpieczeństwa.

(akta kontroli str. 61-121, 315-318, 346-364, 641-658, 662-793)

4. Prowadzony przez pracowników Wydziału Informatyzacji Urzędu spis licencji oprogramowania[32], był niekompletny. Nie obejmował on bowiem licencji oprogramowania nabytych przed 2018 r. oraz licencji niekomercyjnych[33].

   W związku z prowadzonymi przez biegłego badaniami - Naczelnik Wydziału Informatyzacji Urzędu podał, że dane w programie *LogSystem* (w spisie licencji) zdefiniowane były fragmentarycznie, tylko dla części oprogramowania, zaś spis oprogramowania i licencji zawierał informacje na temat liczby wykorzystanych i wolnych licencji jedynie dla systemów, które dostarczone zostały z konsolami centralnego zarządzania.

   NIK zwraca przy tym uwagę, że konsoli takiej, albo aplikacji zarządzania licencjami, nie posiadało jednak 60 używanych w Urzędzie odpłatnych aplikacji i systemów.

   (akta kontroli str. 299-304, 307-308, 346-364, 371-374, 561-580, 599-635)

   Narzędzie *LogSystem*[34] nie zawierało informacji o wszystkich licencjach posiadanych przez Urząd programów. Narzędzie to nie wykrywało wszystkich programów, zapisanych na stacjach roboczych, oraz nie było w stanie ujawnić faktu odinstalowania danego programu (w okresie od 19 maja 2021 r. wydatków z tytułu wsparcia tego oprogramowania wynosiły 83,0 tys. zł).

   Zgodnie z § 30 ust. 5 w zw. z § 30 ust. 2 pkt 2 Polityki Bezpieczeństwa Informatycznego Urzędu[35], oraz zgodnie z § 31 ust. 5 w zw. z § 31 ust. 2 pkt 2 Polityki Bezpieczeństwa Informatycznego Urzędu[36], ewidencja elementów infrastruktury informatycznej (w tym - oprogramowania) powinna być prowadzona przy pomocy programów *LogSystem* oraz *HP IMC*[37].

   Dyrektor Departamentu Organizacyjnego podał w swoich wyjaśnieniach, że:

   – błędy w zakresie rozpoznawania oprogramowania pojawiały się stopniowo, od początku 2020 r.; usterki te nie miały charakteru błędu, z powodu którego jednoznacznie można byłoby zakwalifikować funkcjonalność jako niesprawną; przyczyną błędów mogły być kolejne wersje (aktualizacje) popularnego systemu operacyjnego, pakietu biurowego oraz jednej z aplikacji, będącej komponentem, z którego korzystało oprogramowanie monitorujące;

[31] Tj. nie uwzględnionymi w wykazie dopuszczonego oprogramowania.
[32] Przy pomocy narzędzia *LogSystem*.
[33] Wskazanych w wykazie dopuszczonego oprogramowania (załącznik do procedury eksploatacyjnej przygotowania komputera dla pracownika) – 13 pozycji licencji instalowanych jako oprogramowanie wymagane, dziewięć pozycji licencji instalowanych fakultatywnie.
[34] W wersji 6.8.82.
[35] Załącznik nr 4 do zarządzenia nr 40/2018 Marszałka Województwa Kujawsko-Pomorskiego z dnia 9 lipca 2018 r. w sprawie wdrożenia dokumentacji systemu zarządzania bezpieczeństwem informacji w Urzędzie Marszałkowskim Województwa Kujawsko-Pomorskiego w Toruniu.
[36] Załącznik nr 4 do zarządzenia nr 68/2021 Marszałka Województwa Kujawsko-Pomorskiego z dnia 1 października 2021 r. w sprawie wdrożenia dokumentacji systemu zarządzania bezpieczeństwem informacji w Urzędzie Marszałkowskim Województwa Kujawsko-Pomorskiego w Toruniu.
[37] Narzędzie do zarządzania aplikacjami sieciowymi.

- brak prawidłowego działania powyższego systemu został zasygnalizowany przez Naczelnika Wydziału Informatyzacji Urzędu w notatce z 15 lutego 2022 r.; pracownik ten zalecił, aby dokonać zakupu funkcjonalnego oprogramowania;
- nie zapewniono środków na zakup powyższego narzędzia, ponieważ w 2022 r. nie wystąpiły oszczędności przy realizacją zakupów przewidzianych na ten rok; w sierpniu br. złożono jednak zapotrzebowanie do budżetu na następny rok;
- w związku z ustaleniami niniejszej kontroli NIK, w konsoli zarządzania programu antywirusowego włączono funkcjonalność, monitorującą aplikacje zainstalowane na stacjach roboczych; według stanu na dzień 22 września 2022 r. trwało gromadzenie danych dla tej funkcjonalności; weryfikacja prawidłowości działania programu antywirusowego w tym aspekcie ma nastąpić do końca listopada 2022 r.; przy pomocy powyższego rozwiązania uzyskana została także możliwość tworzenia okresowych raportów o aplikacjach zainstalowanych w zadanym okresie; takie wykorzystanie programu antywirusowego ma stanowić działanie uzupełniające, które ma trwać do momentu wymiany posiadanego narzędzia do monitorowania oprogramowania.

Naczelnik Wydziału Informatyzacji Urzędu - w związku z przeprowadzonymi oględzinami - podał, że wspomniany wyżej program antywirusowy nie odnotowywał faktu odinstalowania danego oprogramowania, niemniej jednak - umożliwiał przeszukanie sieci Urzędu pod kątem zainstalowania, albo braku zainstalowania danego programu.

Skutkiem braku posiadania sprawnego narzędzia do prowadzenia ewidencji licencji oprogramowania było m.in. odstąpienie od prowadzenia przeglądów oprogramowania i licencji w celu weryfikacji kompletności i aktualności tej ewidencji, nieposiadanie stałej i aktualnej wiedzy odnośnie kompletności danych dotyczących wszystkich posiadanych i wykorzystywanych licencji - w ramach wymaganego narzędzia do monitorowania oprogramowania, a także - istotne utrudnienie możliwości potwierdzenia, że oprogramowanie, którego licencje wygasły[38], faktycznie zostało wycofane z użycia.

(akta kontroli str. 59-122, 287-295, 515, 637-638, 641-658)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia, że właściwi w sprawach zarządzania oprogramowaniem pracownicy Urzędu Marszałkowskiego Województwa Kujawsko-Pomorskiego nie posiadali pełnej wiedzy na temat używanego tam oprogramowania. Wynikało to z faktu, że nie weryfikowano systematycznie wszystkich posiadanych zasobów pod kątem instalowania i korzystania przez pracowników z nielegalnego oprogramowania. Prawidłowo jednak wykorzystywano udzielone licencje.

[38] W okresie od 2019 r. wygasło sześć sztuk zakupionych przez Urząd licencji i nie zostały one nabyte ponownie.

2. Optymalizacja wykorzystania oprogramowania oraz wydatków związanych z jego nabyciem i użytkowaniem.

2.1. Na podstawie opisanej wyżej, wybranej próby 20 licencji oprogramowania, nabytych od początku 2019 r.[39] stwierdzono, że:

- zapotrzebowanie na dany zakup[40] było weryfikowane przez pracowników Departamentu Organizacyjnego[41];
- liczba nabytych licencji odpowiadała potrzebom Urzędu.

Naczelnik Wydziału Informatyzacji Urzędu podał, że liczba użytkowników licencji danego oprogramowania była określana na podstawie wykazu przewidywanych użytkowników w komórce organizacyjnych. W przypadku analizowania zapotrzebowania na licencje dotyczące systemów informatycznych - wykorzystywano posiadane narzędzia monitorowania i ochrony środowiska informatycznego tak, aby dobrać najkorzystniejszy pod względem kosztów, sposób licencjonowania (np. zakup systemu operacyjnego dla środowiska wirtualizacyjnego licencjonowanego na wirtualny system operacyjny, bądź liczbę rdzeni procesora w serwerze pełniącym rolę wirtualizatora).

(akta kontroli str. 296-298, 315-318, 418-512, 595)

2.2. Łączna wartość wydatków Urzędu na informatyzację wynosiła w latach 2019, 2020 i 2021 odpowiednio 4 773,1 tys. zł, 4,615,5 tys. zł i 5,797,3 tys. zł[42]. W przeliczeniu na jednego pracownika[43] wydatki te wynosiły odpowiednio 4,6 tys. zł. 4,4 tys. zł oraz 5,6 tys. zł. Łączny koszt utrzymania oprogramowania wynosił odpowiednio 1 148,8 tys. zł, 1 563,8 tys. zł oraz 1 890,8 tys. zł. Zaś w przeliczeniu na jednego pracownika wydatki te wynosiły odpowiednio 1,1 tys. zł, 1,5 tys. zł oraz 1,8 tys. zł.

Do bieżącego pomiaru efektywności wykorzystania zasobów informatycznych Urzędu, w zakresie zarządzania licencjami oprogramowania wykorzystywano wskaźniki takie jak liczba komputerów, w tym – z systemem operacyjnym w wersji starszej niż Windows 10[44], oraz efektywność bieżącego wykorzystania licencji na poszczególnych stanowiskach w aplikacjach posiadających konsolę centralnego zarządzania (konsoli takiej, albo aplikacji zarządzania licencjami, nie posiadało jednak 60 używanych w Urzędzie odpłatnych aplikacji i systemów).

W Urzędzie wykorzystywano dwa systemy zintegrowane - finansowo-księgowy KSAT2000i oraz narzędzie do rozliczania opłat za korzystanie ze środowiska SOZAT. Na podstawie listy logowań oraz listy zdarzeń stwierdzono, że wszystkie moduły powyższych systemów były wykorzystywane[45]. W badanym okresie system

---

[39] A także – na podstawie dokumentacji zamówienia na moduł pracowniczych planów kapitałowych systemu finansowo-księgowego KSAT.

[40] Zgłaszane przez kierowników komórek organizacyjnych Urzędu.

[41] Dyrektora Departamentu lub Naczelnika Wydziału Informatyzacji Urzędu.

[42] Ujęto koszty zakupu urządzeń, licencji, utrzymania aplikacji, napraw urządzeń wynagrodzenia pracowników wykonujących zadania z zakresu obsługi informatycznej Urzędu,

[43] Rozumianego jako jeden etat. Liczba etatów we wskazanych wyżej latach (odpowiednio 1038,0; 1041,5; 1035,9) liczona według metodologii sprawozdania Z-06.

[44] Według stanu na dzień 6 września 2022 r. w Urzędzie używano 206 urządzeń wyposażonych w systemy operacyjne w niewspierane pod względem bezpieczeństwa. Zostały one zabezpieczone przy pomocy oprogramowania *Eset Endpoint Security* (wraz z modułami *Live Guard Advanced* i *Inspect*), *Fortigate*, *Fortianalyzer* (z modułem *Indicators of Compromise*) oraz *Greycortex*. Wymiana stacji roboczych, na których zainstalowane były powyższe systemy operacyjne, planowana była na rok 2023.

[45] W skład SOZAT wchodziły moduły opłat: za korzystanie ze środowiska, za składowanie odpadów, dotyczących gospodarki produktami i opakowaniami, dotyczących gospodarki odpadami, dotyczących baterii i akumulatorów, dotyczących zużytego sprzętu elektrycznego, dotyczących recyklingu pojazdów oraz recyklingowej. W skład KSAT wchodziły następujące moduły: oprogramowanie i struktura bazy danych,

finansowo-księgowy został rozszerzony o moduł do obsługi pracowniczych planów kapitałowych[46].

Zamówienie na obsługę serwisową systemu do rozliczania opłat środowiskowych nastąpiło w trybie konkurencyjnym (wraz z dostawą i wdrożeniem). W związku z treścią licencji na użytkowanie poszczególnych modułów systemu finansowo-księgowego – obsługę tego systemu prowadził jego autor[47].

Odnosząc się do kwestii analiz potrzeb i wymagań w zakresie zarządzania licencjami oprogramowania Skarbnik Województwa Kujawsko-Pomorskiego podał, że system do rozliczania opłat za korzystanie ze środowiska nie posiadał alternatywy, natomiast system finansowo-księgowy posiadał wysoką funkcjonalność i wartość użytkową a w szczególności - był otwarty na zmiany oraz niezwłocznie aktualizowany pod względem prawnym; funkcjonalność tego systemu potwierdzał fakt, że był on używany w pięciu innych urzędach marszałkowskich.

Zgodnie z wyjaśnieniami Dyrektora Departamentu Organizacyjnego:

- pracownicy Wydziału Informatyzacji Urzędu sprawdzali przyczyny przerw w wykorzystywaniu komputerów wynoszących co najmniej 12 miesięcy - korzystając w tym zakresie z konsoli zarządzania programu Eset Protect; stopień wykorzystania oprogramowania, wyposażonego przez konsole zarządzania licencjami, monitorowany był na bieżąco; ocena wykorzystania oprogramowania klienckiego, nie posiadającego takiego narzędzia, była pozostawiona w gestii komórki organizacyjnej, w której zatrudniony był dany użytkownik;
- pracownicy Urzędu otrzymywali jedynie uprawnienia i narzędzia informatyczne, niezbędne do wykonywania obowiązków służbowych[48].

Prace związane z usuwaniem problemów z działaniem oprogramowania prowadzone były na bieżąco. Obsługa zgłoszeń w tym zakresie stanowiła jedno z najbardziej pracochłonnych zadań, realizowanych przez administratorów i pracowników zapewniających wsparcie techniczne m.in. w 2022 r. przekazano producentowi systemu KSAT 78 zgłoszeń istotnych problemów, zaś producentowi Generatora Wniosków o Dofinansowanie – 12 zgłoszeń[49].

Postępowanie w przypadku nieprawidłowego działania oprogramowania obejmowało sprawdzenie źródła pochodzenia błędu[50]. W przypadku, gdy problemu nie był w stanie usunąć administrator, zgłoszenie kierowano do producenta.

Jako oprogramowanie w chmurze pracownicy Urzędu wykorzystywali pakiet biurowy oraz system informacji prawnej. W okresie od 24 lipca do 22 września 2022 r. nielimitowana licencja tego systemu została wykorzystana 252 razy. Ponadto w 2022 r. licencja obejmująca 50 dostępów została wykorzystana 47 razy, zaś licencja obejmująca 20 dostępów – została w pełni wykorzystana.

Natomiast cztery licencje pakietu biurowego, zakupione w latach 2021-2022, obejmujące łącznie 186 dostępów, zostały wykorzystane 178 razy.

---

repozytorium, struktura organizacyjna Urzędu, centralna kartoteka kontrahentów, pomoc materialna dla uczniów, budżet, wieloletni plan inwestycyjny, generator raportów *ad-hoc*, centralny rejestr umów, ewidencja kadrowa, fakturowanie, gospodarka mieniem, księga główna, należności i zobowiązania, środki trwałe, administrator systemu.

[46] Nabyty za kwotę 49,2 tys. zł.

[47] System ten został nabyty w 2010 r.

[48] Lista oprogramowania została określona w odpowiedniej procedurze eksploatacyjnej.

[49] W tym – dwa błędy krytyczne.

[50] Użytkownik, system serwerowy, aplikacja.

Zgodnie z wyjaśnieniami Dyrektora Departamentu Organizacyjnego weryfikacja adekwatności przydzielonych użytkownikom narzędzi informatycznych odbywała się na bieżąco a jej kontekstem było udostępniania jedynie niezbędnego oprogramowania.

Nie stwierdzono przypadków zwrotnego przekazania do Urzędu oprogramowania komputerowego, po upływie terminów trwałości projektów finansowanych ze środków z budżetu Unii Europejskiej.

(akta kontroli str. 236-370, 380- 417, 559-636, 897-875)

2.3. Łączny koszt zakupu licencji oprogramowania wynosił w latach 2019, 2020, 2021 i 2022[51] odpowiednio 232,8 tys. zł, 387,1 tys, zł, 671,0 tys. zł oraz 533,8 tys. zł. Jak już opisano to wcześniej łączny koszt utrzymania oprogramowania wynosił odpowiednio 1 148,8 tys. zł w 2019 r., 1 563,8 tys. zł w 2020 r. oraz 1 890,8 tys. zł w 2021 r.

Komórką organizacyjną Urzędu, posiadającą zagregowane informacje w powyższym zakresie, był Departament Finansów.

(akta kontroli str. 307-308, 420-462)

2.4. Zasady badania ryzyka przed zakupem oprogramowania, w tym - pod kątem oceny ryzyk związanych z ochroną danych osobowych, w sposób ogólny określono w Polityce Bezpieczeństwa Informatycznego. Notatki z wyboru ofert dotyczących nabywanego oprogramowania - odpowiednio do nabywanej usługi - nie zawierały analizy ryzyk związanych z ochroną danych osobowych.

Dyrektor Departamentu Organizacyjnego podał w swoich wyjaśnieniach, że:

- w ramach dokumentacji systemu zarządzania bezpieczeństwem informacji wprowadzono Politykę Bezpieczeństwa Danych Osobowych; przy ocenie skutków planowanych operacji przetwarzania dla ochrony danych osobowych analizowane były także ryzyka związane z oprogramowaniem;
- na etapie planowania zakupów poszczególnych programów, określając kryteria w zakresie doświadczenia dostawców, dokonywano najczęściej wyboru rozwiązań powszechnie znanych, spełniających wysokie standardy zabezpieczeń i tym samym gwarantujących akceptowalne ryzyko w obszarze IT.

(akta kontroli str. 346-364, 641-658, 662-668, 770-779)

2.5. Jako oprogramowanie w formie usługi pracownicy Urzędu wykorzystywali pakiet biurowy oraz system informacji prawnej.

Nabywanie oprogramowania w Urzędzie (w tym – oprogramowania jako usługi) odbywało się zgodnie z ogólną procedurą zakupów. Wymagania w zakresie gwarantowanego poziomu usług, bezpieczeństwa i zgodności z przepisami prawa określone były w opisie przedmiotu zamówienia oraz badane w trakcie analizy złożonych ofert.

Ustalenia dotyczące oceny nabywanego oprogramowania w zakresie umowy o gwarantowanym poziomie świadczenia usług, zostały opisane w dalszej części niniejszego wystąpienia pokontrolnego.

(akta kontroli str. 321, 559-560)

Stwierdzone nieprawidłowości

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

[51] Do 16 sierpnia.

1. W Urzędzie nie wykorzystywano dwóch wieczystych licencji *Fortinet Fortitoken Mobile FTM-ELIC-200* dla łącznie 400 użytkowników, zakupionych 23 listopada 2021 r. za kwotę 69,2 tys. zł.

   Naczelnik Wydziału Informatyzacji Urzędu podał, że Urząd posiadał licencje dla 1 204 użytkowników powyższego oprogramowania, z czego – według stanu z dnia 14 września 2022 r. - wykorzystywanych było - 769 a wolnych – 435; zakup licencji dla takiej liczby użytkowników miał umożliwiać niezwłoczne przejście wszystkich pracowników w tryb pracy zdalnej a niewykorzystywane licencje przeznaczone były dla pracowników, którzy dotąd nie świadczyli pracy w powyższym trybie.

   NIK zauważa, że zakup dwóch powyższych licencji można uznać za przedwczesny zważywszy, że konieczność ich wykorzystania nie pojawiła się przez kolejne dziewięć miesięcy.

   (akta kontroli str. 293, 319-320, 507-512)

2. W Urzędzie nie określono i nie wdrożono zasad nabywania oprogramowania jako usługi[52], tj. odpowiednio do nabywanej usługi[53]. Dotyczyło to:

- wiarygodności dostawcy - pod kątem zapewniania wsparcia technicznego i bezpieczeństwa;
- spełnienia wymagań bezpieczeństwa;
- dostępności umowy o gwarantowanym poziomi usług;
- spełnienia wymagań związanych z zarządzaniem danymi (śledzenie zmian na poziomie rekordów bazy danych, zapewnienia możliwości eksportu danych w popularnych formatach, zasady rozdzielania danych);
- zapewnienia szyfrowania *data-in-transit* w oparciu o bezpieczne protokoły i algorytmy;
- polityki kopii zapasowej, w tym częstości wykonywania kopii i okresu retencji oraz przechowywania;
- spełnienia wymagań kontroli dostępu;
- spełnienia wymagań zgodności, w tym wynikających z RODO[54].

Dyrektor Departamentu Organizacyjnego podał w swoich wyjaśnieniach, że:

- weryfikacja dostępności usługi SLA[55] stanowiła kluczowy element wpływający na wybór usługi bądź oprogramowania dostarczanego w formie usługi; jeśli oferowania usługa nie spełniała wymagań w powyższym obszarze, zakup nie był realizowany;
- na etapie planowania zakupów poszczególnych programów, określając kryteria w zakresie doświadczenia dostawców, dokonuje się najczęściej wyboru rozwiązań powszechnie znanych, spełniających wysokie standardy zabezpieczeń, a także spełniające wymagania w zakresie dostępności usług SLA;

[52] Ang. *Software as a Service* (SaaS).
[53] Por. – opinia biegłego, s. 17-18.
[54] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L z 2016 r., poz. 119 Nr 1 ze zm.)
[55] Umowa o gwarantowanym poziomie świadczenia usług (ang. *Service Level Agreement*).

– przykładem stosowania wobec dostawcy wymogów określających zdolności techniczne była specyfikacja zamówienia na zakup systemu kontroli dostępu do sieci typu NAC (zgodnie z którą zdolność techniczna lub zawodowa wykonawcy zamówienia miała być potwierdzona wcześniejszym wykonaniem dwóch wdrożeń o określonej wartości w powyższym zakresie, a także – posiadaniem przez pracowników wykonawcy certyfikatów potwierdzających pewne umiejętności i wiedzę).

NIK zwraca uwagę, że notatki z wyboru ofert dotyczących nabywanego oprogramowania jako usługi, odpowiednio do nabywane usługi - nie zawierały opisów analizy: wiarygodności dostawcy, spełnienia wymagań bezpieczeństwa, dostępności umowy o gwarantowanym poziomi usług, spełnienia wymagań związanych z zarządzaniem danymi, zapewnienia szyfrowania, polityki kopii zapasowej, spełnienia wymagań kontroli dostępu oraz spełnienia wymagań zgodności.

(akta kontroli str. 59-209, 239-275, 315-318, 346-364, 409-417, 641-658, 770-779)

Ocena cząstkowa

W latach 2019-2020 oraz pierwszych trzech kwartałach 2022 r. dokonywane zakupy oprogramowania dotyczyły produktów niezbędnych i w związku z tym - wykorzystywanych w znaczącym stopniu. W 2021 r. zakupiono dwie, niewykorzystane jak dotąd, licencje oprogramowania do wsparcia pracy zdalnej 400 użytkowników, co Najwyższa Izba Kontroli ocenia jako niegospodarne. Izba zwraca również uwagę na fakt, że bieżące analizy funkcjonalności i efektywności posiadanego oprogramowania nie zapobiegły nieprawidłowemu działaniu narzędzia do prowadzenia ewidencji oprogramowania. NIK zwraca również uwagę, że brak posiadania przez Urząd kodów źródłowych systemu zintegrowanego uniemożliwia powierzenie jego obsługi podmiotowi wybranemu w trybie konkurencyjnym.

IV. Uwagi i wnioski

Uwagi

NIK nie formułuje uwag.

Wnioski

1. Wdrożenie kompleksowych i szczegółowych zasad zarządzaniem oprogramowaniem i jego licencjami oraz odpowiednie uzupełnienie zakresów czynności pracowników.
2. Wprowadzenie rozwiązań organizacyjnych i technicznych zapewniających kompletność danych o posiadanym oprogramowaniu.
3. Usunięcie z urządzeń programów wycofanych ze względu na luki w bezpieczeństwie, nieznajdujących się w wykazie dopuszczonego oprogramowania, w nieaktualnych wersjach, a także - niewymagających instalacji.
4. Objęcie regularnym monitorowaniem całego oprogramowania oraz dokumentowanie podejmowanych czynności, w tym działań naprawczych.
5. Określenie i wdrożenie szczegółowych zasad nabywania i wykorzystywania oprogramowania użytkowanego jako usługa.

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 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 Bydgoszczy. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 dni od otrzymania wystąpienia pokontrolnego, o sposobie 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.

Bydgoszcz, 28 października 2022 r.

kontroler
(-) Maciej Gajdzik
doradca techniczny

Najwyższa Izba Kontroli
Delegatura w Bydgoszczy
p.o. Dyrektor
(-) Tomasz Sobecki