Ministerstwo
Spraw Wewnętrznych
i Administracji
Departament Kontroli

Warszawa, dnia 18 maja 2022 r.

Informacja o wynikach kontroli
na temat: *Działanie systemów teleinformatycznych używanych do realizacji zadań publicznych*
w Komendzie Głównej Państwowej Straży Pożarnej.

I. Podstawa prawna

Czynności kontrolne zostały przeprowadzone na podstawie ustawy z dnia 15 lipca 2011 r. *o kontroli w administracji rządowej*[1].

II. Tryb kontroli

Kontrola została przeprowadzona przez Departament Kontroli i Nadzoru (obecnie Departament Kontroli) Ministerstwa Spraw Wewnętrznych i Administracji w trybie zwykłym, zgodnie z *Planem kontroli Ministerstwa Spraw Wewnętrznych i Administracji na rok 2019.*

III. Termin kontroli

Od 20 maja 2019 r. do 28 czerwca 2019 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.
3) Zapewnienie dostępności informacji zawartych na stronach internetowych KG PSP dla osób niepełnosprawnych.
4) Przestrzeganie przepisów rozporządzenia 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* (RODO)[2] w zakresie bezpieczeństwa danych osobowych przetwarzanych w systemach teleinformatycznych.

V. Kontrolą objęto okres od 1 stycznia 2018 r. do 15 maja 2019 r.

VI. Ustalenia kontroli – ocena kontrolowanej działalności

W okresie objętym kontrolą pozytywnie oceniono świadczenie usług z wykorzystaniem elektronicznej skrzynki podawczej na platformie ePUAP oraz funkcjonowaniem strony internetowej, która m.in. zawierała informacje dotyczące danych kontaktowych, sposobu postępowania ze skargami i wnioskami, a także istotne informacje dla osób niepełnosprawnych, ułatwiające im korzystanie z tej strony.

Pozytywnie oceniono również działania związane z opracowaniem i aktualizacją dokumentu pt. *„Zasady ewidencjonowania zdarzeń w Systemie Wspomagania Decyzji Państwowej Straży Pożarnej”* oraz działania podejmowane w związku z wystąpieniem incydentu bezpieczeństwa polegającego na

[1] t.j. Dz. U. z 2020 r. poz. 224.
[2] Dz. Urz. UE. L Nr 119, str. 1.; zwanego dalej także rozporządzeniem RODO.

zainfekowaniu wirusem lokalnego komputera. Działania zaradcze przyczyniły się do tego, że wirus się nie rozprzestrzenił w sieci i nie zainfekował kolejnych zasobów teleinformatycznych.

Pomimo powyższych pozytywnych zachowań kontrola wykazała szereg **nieprawidłowości,** które polegały głównie na:

- stosowaniu niekompletnych procedur oraz czynności wynikających z Systemu Zarządzania Bezpieczeństwem Informacji[3] oraz braku aktualizacji polityk bezpieczeństwa informacji powiązanych z procedurami/instrukcjami/wytycznymi określającymi zasady użytkowania systemu,
- braku szczegółowych harmonogramów i procedur wykonywania kopii zapasowych systemów operacyjnych, konfiguracji, bazy danych itp. istotnych z punktu bezpieczeństwa systemów objętych kontrolą,
- nieprzeprowadzeniu w przypadku wystąpienia poważnej awarii pełnego procesu szacowania ryzyka w celu podjęcia działań zaradczych, w tym zminimalizowania możliwości wystąpienia podobnych awarii w przyszłości,
- nieprzeprowadzaniu okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz niepodejmowaniu działań minimalizujących ryzyko zmaterializowania się ewentualnych zagrożeń,
- niewypełnianiu lub częściowym wypełnianiu wniosków o nadanie/odebranie uprawnień do usług teleinformatycznych,
- istnieniu aktywnych kont pomimo braku świadczenia przez ich użytkowników stosunku pracy lub pełnienia służby,
- niezachowaniu ciągłości poszczególnych umów serwisowych,
- niedokumentowaniu szkoleń nowych użytkowników realizowanych przez wiodących administratorów (uchybienie).

Wskazane uchybienie oraz nieprawidłowości świadczyły o braku właściwego nadzoru ze strony kierownictwa kontrolowanej jednostki nad wykonywaniem zadań związanych z działaniem systemów teleinformatycznych używanych do realizacji zadań publicznych. Pomimo niewystąpienia negatywnych skutków w kontrolowanym obszarze, istnieje konieczność podjęcia w trybie pilnym skutecznych czynności naprawczych, które wyeliminują powstałe nieprawidłowości i usprawnią sposób realizacji kontrolowanych zagadnień.

VII. Wnioski i zalecenia pokontrolne

W celu wyeliminowania ze służbowej działalności stwierdzonych w trakcie kontroli nieprawidłowości i uchybień oraz usprawnienia funkcjonowania kontrolowanej jednostki zalecono:

1. Podjęcie działań zmierzających do opracowania szczegółowych procedur/instrukcji/wytycznych związanych z obsługą kontrolowanych systemów informatycznych używanych do realizacji zadań publicznych, w tym uaktualnienie obowiązujących w tym zakresie wewnętrznych uregulowań, m.in. takich jak polityka bezpieczeństwa informacji poprzez dostosowanie ich do obowiązujących przepisów z uwzględnieniem zasad wynikających z Systemu Zarządzania Bezpieczeństwem Informacji oraz normy ISO/IEC 27001.
2. Opracowanie szczegółowych harmonogramów i procedur wykonywania kopii zapasowych systemów operacyjnych, konfiguracji, bazy danych, wskazanie osób/podmiotów odpowiedzialnych za ich wykonywanie oraz weryfikację poprawności wykonania tych kopii, istotnych z punktu bezpieczeństwa tych systemów i przetwarzanych w nich informacji.

[3] Zwanego dalej SZBI.

3. Zobowiązanie podległych administratorów do przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz do podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzanych analiz (obligatoryjnie po wystąpieniu każdego incydentu bezpieczeństwa teleinformatycznego z uwzględnieniem bezpieczeństwa systemów i przetwarzanych w nich informacji).
4. Zobowiązanie podległych administratorów do prawidłowej realizacji wszystkich procedur wynikających z decyzji Nr 54, w tym o weryfikację i formalne sporządzenie wniosków dla 41 kont użytkowników Systemu Wspomagania Decyzji KG PSP, wobec których dotychczas tych wniosków nie sporządzono.
5. Ujednolicenie uregulowań wewnętrznych i zasad obowiązujących w zakresie usuwania/blokowania kont dla użytkowników systemów, wobec których ustał stosunek pracy lub pełnienia służby.
6. Podpisywanie umów serwisowych na kolejne okresy, w czasie obowiązywania bieżących umów, w celu zapewnienia formalno-prawnej ich ciągłości.
7. Zobowiązanie podległych administratorów do dokumentowania szkoleń organizowanych dla nowych użytkowników systemu.
8. Podjęcie działań mających na celu zbadanie zasadności utrzymywania bezwzględnego dostępu do danych osobowych przez przedstawicieli firmy „ABAKUS", w szczególności pod kątem wprowadzenia właściwych ograniczeń takiego dostępu w nowobudowanym systemie SWD KG, w tym odseparowanie danych produkcyjnych od części będącej w utrzymaniu serwisu na zasadach określonych w zawartej umowie.
9. Zapewnienie pełnej rozliczalności pod względem dostępu do danych zgromadzonych w zasobach informatycznych przez przedstawicieli firm serwisowych.
10. Podjęcie działań zmierzających do zwiększenia stanu etatowego Biura Informatyki i Łączności KG PSP i zatrudnienia w miarę możliwości specjalistów w dziedzinie teleinformatyki.