

Kategoria: Aktualności

Opublikowano: wtorek, 30, kwiecień 2024 08:49

Joanna Gryboś-Chechelska

Odśłony: 841

Oprogramowanie komputerowe bez wymaganych licencji, nieaktualne, bez wsparcia producenta, wycofane z powodu niedostatecznych zabezpieczeń czy wręcz niebezpieczne – zresztą lista grzechów jest znacznie dłuższa. Urzędy dokonywały nie zawsze uzasadnionych zakupów oprogramowania, często od niezwyfikowanych dostawców, nie monitorowały jego stanu i aktualizacji ani też legalności wykorzystania.

Oprogramowanie w jednostkach administracji publicznej winno być pozyskane legalnie i użytkowanie na mocy licencji udzielonej przez twórcę bądź uprawnionego dystrybutora. Winno być instalowane w przewidziany umową licencyjną sposób, monitorowane na bieżąco, aktualizowane według zaleceń licencjodawcy. Z uwagi na wysoki koszt nabycia oprogramowania oraz jego utrzymania i serwisowania należy dochować należytej staranności w zarządzaniu tym zasobem, w tym zapewnić jego prawidłowe i efektywne użytkowanie, a także chronić je przed atakami i awariami. Kary za naruszenie praw autorskich czy wznowienie licencji mogą sięgać nawet milionów złotych.

Przed podjęciem kontroli NIK pozyskała informacje, z których wynikało, że podmioty administracji publicznej rzadko przeprowadzają lub zlecają audyt oprogramowania. Nie dokonują porównania liczby opłacanych licencji z liczbą licencji faktycznie potrzebnych i wykorzystywanych.

To pierwsza kontrola NIK w całości poświęcona zarządzaniu oprogramowaniem w jednostkach administracji publicznej.

- Zdecydowana większość jednostek administracji publicznej korzystała z oprogramowania nieautoryzowanego.
- Jednostki nie wykorzystywały efektywnie posiadanych narzędzi do monitorowania oprogramowania instalowanego na urządzeniach stacjonarnych, ponosząc niejednokrotnie wysokie wydatki związane z ich nabyciem i utrzymaniem.
- Oprogramowanie instalowane na urządzeniach mobilnych było zupełnie poza zasięgiem nadzoru.
- W kontrolowanych podmiotach nie prowadzono rzetelnych rejestrów zainstalowanego oprogramowania, brakowało więc wiedzy o ich stanie, poziomie aktualizacji i bezpieczeństwa oraz stopniu wykorzystania.
- Proces planowania, nabywania i wdrażania oprogramowania nie zawsze był optymalny i prawidłowy, wskutek czego niekiedy nabywano zbyt dużą liczbę niewykorzystanych następnie licencji czy też naruszano przepisy o zamówieniach publicznych.
- Jednostki nie zapewniły możliwości rozbudowy i utrzymania oprogramowania zintegrowanego bez ingerencji jego twórcy, co oznaczało pełne i często długookresowe uzależnienie od prywatnego licencjodawcy.
- Ministerstwo Finansów nie zadbało o obniżenie awaryjności własnego oprogramowania ani o wdrożenie należytych zasad bezpieczeństwa oprogramowania wytwarzanego i utrzymywanego na jego rzecz.

W 88% skontrolowanych jednostek administracji publicznej **kontrola stwierdziła oprogramowanie nieautoryzowane**, które nie powinno być zainstalowane lub użytkowane – np. bez wymaganych licencji, bez wsparcia producenta czy w nieaktualnych wersjach, a nawet niebezpieczne.

W niemal połowie (47%) podmiotów **stan oprogramowania oznaczał ryzyko poważnego niebezpieczeństwa**. Stwierdzono nawet przypadki instalowania programów bez poprawek krytycznych.

Kategoria: Aktualności

Opublikowano: wtorek, 30, kwiecień 2024 08:49

Joanna Gryboś-Chechelska

Odłony: 841

41% podmiotów korzystało z **oprogramowania użytkowanego nielegalnie**, taki sam procent – z **niedopuszczonego do korzystania w danym urzędzie**. Niewiele mniej, bo 35% jednostek dysponowało aplikacjami w stadium EoL, czyli **wycofywanymi z powodu kresu używalności**.

Działo się tak najczęściej wskutek tego, że jednostki **niedostatecznie monitorowały własne oprogramowanie i nie zapoznawały się każdorazowo z warunkami licencji danego programu**.

Żaden ze skontrolowanych podmiotów **nie potwierdził, że na bieżąco i skutecznie sprawdza stacje robocze i udostępnione udziały sieciowe użytkowników pod kątem obecności nieautoryzowanego oprogramowania**. Większość jednostek deklarowała stosowanie blokady możliwości samodzielnego instalowania oprogramowania jako optymalnego mechanizmu kontrolnego. Niemniej o braku skuteczności powyższego sposobu działania świadczy fakt zdiagnozowania w toku kontroli NIK nieautoryzowanego oprogramowania.

Oprogramowanie na urządzeniach mobilnych pozostawało zupełnie poza nadzorem. Żadna z jednostek nie zapewniła rozwiązań technicznych do monitorowania tego rodzaju oprogramowania, nie zadbała także o stosowne działania organizacyjne. Część podmiotów nie miała świadomości zagrożeń i konsekwencji związanych z instalowaniem i użytkowaniem oprogramowania na urządzeniach mobilnych, uznając, że służą one użytkownikom wyłącznie do prowadzenia rozmów telefonicznych, co nie tylko narażało jednostki na kary finansowe, ale również **zagrożało bezpieczeństwu przetwarzanych w ten sposób danych**.

Aż w **59% przypadków jednostki nie miały pełnej wiedzy co do posiadanego oprogramowania**, prowadząc niekompletne spisy programów i licencji. W efekcie nie było możliwe ustalenie rzetelnej liczby faktycznie wykorzystanych, zainstalowanych programów. Powodowało to również brak możliwości ustalenia faktycznego wykorzystania posiadanego oprogramowania.

Niemal żadna jednostka (94%) **nie ustanowiła i nie wdrożyła formalnych zasad zarządzania oprogramowaniem**, obejmujących cały cykl jego życia i określających np. kwestie nabywania i wycofywania licencji, ewidencjonowania, inwentaryzacji i przeglądów, bezpieczeństwa i nośników instalacyjnych, monitorowania stanu użycia, ważności i legalności licencji, a także potencjalnej konieczności działań naprawczych.

Zakup licencji był dokonywany centralnie: **uprawnienia do zakupów licencji albo ich zatwierdzania miała jedna, wyznaczona komórka organizacyjna**. W 53% podmiotów stwierdzono na tym etapie nieprawidłowości wskazujące, że proces ten mógł nie być optymalny – m.in. nabyto licencje, które nie były wykorzystywane bądź nawet zainstalowane albo zakupione w liczbie większej, niż faktycznie była potrzebna. Dochodziło np. do zatwierdzania odbioru wadliwego elementu systemu informatycznego czy do nieodnowienia wsparcia licencji. Kontrolerzy stwierdzili przypadki nieprawidłowego planowania i nabywania licencji, co kłóciło się z wymogiem optymalizacji i skutkowało w sumie niegospodarnością sięgającą 12,5 mln zł.

Wśród podmiotów posługujących się zintegrowanymi systemami informatycznymi (ZSI) aż **43% postępowało nieprawidłowo, m.in. naruszając przepisy ustawy o zamówieniach publicznych w zakresie zamówienia w trybie z wolnej ręki czy utrzymując niewykorzystywane moduły oprogramowania**. W dziesięciu z nich nie zapewniono możliwości rozbudowy i utrzymania takiego oprogramowania bez ingerencji jego twórcy, co oznaczało pełne uzależnienie od prywatnego

Kategoria: Aktualności

Opublikowano: wtorek, 30, kwiecień 2024 08:49

Joanna Gryboś-Chechelska

Odłony: 841

licencjodawcy, mogącego wymuszać na podmiocie publicznym długookresową współpracę z pozycji hegemonu.

Oprogramowanie typu SaaS (software as a service), całkowicie przenoszące odpowiedzialność za instalację, zarządzanie i aktualizację na dostawcę, **tylko w 40% było nabywane na warunkach umożliwiających weryfikację**, czy spełnia ono wymogi i potrzeby danej jednostki. **Nie zawsze też sprawdzano wiarygodność dostawców.**

Minister Finansów nie wyegzekwował od podmiotów wytwarzających, utrzymujących i unowocześniających oprogramowanie resortu, by ich usługi były realizowane terminowo i by obniżono awaryjność systemów.

Minister nie doprowadził również do wdrożenia zasad bezpieczeństwa oprogramowania wytwarzanego i utrzymywanego na jego rzecz, o standardzie nie niższym od obowiązującego w Ministerstwie i jednostkach resortu finansów. Nierzetelnie też przeprowadził postępowanie o udzielenie zamówienia publicznego, co skutkowało wydaniem niemal 1,5 mln zł za sam fakt wznowienia wsparcia licencji w związku z opóźnieniem w zawarciu umowy.

W spółce Aplikacje Krytyczne sp. z o.o., realizującej projekty informatyczne zarządzane przez Ministra Finansów, nie zautomatyzowano procesu monitorowania posiadanych i użytkowanych licencji. Monitoringiem nie objęto wszystkich urządzeń, na których instalowane było oprogramowanie. Wskutek wydłużonego czasu weryfikacji zainstalowanych aplikacji rosło ryzyko użytkowania nielegalnego oprogramowania, w tym korzystania z aplikacji niebezpiecznych. Poza tym zbyt wielu osobom przyznano uprawnienia do instalowania oprogramowania, co budzi niepokój z uwagi na profil działalności spółki, obligujący do stosowania najwyższych standardów zarządzania i bezpieczeństwa.

WNIOSKI

Jednostki samorządu terytorialnego oraz inne państwowe jednostki organizacyjne

Najwyższa Izba Kontroli wskazuje na konieczność podejmowania przez kierowników jednostek administracji publicznej niezbędnych działań służących zapewnieniu prawidłowego zarządzania oprogramowaniem komputerowym, w tym w szczególności:

- określenia i wprowadzenia szczegółowych zasad zarządzania oprogramowaniem (licencjami), w tym nabywania oprogramowania SaaS;
- wprowadzenia rozwiązań technicznych zapewniających kompletność danych o posiadanym oprogramowaniu;
- objęcia bieżącym monitorowaniem całego oprogramowania, niezależnie od miejsca jego instalacji, i dokumentowania podejmowanych czynności, w tym działań naprawczych;
- prowadzenia regularnej analizy stopnia wykorzystania poszczególnych aplikacji.

Ministerstwa

Najwyższa Izba Kontroli wskazuje na konieczność podejmowania przez kierowników jednostek zlecających realizację projektów i programów informatycznych niezbędnych i skutecznych działań nadzorczych wobec podmiotów, którym zlecono ich realizację, w celu:

- skutecznego egzekwowania wykonywania działań naprawczych dotyczących zidentyfikowanych

Kategoria: Aktualności

Opublikowano: wtorek, 30, kwiecień 2024 08:49

Joanna Gryboś-Chechelska

Odśłony: 841

problemów mogących wpływać negatywnie na efektywność działań dotyczących wytwarzanego, utrzymywanego bądź unowocześnianego przez te podmioty oprogramowania na rzecz jednostki zlecającej;

- zapewnienia bezpieczeństwa informatycznego wytwarzanego i utrzymywanego oprogramowania o standardzie nie niższym od obowiązującego w podmiocie zlecającym;
- opracowania i skutecznego wdrożenia w resorcie katalogu oprogramowania dopuszczonego i niedopuszczonego.

Podmioty publiczne, które zostały utworzone w celu wytwarzania, utrzymania lub unowocześniania oprogramowania na potrzeby ministerstw

W odniesieniu do podmiotów publicznych utworzonych w celu wytwarzania, utrzymania lub unowocześniania oprogramowania na potrzeby ministerstw Najwyższa Izba Kontroli wskazuje jako niezbędne:

- objęcie regularnym monitorowaniem całego oprogramowania, niezależnie od miejsca jego instalacji;
- instalowanie jedynie oprogramowania dopuszczonego do użycia w ramach organizacji.

W wyniku kontroli skierowano do rzecznika dyscypliny finansów publicznych zawiadomienia dotyczące nieprawidłowości stwierdzonych w trzech jednostkach kontrolowanych, w dwóch przypadkach dotyczące udzielania zamówień publicznych z naruszeniem przepisów dot. przesłanek stosowania zamówienia z wolnej ręki na łączną kwotę ponad 9 mln zł i w jednym w związku z zaniechaniem prowadzenia audytu wewnętrznego. Ponadto do Prezesa Urzędu Zamówień Publicznych skierowane zostało zawiadomienie dotyczące udzielania przez kontrolowaną jednostkę zamówień z naruszeniem przepisów określających przesłanki stosowania trybu zamówienia z wolnej ręki.

Źródło: NIK