Ministerstwo
Spraw Wewnętrznych
i Administracji
Departament Kontroli

Warszawa, dnia 1 sierpnia 2022 r.

Informacja o wynikach kontroli
na temat: *Działanie systemów teleinformatycznych używanych do realizacji zadań publicznych albo realizacji obowiązków wynikających z art. 13 ust. 2 ustawy o informatyzacji działalności podmiotów realizujących zdania publiczne* w Wyższej Szkole Policji w Szczytnie

I. Podstawa prawna

Czynności kontrolne zostały przeprowadzone na podstawie ustawy z dnia 15 lipca 2011 r. *o kontroli w administracji rządowej*[1] w związku z art. 25 ust. 1 pkt 3 lit. b) ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne*[2].

II. Tryb kontroli

Kontrola została przeprowadzona przez Departament Kontroli Ministerstwa Spraw Wewnętrznych i Administracji w trybie zwykłym, zgodnie z *Planem kontroli Ministerstwa Spraw Wewnętrznych i Administracji na rok 2022.*

III. Termin kontroli

Od 7 lutego 2022 r. do 31 marca 2022 r.

IV. Zakres kontroli obejmował następujące zagadnienia:

1) Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.
2) Zarządzanie bezpieczeństwem informacji w systemach teleinformatycznych.

V. Kontrolą objęto okres od 1 stycznia 2021 r. do 31 stycznia 2022 r.[3]

VI. Ustalenia kontroli – ocena kontrolowanej działalności

Oceniono **pozytywnie mimo stwierdzonych nieprawidłowości** sposób realizacji w Wyższej Szkole Policji w Szczytnie[4] zadań związanych z działaniem systemów teleinformatycznych używanych do realizacji zadań publicznych.

Pozytywnie oceniono świadczenie usług z wykorzystaniem elektronicznej skrzynki podawczej na platformie ePUAP oraz funkcjonowanie strony internetowej, która zawierała m.in. informacje dotyczące danych kontaktowych oraz posiadała bezpośredni dostęp do Biuletynu Informacji Publicznej gdzie znajdowały się informacje o sposobie postępowania ze skargami i wnioskami, w tym o sposobie składania petycji.

[1] t.j. Dz. U. z 2020 r. poz. 224.
[2] Dz. U. z 2021 r., poz. 2070 ze zm., zwana dalej: ustawą *o informatyzacji*.
[3] Z zastrzeżeniem, że w ramach obszaru określonego w pkt 2 zakresu przedmiotowego kontroli, tj. w zakresie obszaru związanego z projektowaniem, wdrażaniem i funkcjonowaniem systemów teleinformatycznych kontrolą zostanie objęty okres od dnia rozpoczęcia prac projektowych, zaś w zakresie umów serwisowych okres od dnia zawarcia badanej umowy.
[4] Zwana dalej: WSPol w Szczytnie.

Pozytywnie oceniono również działania związane z opracowaniem i aktualizacją dokumentacji pt. *System zarządzania bezpieczeństwem informacji* oraz *Polityka Bezpieczeństwa Danych osobowych oraz Instrukcja Zarządzania Systemem Informatycznym służącym do Przetwarzania Danych osobowych jako element Systemu Zarządzania Bezpieczeństwem Informacji*.

W toku kontroli **pozytywnie** oceniono sposób zarządzania incydentami bezpieczeństwa informacji, zasady minimalizujące ryzyka utraty informacji w wyniku awarii, zasady zarządzania uprawnieniami do pracy w systemach oraz zasady bezpiecznej pracy na odległość. Jednostka kontrolowana podejmowała właściwe działania w obszarze podnoszenia świadomości pracowników zaangażowanych w proces przetwarzania informacji, przeprowadzając adekwatne w tym zakresie szkolenia. Ponadto, prawidłowo stosowano zabezpieczenia techniczne i organizacyjne dostępu do informacji i systemów teleinformatycznych, zapewniono inwentaryzację sprzętu i oprogramowania informatycznego oraz rozliczalność działań użytkowników w systemach teleinformatycznych.

Pomimo ww. pozytywnych aspektów działalność WSPol, w trakcie kontroli w niektórych obszarach stwierdzono **nieprawidłowości** mające istotny wpływ na sposób zarządzania bezpieczeństwem informacji. Poległy one na:

- niezabezpieczeniu hasłem BIOS-u[5] niektórych stanowisk komputerowych;
- złym ustawieniu dzienników systemowych na niektórych stanowiskach komputerowych;
- braku czujnika ochrony zadymienia w jednej z serwerowni;
- niezainstalowaniu czujników ochrony przed zalaniem w trzech serwerowniach;
- nieopracowaniu szacowania ryzyka dla dwóch systemów informatycznych;
- nieprzeprowadzaniu okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji.

W toku kontroli stwierdzono również **uchybienie** polegające na niewskazaniu w Biuletynie Informacji Publicznej w zakładce skargi i wnioski, elektronicznej platformy usług administracji publicznej ePUAP i poczty elektronicznej, za pomocą których możliwe było przekazywanie dokumentów w formie elektronicznej.

Stwierdzone i wskazane powyżej nieprawidłowości (w tym uchybienie) nie spowodowały negatywnych skutków w służbowej działalności WSPol. Miały one charakter incydentalny, a ich wystąpienie zostało spowodowane brakiem wymaganej staranności w realizacji niektórych zadań służbowych przez wyznaczone osoby. Wartym uwagi jest jednak to, że wszystkie nieprawidłowości (w tym uchybienie) zostały skutecznie usunięte jeszcze w trakcie trwania czynności kontrolnych. Szybka i jednoznaczna reakcja osób odpowiedzialnych za stwierdzone nieprawidłowości, mająca na celu usprawnienie funkcjonowania kontrolowanego podmiotu, była nie tylko właściwa, ale i adekwatna z uwagi na rodzaj i wagę stwierdzonych nieprawidłowości.

VII. Wnioski i zalecenia pokontrolne

W celu usprawnienia funkcjonowania kontrolowanej jednostki sformułowano następujące zalecenia:

1. Wypracowanie skutecznych mechanizmów nadzoru, które zagwarantują prawidłowy i terminowy sposób realizacji zadań związanych z działaniem systemów teleinformatycznych używanych do realizacji zadań publicznych.
2. Prowadzenie (co najmniej raz w roku) audytu wewnętrznego w zakresie bezpieczeństwa informacji.

[5] BIOS – podstawowy system wejścia-wyjścia, zapisany w pamięci stałej zestaw procedur pośredniczących pomiędzy systemem operacyjnym a sprzętem.