PREZES
NAJWYŻSZEJ IZBY KONTROLI
Krzysztof Kwiatkowski

KPB.410.004.03.2015
P/15/042

WYSTĄPIENIE POKONTROLNE

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli

P/15/042 – Zapewnienie bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych.

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli
Departament Porządku i Bezpieczeństwa Wewnętrznego

Kontrolerzy

1. Anna Mach, główny specjalista kontroli państwowej, upoważnienie do kontroli nr 93500 z dnia 1 czerwca 2015 r.

(dowód: akta kontroli Tom I str. 1-2)

2. Katarzyna Szymańska, specjalista kontroli państwowej, upoważnienie do kontroli nr 93497 z dnia 1 czerwca 2015 r.

(dowód: akta kontroli Tom I str. 3-4)

3. Łukasz Garbień, doradca prawny, upoważnienie do kontroli nr 95757 z dnia 4 sierpnia 2015 r.

(dowód: akta kontroli Tom I str. 5-6)

Jednostka kontrolowana

Ministerstwo Skarbu Państwa
Ul. Krucza 36 / Wspólna 6, 00-522 Warszawa

Kierownik jednostki kontrolowanej

Ministrem Skarbu Państwa od dnia 16 czerwca 2015 r. do dnia 15 listopada 2015 r. był Andrzej Czerwiński. Uprzednio funkcję Ministra Skarbu Państwa pełnił Włodzimierz Karpiński (od dnia 24 kwietnia 2013 r.)[1]

Dyrektorem Generalnym Ministerstwa Skarbu Państwa od dnia 19 lutego 2012 r. był Mirosław Skowerski.

(dowód: akta kontroli Tom I str. 7-8)

II. Ocena kontrolowanej działalności

Ocena ogólna

W oparciu o stosowany w metodyce CobiT 4.1 Model dojrzałości[2], NIK ocenia poziom zarządzania procesem „zapewnienie bezpieczeństwa systemów informatycznych" w MSP jako „powtarzalne lecz intuicyjne".

Uzasadnienie oceny ogólnej

W kontrolowanej jednostce istnieje świadomość potrzeby zapewnienia bezpieczeństwa teleinformatycznego, jednak jest ona fragmentaryczna i ograniczona. Rozwijana jest polityka dotycząca bezpieczeństwa, ale nie towarzyszą jej adekwatne narzędzia. Chociaż systemy dostarczają informacji

[1] Z dniem 16 listopada 2015 r. na stanowisko Ministra Skarbu Państwa powołany został Dawid Jackiewicz.

[2] Oceny dokonano w oparciu o stosowany w metodyce CobiT4.1 Model dojrzałości. Zgodnie z tą metodyką przyjmuje się sześciostopniową skalę ocen zarządzania procesem zapewnienia bezpieczeństwa: 0 Nieistniejące, 1 Początkowe/doraźne, 2 Powtarzalne lecz intuicyjne, 3 Zdefiniowane, 4 Kontrolowane i mierzalne, 5 zoptymalizowane. Cobit - (Control Objectives for Information and related Technology) uznany międzynarodowy standard i zbiór dobrych praktyk w obszarze technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego.

dotyczących bezpieczeństwa, to dane te nie są analizowane. Bezpieczeństwo IT jest postrzegane głównie, jako przedmiot odpowiedzialności i domena działu IT, a nie zadanie leżące w gestii całego Ministerstwa.

W ocenie NIK brak kompleksowego systemu zarządzania bezpieczeństwem informacji w Ministerstwie Skarbu Państwa utrudniał właściwą ich ochronę. Ponadto nieopracowanie szczegółowych procedur wskazanych w Polityce Bezpieczeństwa Systemów Teleinformatycznych dotyczących bezpieczeństwa danych przetwarzanych w MSP, a także niedostosowanie tego dokumentu do obowiązujących wymogów prawa, mogły przyczyniać się do osłabienia tej ochrony. W tym kontekście Izba pozytywnie ocenia podjęte przez Ministerstwo działania w celu opracowania i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji.

Stwierdzone nieprawidłowości dotyczyły w szczególności niezapewnienia rozliczalności „Zintegrowanego Systemu Informacji db" (dalej: ZSI) oraz braku klasyfikacji i ochrony informacji (innych niż dane osobowe).

III. Opis ustalonego stanu faktycznego

1. Wspieranie bezpieczeństwa IT na poziomie całej organizacji

1.1. Zarządzanie bezpieczeństwem IT

Opis stanu faktycznego

Zarządzeniem Nr 37 Ministra Skarbu Państwa z dnia 8 października 2013 r. w sprawie ustalenia regulaminu organizacyjnego Ministra Skarbu Państwa[3] do zakresu zadań Biura Dyrektora Generalnego MSP (dalej: BDG) przypisano zapewnienie sprawnego i niezawodnego działania systemów teleinformatycznych Ministerstwa, poprzez wykonywanie zadań obejmujących administrowanie, koordynowanie i nadzorowanie działań służących aktualizacji i rozwojowi całościowego programu informatyzacji Ministerstwa.

(dowód: akta kontroli Tom I str. 481-508)

Stosownie do § 8 Wewnętrznego Regulaminu Organizacyjnego BDG, zatwierdzonego przez Dyrektora Generalnego MSP z dnia 15 września 2014 r.[4], do zadań Wydziału Systemów Teleinformatycznych należy w szczególności:

- kierowanie i nadzór nad procesami budowy, eksploatacji, ochrony i rozwoju Zintegrowanego Systemu Informatycznego MSP, w tym administrowanie Zintegrowanym Systemem Informatycznym – ZSI db,
- zarządzenie i administrowanie zasobami teleinformatycznymi Ministerstwa, w tym utrzymanie produkcyjne systemów informatycznych, zarządzanie zasobami sieci komputerowej LAN oraz sieci telekomunikacyjnej, zarządzanie uprawnieniami do systemów informatycznych według właściwości Wydziału i dostępem użytkowników do zasobów MSP, administrowanie usługami katalogowymi Active Directory oraz pozostałymi systemami według właściwości Wydziału,

[3] Zmieniony zarządzeniami Nr 41 z 25 września 2014 r., Nr 51 z 17 października 2014 r., Nr 10 z 24 marca 2015 r., Nr 18 z 26czerwca 2015 r., Nr 23 z 31 lipca 2015 r., Nr 48 z 22 października 2015 r. i Nr 49 z 10 listopada 2015 r.

[4] Uprzednio obowiązywał Wewnętrzny Regulamin Organizacyjny BDG zatwierdzony przez Dyrektora Generalnego MSP w dniu 6 listopada 2013 r.

- prowadzenie polityki bezpieczeństwa teleinformatycznego Ministerstwa, w tym tworzenie zabezpieczeń organizacyjnych i systemowych w zakresie ochrony i bezpieczeństwa zasobów teleinformatycznych Ministerstwa oraz nadzór nad ich realizacją i przestrzeganiem.

Zgodnie z § 9 Regulaminu do zadań Wydziału Wsparcia IT należy m.in.:

- zarządzenie i administrowanie zasobami teleinformatycznymi Ministerstwa, w tym utrzymanie produkcyjne systemów teleinformatycznych, zarządzanie i administrowanie platformami Lotus Domino i VMware, macierzami i siecią SUN oraz systemem backupu TSM, zarządzanie uprawnieniami do systemów informatycznych według właściwości Wydziału, zarządzanie i utrzymanie usługi Centralnego Wydruku oraz zarządzanie pozostałymi systemami według właściwości Wydziału,
- prowadzenie wsparcia IT dla użytkowników MSP – Service Desk,
- zarządzanie zasobami sprzętowymi IT.

(dowód: akta kontroli Tom III str. 1-52)

Na dzień zakończenia kontroli w ww. Wydziałach zatrudnionych było odpowiednio pięć i sześć osób. Audytor zewnętrzny wskazał, że istnieje duża zależność Ministerstwa od podmiotów zewnętrznych w zakresie utrzymania systemów IT. W latach 2014-2015 BDG nie kierowało do kierownictwa MSP wniosków o zwiększenie obsady kadrowej do poziomu pozwalającego na realizowanie zadań.

(dowód: akta kontroli Tom I str. 145-146, Tom III str. 99-124, 276-277)

Dyrektor Generalny MSP wyjaśnił, że: *„z uwagi na zmieniające się standardy, konieczność ciągłego podnoszenia jakości usług, zwiększania poziomu niezawodności i bezpieczeństwa systemów IT oraz w związku ze zmianami dotyczącymi przede wszystkim wdrażania nowych rozwiązań przy niezmiennym składzie osobowym Wydziału Systemów Teleinformatycznych oraz Wydziału Wsparcia IT w [BDG], zapewnienie asysty i wsparcia w stopniu pozwalającym na wykonywanie podstawowych zadań przez Pion IT jest realizowane przy udziale pracowników firm zewnętrznych na podstawie zawartych umów."* Ponadto, Dyrektor Generalny MSP podał, że kierownictwo Ministerstwa nie rozważało zwiększenia etatyzacji ww. wydziałów ze względu na ograniczoną liczbę etatów.

(dowód: akta kontroli Tom III str. 276-277)

Zarządzeniem nr 14 Dyrektora Generalnego z dnia 11 maja 2015 r. powołany został Zespół ds. wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w MSP, który ma zostać wdrożony w MSP z końcem II kwartału 2016 r.

Do zadań Zespołu należy m.in. realizacja zadań związanych z ustanowieniem i wdrożeniem SZBI, opracowywanie wewnętrznych regulacji prawnych oraz doprecyzowanie procedur oraz instrukcji obejmujących zidentyfikowane obszary zagrożeń lub potencjalnych zagrożeń, kontrole aktywów, bezpieczeństwo fizyczne i środowiskowe.

Harmonogram i działania podejmowane w ramach realizacji SZBI opisano w punkcie 2.4 niniejszego wystąpienia pokontrolnego.

(dowód: akta kontroli Tom I str. 476-480)

Zarządzeniem nr 21 Dyrektora Generalnego MSP z dnia 12 lipca 2013 r. w Ministerstwie powołano Zespół ds. Bezpieczeństwa Systemów Teleinformatycznych. Do zadań Zespołu należy m.in. przedkładanie Dyrektorowi Generalnemu do zatwierdzenia zasad polityki bezpieczeństwa oraz ich aktualizacji, monitorowanie bezpieczeństwa infrastruktury teleinformatycznej, informowanie o wystąpieniu zagrożeń lub naruszeniu bezpieczeństwa sieciowego, reagowanie na zgłoszone incydenty komputerowe.

Zgodnie z § 2 pkt 2 ww. zarządzenia Zespół przekazywał Dyrektorowi Generalnemu kwartalne raporty o stanie bezpieczeństwa infrastruktury teleinformatycznej.

(dowód: akta kontroli Tom I str. 577, Tom II str. 231-248, Tom III str. 282-286)

Dyrektor BDG podał m.in., że *„monitorowanie stanu bezpieczeństwa infrastruktury teleinformatycznej w Ministerstwie wykonywane na bieżąco przez pracowników Pionu IT w BDG nie jest dokumentowane."*

(dowód: akta kontroli Tom II str. 230)

W Ministerstwie w dniu 20 października 2014 r, opracowano, przy udziale Prevenity Sp. z o.o., dokument „Szacowanie ryzyka związanego z bezpieczeństwem informacji". Prowadzony rejestr ryzyk obejmuje m.in. zagrożenia: zewnętrzne i wewnętrzne IT, ludzkie, fizyczne i środowiskowe zewnętrzne i wewnętrzne oraz prawne, regulacyjne i kontaktowe.

(dowód: akta kontroli Tom I str. 462-475)

Rekomendowanie sposobów zapewnienia bezpieczeństwa w zakresie dostępu do systemów teleinformatycznych w głównej mierze jest domeną pionu IT, z wyłączeniem zapewnienia fizycznego bezpieczeństwa MSP (ochrona budynku, system kontroli wejść/wyjść), za które odpowiada Wydział Ochrony Informacji Niejawnych w BDG.

W toku kontroli przedłożono dwie propozycje działań związanych z zapewnieniem bezpieczeństwa przedstawione kierownictwu MSP – Dyrektorowi Generalnemu - dotyczące stworzenia repozytorium dokumentów w ramach systemu Fidelis oraz wprowadzenia kart hybrydowych. Propozycja dotycząca kart została zaakceptowana przez Dyrektora Generalnego w dniu 12 września 2015 r.

(dowód: akta kontroli Tom I str. 459, Tom II str. 508, 558-559)

Decyzją z dnia 9 stycznia 2014 r. Dyrektor Generalny MSP wyraził zgodę na stworzenie repozytorium dokumentów dla systemu Fidelis na podstawie wybranych danych przekazanych przez Dyrektorów Departamentów/Biur MSP.

System Fidelis analizuje ruch sieciowy m.in. wykrywa, alarmuje, blokuje, raportuje różnego rodzaju incydenty związane z naruszeniem zaimplementowanych do systemu polityk. Naczelnik Wydziału Systemów Teleinformatycznych w notatce do Dyrektora Generalnego podał, że: *„Do pełnego wykorzystania możliwości systemu brakuje bazy, repozytorium dokumentów (wzorów pism, notatek, etc.), które z uwagi na znaczenie dla organizacji powinny być dodatkowo chronione przed wyciekiem. Stworzenie takiego zbioru i jego późniejsza aktualizacja spowoduje utrzymanie aktualnie najwyższego możliwego poziomu bezpieczeństwa informacji MSP"*.

(dowód: akta kontroli Tom I str. 508)

Repozytorium takie nie zostało stworzone, pomimo że Zastępca Dyrektora Biura Dyrektora Generalnego MSP wskazywał na konieczność stworzenia repozytorium dokumentów, które z uwagi na znaczenie dla Ministerstwa powinny być dodatkowo chronione przez wyciekiem (tj. dokumenty zapisane w formie elektronicznej, których niekontrolowany wypływ może narazić MSP na straty materialne, szkodę na wizerunku bądź odpowiedzialność karno-cywilną).

(dowód: akta kontroli Tom II str. 508-513)

Zastępująca Dyrektora Generalnego MSP wyjaśniła, że *„do [BGD] nie wpłynęło żadne zgłoszenie z komórki organizacyjnej MSP, na podstawie którego można by było utworzyć repozytorium dla systemu Fidelis. Podczas realizacji umowy (...), której przedmiotem było wykonanie usługi przeprowadzenia audytu bezpieczeństwa infrastruktury sieciowej, audytu obecnego stanu zarządzania bezpieczeństwem informacji oraz ustanowienie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w [MSP], wykonawca przeprowadził klasyfikację informacji przetwarzanych w MSP przy współpracy z wyznaczonymi pracownikami komórek organizacyjnych."*

(dowód: akta kontroli Tom III str. 132)

W MSP funkcjonują następujące systemy informatyczne:

1) Zintegrowany System Informatyczny (ZSI db),
2) System Elektronicznego Zarządzania Dokumentacją (EZD),
3) system poczty elektronicznej,
4) system obiegu dokumentów Lotus Notes,
5) System Informatyczny Rejestrów (SIR),
6) System przesyłania sprawozdań „Publikator".

(dowód: akta kontroli Tom I str. 27-28)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

1.2. Plan zapewnienia bezpieczeństwa IT

Opis stanu faktycznego

Zarządzeniem nr 1 Dyrektora Generalnego Ministerstwa Skarbu Państwa z dnia 4 lutego 2014 r. wprowadzono do stosowania w MSP „Politykę bezpieczeństwa systemów teleinformatycznych Ministerstwa Skarbu Państwa" (dalej: Polityka Bezpieczeństwa).

(dowód: akta kontroli Tom I str. 10-23)

Stosownie do § 1 ust. 2 Polityki Bezpieczeństwa, dokument ten opracowano zgodnie z postanowieniami rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[5]. Dokument ten opracowany został przez Zespół ds. Bezpieczeństwa Teleinformatycznego.

Postanowienia Polityki Bezpieczeństwa obejmują w szczególności:

[5] Dz. U. Nr 100, poz. 1024.

- autoryzację i organizację bezpieczeństwa systemów teleinformatycznych,
- bezpieczeństwo fizyczne i środowiskowe,
- bezpieczeństwo sprzętu i zasobów informatycznych,
- kontrola i zarządzanie dostępem do sieci LAN,
- zarządzanie zmianami i konfiguracją,
- procedury dostępu do systemów i zasobów,
- dostęp i rejestracja użytkowników,
- zdalny dostęp.

(dowód: akta kontroli Tom I str. 9-23, Tom III str. 270, 273-274)

Do dnia zakończenia kontrolo w MSP nie opracowano szczegółowych procedur wskazanych w Polityce Bezpieczeństwa.

(dowód: akta kontroli Tom I str. 9-23, Tom II str. 229)

Instrukcja zarządzania systemem informatycznym w Ministerstwie Skarbu Państwa przyjęta została zarządzeniem nr 27 Dyrektora Generalnego MSP z dnia 9 września 2015 r.[6] i stanowi wypełnienie obowiązku Administratora danych związanego z prowadzeniem dokumentacji opisującej sposób przetwarzania danych oraz środki ich ochrony, zgodnie z art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[7] (zwanej dalej: uodo). W dokumencie tym ujęta została m.in. Instrukcja zarządzania systemem ZSI db obejmująca procedury: przydzielanie uprawnień dla użytkowników, uzyskiwanie dostępu do systemu, tworzenie i przechowywanie kopii zapasowych pozyskanych danych, zapewnienie aktualności i poprawności danych, rozpoczynanie i kończenie pracy oraz instrukcja postępowania w przypadku naruszenia ochrony danych osobowych.

(dowód: akta kontroli Tom I str. 24-99)

Ustalone nieprawidłowości

Oceniając poziom zarządzania procesami zapewnienia bezpieczeństwa systemów teleinformatycznych z punktu widzenia stosowanego w metodyce CobiT 4.1 Modelu dojrzałości, biorąc pod uwagę minimalne wymagania dla systemów teleinformatycznych zawarte w rozporządzeniu KRI oraz dobre praktyki, w tym zalecenia zawarte w Polskich Normach w zakresie działań związanych z zapewnieniem warunków bezpieczeństwa systemów informatycznych stwierdzono, że:

Polityka Bezpieczeństwa nie została opracowania zgodnie z rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[8] (dalej: KRI), na co w toku kontroli wskazywało kierownictwo MSP.

Dyrektor Generalny MSP podał, że *„projekt tworzenia dokumentacji dotyczącej bezpieczeństwa systemów IT w MSP rozpoczął się od prac nad stworzeniem dokumentu pn. „Polityka bezpieczeństwa systemów teleinformatycznych*

---

[6] Uprzednio obowiązywała Instrukcja zarządzania systemem ZSi db, ujęta w Instrukcji zarządzania systemem informatycznym w Ministerstwie Skarbu Państwa, stanowiąca załącznik nr 2 do zarządzenia nr 18 Ministra Skarbu Państwa z dnia 13 czerwca 2006 r. w sprawie ochrony danych osobowych w Ministerstwie Skarbu Państwa.

[7] Dz. U. z 2014 r., poz. 1182 ze zm.

[8] Dz. U. poz. 526 ze zm.

Ministerstwa Skarbu Państwa" w ograniczonym zakresie do stosowania ogólnych zasad oraz zbiorem reguł dotyczących wyłącznie zarządzania bezpieczeństwem systemów teleinformatycznych MSP. Rozporządzenie (...) znacznie szerzej definiuje wymagania dla m.in. systemów teleinformatycznych w zakresie ich stosowania. W związku z pracami związanymi z wdrożeniem [SZBI] przedmiotowy dokument zostanie zmodyfikowany i dostosowany do wymagań."

(dowód: akta kontroli Tom I str. 10-23, Tom III str. 201)

Ponadto, w Ministerstwie nie zostały opracowane procedury wskazane w Polityce Bezpieczeństwa, tj. brak jest m.in. procedury dostępu do obszarów bezpiecznych (§ 5 ust. 5), wydawania sprzętu (§ 6 ust. 3), przyjętego standardu oprogramowania (§ 7 ust. 2), uświadamiania pracowników o zagrożeniach związanych z pracą w sieci (§ 8 ust. 6), zarządzania dostępem do sieci LAN (§ 9 ust. 5), postępowania podczas zmian (§ 11 ust. 2), rejestrowania i wyrejestrowywania użytkowników (§ 14 ust. 1), rejestrowania konta użytkownika (§ 15 ust. 1), zdalnego zarządzania systemami oraz sprzętem (§ 17 ust. 4).

Dyrektor BDG podał, że „*wobec faktu, że obecnie w MSP wdrażany jest [SZBI] dokument „Polityka Bezpieczeństwa Systemów Teleinformatycznych Ministerstwa Skarbu Państwa" (PBST), który został wprowadzony w życie (...) już w trakcie realizacji umowy na wykonanie usługi przeprowadzenia audytu bezpieczeństwa infrastruktury sieciowej, audytu obecnego stanu zarządzania bezpieczeństwem informacji oraz ustanowienie i wdrożenie [SZBI] (...) podlegać będzie aktualizacji. Tworzenie odrębnych procedur, umów wskazanych w treści PBST są ściśle powiązane z ustanowieniem SZBI w MSP*".

(dowód: akta kontroli Tom I str. 9-23, Tom II str. 229)

W ocenie NIK Polityka Bezpieczeństwa, zawierająca ogólne zasady bezpieczeństwa teleinformatycznego w MSP, bez szczegółowych procedur, nie stanowi spójnego systemu ochrony bezpieczeństwa danych, który w możliwie pełnym stopniu minimalizuje ryzyka naruszenia tego bezpieczeństwa. Przyjęcie przez kierownictwo MSP rozwiązań tymczasowych jest działaniem nierzetelnym, wskazującym na nieosiągnięcie wymogu określonego w § 20 ust. 1 KRI, według którego podmiot realizujący zadania publiczne opracowuje i ustanawia, utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji.

1.3. Testowanie nadzorowanie i monitorowanie bezpieczeństwa

Opis stanu faktycznego

W dniu 20 listopada 2013 r. zawarto z konsorcjum EXATEL S.A., Eversys Sp. z o.o. i Prevenity Sp. z o.o. (dalej: audytor zewnętrzny) umowę na przeprowadzenie audytu bezpieczeństwa infrastruktury sieciowej i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

W dniu 4 kwietnia 2014 r. kierownictwu MSP przedłożono Analizę obecnego stanu bezpieczeństwa informacji oraz stosowanych metod ich ochrony. Głównym celem prac było „*zidentyfikowanie ewentualnych niezgodności i niedociągnięć oraz wskazanie koniecznych udoskonaleń w stosowanych środkach bezpieczeństwa organizacyjnego i technicznego, w odniesieniu do wymagań i wytycznych określonych w przepisach prawa, standardzie ISO/IEC 27001:2005 oraz innych regulacjach mających odniesienie do funkcjonowania MSP.*" W wyniku

przeprowadzonych działań[9] stwierdzono, że w Ministerstwie nie funkcjonuje System Zarządzania Bezpieczeństwem Informacji. Na podstawie przeprowadzonych wywiadów, analiz i obserwacji, stwierdzono również znaczny stopień niezgodności stosowanego obecnie podejścia z wymaganiami standardu ISO/IEC 27001 oraz dobrymi praktykami w obszarze bezpieczeństwa informacji.

W celu wyeliminowania lub ograniczenia stwierdzonych podatności audytor zewnętrzny zalecił MSP podjęcie m.in. działań w zakresie:

1) przeglądu elementów infrastruktury IT pod kątem aktualności stosowanego oprogramowania i podjęcia działań mających na celu eliminację przypadków stosowania oprogramowania niewspieranego obecnie przez producentów oraz przypadków stosowania oprogramowania ze znanymi podatnościami bezpieczeństwa,
2) wdrożenia polityki haseł i blokowania kont dostępowych użytkowników w elementach infrastruktury IT i aplikacjach, które wspierają takie rozwiązania,
3) analizy zakresu dostępu podmiotów zewnętrznych do informacji uznanych przez audytora zewnętrznego za wrażliwe.

(dowód: akta kontroli Tom I str. 139-212)

W odniesieniu do realizacji zaleceń powyższego audytu zewnętrznego Dyrektor BDG wyjaśnił w kwestii:

a) przeglądu elementów infrastruktury IT: *„w wyniku przeprowadzonych prac w dniu 21 września 2015 r. zostało opublikowane ogłoszenie o zamówieniu publicznym, którego przedmiotem jest modernizacja infrastruktury teleinformatycznej MSP wraz ze wsparciem serwisowym, co pozwoli na zrealizowanie rekomendacji*",

b) wdrożenia polityki haseł i blokowania kont: *„zakres dotyczący wdrożenia polityki haseł i zarządzania kontami zawarto w projekcie przygotowywanego dokumentu SZBI",*

c) analizy zakresu dostępu podmiotów zewnętrznych do informacji wrażliwych: *jeżeli chodzi o dostęp podmiotów zewnętrznych do informacji przetwarzanych w systemach MSP - w zawartych umowach występują zapisy gwarantujące zabezpieczenie poufności informacji uzyskanych w związku z ich realizacją przez wykonawców.*

(dowód: akta kontroli Tom III str. 167, umowy)

W dniu 14 kwietnia 2014 r. audytor zewnętrzny przedłożył dokument „Audyt środowiska IT oraz usługi konsultacyjne dla Ministerstwa Skarbu Państwa". W dokumencie tym przedstawiono wyniki przeglądu pod kątem poprawności konfiguracji i podatności na zagrożenia, konfiguracji serwerów oraz urządzeń sieciowych pracujących w sieci MSP i realizujących funkcje na jego rzecz.

(dowód: akta kontroli Tom I str. 220-416)

---

[9] W przeprowadzonej analizie, zaznaczono, że: „ocena stanu bezpieczeństwa informacji i stosowanych metod ich ochrony w MSP, odzwierciedla stan obecny i nie uwzględnia efektów jakie są spodziewane w wyniku prowadzonych obecnie działań projektowych".

W okresie objętym kontrola nie przeprowadzano testów bezpieczeństwa Zintegrowanego Systemu Informatycznego MSP.

Dyrektor BDG wyjaśnił m.in., że testy bezpieczeństwa *„zaplanowane są do wykonania jako jeden z elementów planowanego na lata 2016/2017 audytu bezpieczeństwa infrastruktury sieciowej MSP."*

(dowód: akta kontroli Tom II str. 382-383)

Zdaniem NIK przeprowadzanie takich testów jest w chwili obecnej standardem monitorowania bezpieczeństwa i istotnym elementem ciągłego doskonalenia procesu zapewnienia bezpieczeństwa. Obowiązek zarządzania podatnościami technicznymi wynika z pkt. A.12.6.1 normy PN-ISO/IEC 27001[10].

Stosownie do art. 20 ust. 2 pkt 14 rozporządzenia KRI, zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

W okresie od 30 września do 3 grudnia 2014 r. Zespół Audytu Wewnętrznego MSP przeprowadził audyt w zakresie bezpieczeństwa informacji, którego celem była ocena zgodności funkcjonowania systemu zarządzania bezpieczeństwem informacji.

W ramach zadania audytowego stwierdzono m.in. słabości kontroli zarządczej obejmujące: brak szczegółowych procedur, o których mowa w Polityce Bezpieczeństwa oraz brak mechanizmów umożliwiających liczenie i monitorowanie rodzajów, rozmiarów i kosztów incydentów związanych z bezpieczeństwem systemów teleinformatycznych (np. rejestr incydentów).

(dowód: akta kontroli Tom I str. 417-444)

W planie audytu wewnętrznego na 2015 r. ujęto zadanie zapewniające pn. Ocena wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji.

(dowód: akta kontroli Tom I str. 445-448)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

1.4. Definicja incydentu związanego z bezpieczeństwem

Opis stanu faktycznego

Obsługa incydentów bezpieczeństwa należy do zakresu zadań Zespołu ds. Bezpieczeństwa Teleinformatycznego.

(dowód: akta kontroli Tom I str. 476-480)

Rejestry incydentów w Ministerstwie Skarbu Państwa prowadzone są odrębnie dla zdarzeń przekazanych przez Zespół Reagowania na Incydenty Komputerowe CERT oraz odrębnie dla zdarzeń zidentyfikowanych przez Helpdesk.

Klasyfikacja problemu i incydentu opisana jest w dokumencie „Instrukcja operatora", stanowiącym element systemu rejestracji zgłoszeń informatycznych. System ten został uruchomiony w dniu 4 maja 2015 r.

---

[10] Zgodnie z tym pkt. Informacje o podatnościach technicznych wykorzystywanych systemów informacyjnych należy niezwłocznie pozyskiwać, oceniać stopień narażenia organizacji na te podatności i podejmować odpowiednie środki w celu przeciwdziałania związanemu z nim ryzyku.

Zgodnie z ww. Instrukcją incydent to *„każde zdarzenie, które powoduje, lub może powodować przerwę w dostarczaniu usługi informatycznej zdefiniowanej na przykład, jako dostępność lub wydajność systemu, czy też pewna określona jego funkcjonalność"*. Jako problem zdefiniowano zaś *„nieznaną przyczynę jednego lub wielu incydentów"*.

(dowód: akta kontroli Tom II str. 389, 406-472)

Ministerstwo na bieżąco współpracuje z Zespołem Reagowania na Incydenty Komputerowe CERT.GOV.PL. Wydział Systemów Teleinformatycznych otrzymuje od Agencji Bezpieczeństwa Wewnętrznego (dalej: ABW) zalecenia co do blokowania ruchu z/do niebezpiecznych adresów oraz domen, jak również informacje na temat wykrytych zagrożeń bezpieczeństwa, zaleceń co do konfiguracji urządzeń itp. W ramach współpracy z ABW w MSP została wdrożona sonda systemu ARAKIS-GOV (bezterminowo).

W okresie objętym kontrolą wystąpiło 31 incydentów zgłoszonych przez CERT.GOV.PL. W odpowiedzi na zgłaszane zagrożenia każdorazowo podejmowano stosowne działania, obejmujące aktualizacje systemów, blokady adresów na firewallach oraz wyłączanie zbędnych usług.

(dowód: akta kontroli Tom II str. 473-490)

Pracownicy Ministerstwa, odpowiedzialni m.in. za bezpieczeństwo infrastruktury IT rozpowszechniali informacje o potencjalnych zagrożeniach, ich przyczynach i metodach uniknięcia poprzez przesyłanie pracownikom MPS korespondencji mailowej.

(dowód: akta kontroli Tom II str. 526-530)

Ustalone nieprawidłowości

Oceniając poziom zarządzania procesami zapewnienia bezpieczeństwa systemów teleinformatycznych z punktu widzenia stosowanego w metodyce CobiT 4.1 Modelu dojrzałości, biorąc pod uwagę minimalne wymagania dla systemów teleinformatycznych zawarte w rozporządzeniu KRI oraz dobre praktyki, w tym zalecenia zawarte w Polskich Normach w zakresie działań związanych z zapewnieniem warunków bezpieczeństwa systemów informatycznych stwierdzono, że w Ministerstwie funkcjonują dwa odrębne rejestry incydentów prowadzone przez:

- Wydział Systemów Teleinformatycznych – w wykazie ujęto 31 zdarzeń[11] dotyczących wyłącznie informacji uzyskanych z CERT.GOV.PL (klient botnetu, fałszywe emaile o podłożeniu ładunków wybuchowych, ataki przeciwko szyfrom),
- Wydział Wsparcia IT w ramach systemu rejestracji zgłoszeń informatycznych (Helpdesk) – w rejestrze ujęto łącznie 11 wpisów[12] dotyczących zainfekowanego komputera i wiadomości pocztowych oraz udostępnienia konta i hasła do domeny msp osobie nieuprawnionej będącej pracownikiem MSP.

(dowód: akta kontroli Tom II str. 473-490, Tom III str. 286-285)

[11] Na dzień 25 sierpnia 2015 r.

[12] Na dzień 30 września 2015 r.

Ponadto, w MSP nie zdefiniowano mierników pozwalających na identyfikację powtarzających się rodzajów incydentów i klasyfikację ich istotności. W toku kontroli nie wskazano również, w jaki sposób gromadzone są dowody umożliwiające ewentualne zgłoszenie stwierdzonego incydentu obejmującego naruszenie przepisów prawa / regulacji wewnętrznych oraz wymagań związanych z zawartymi umowami z dostawcami usług informatycznych.

W odniesieniu do powyższych kwestii Dyrektor BDG podał jedynie, że *„rozpoczęty proces związany z rejestracją incydentów pozwoli w perspektywie czasu na dokonanie analizy, a w efekcie końcowym na zdefiniowanie i sklasyfikowanie powtarzających się zdarzeń i incydentów."*

(dowód: akta kontroli Tom I str. 180, Tom III str. 167)

W ocenie NIK brak jednego, zcentralizowanego rejestru incydentów uniemożliwia kierownictwu Ministerstwa stworzenie odpowiednich warunków do monitorowania stanu bezpieczeństwa jednostki, reagowania na incydenty oraz analizowania ich w celu doskonalenia sytemu zabezpieczeń. Zalecenie określenia procedur związanych z odnotowywaniem działań dotyczących incydentów bezpieczeństwa zawarte jest w pkt. 16.1.1. normy PN-ISO/IEC 27002.

Brak jednolitej procedury reagowania oraz jednoznacznego wskazania komórki odpowiedzialnej za reakcję, NIK ocenia jako nierzetelne i wskazujące na nieosiągnięcie wymogu określonego w § 20 ust. 2 pkt 13 KRI, według którego zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

1.5. Zarządzanie kluczami kryptograficznymi

Opis stanu faktycznego

Zgodnie z informacją przekazaną przez Zastępcę Dyrektora BDG *„obsługa PKI w zakresie używania zabezpieczeń kryptograficznych i zarządzania kluczami kryptograficznymi obecnie obejmuje urządzenia (komputery i serwery)."*

(dowód: akta kontroli Tom II str. 519)

Na I półrocze 2016 r. planowane jest uruchomienie systemu PKI rozbudowanego o zarządzanie i obsługę kart inteligentnych „Smart Card" dla pracowników Ministerstwa. W związku z realizacją powyższego zadania w dniu 3 lutego 2015 r. przygotowany został, w ramach dokumentacji powykonawczej, dokument - „System PKI dla Ministerstwa Skarbu Państwa".

(dowód: akta kontroli Tom II str. 558-584)

Według informacji przekazanych przez Dyrektora BDG system ZSI nie korzysta z zabezpieczeń kryptograficznych.

(dowód: akta kontroli Tom II str. 518)

Dyrektor BDG wyjaśnił, że *„obecnie zastosowanie kryptografii dla [ZSI] z uwagi na jego dostępność dla pracowników, która realizowana jest wyłącznie w siedzibie urzędu, nie jest w MSP wymagane. Ponadto (...) zastosowanie kryptografii wpłynęłoby negatywnie na wydajność systemu ZSI i w znaczący sposób obniżyłoby*

komfort pracy z systemem. Ponadto wprowadzenie mechanizmów szyfrowania danych wiązałoby się z zakupem dodatkowych (płatnych) opcji dla RDBMS Oracle takich, jak Oracle Advanced Security, czy Oracle Label Security".

(dowód: akta kontroli Tom III str. 228)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości

1.6. Ochrona przed złośliwym oprogramowaniem, jego wykrywanie i wprowadzanie poprawek

Opis stanu faktycznego

W MSP nie było formalnie przyjętej polityki zapobiegania złośliwemu oprogramowaniu. W Ministerstwie funkcjonowały: system antywirusowy i antyspamowy Secure Mail Inteligence (SMI) oraz centralny system antywirusowy GData.

(dowód: akta kontroli Tom II str. 384-387)

W przypadku wykrycia złośliwego oprogramowania przez system SMI jest ono usuwane, a użytkownik do którego adresowana była przesyłka otrzymuje informację o treści „wiadomość zainfekowana". System antywirusowy po wykryciu złośliwego oprogramowania informuje użytkownika komunikatem o infekcji, a zainfekowany plik zostaje usunięty.

(dowód: akta kontroli Tom III str. 178-180)

Sprawność procesu dystrybucji oprogramowania, uaktualnień i definicji weryfikowana była przez pracowników Wydziału Wsparcia IT. Procesy związane z dystrybucją oprogramowania, jego aktualizacją oraz aktualizacją definicji dokonywane są automatycznie dla stacji roboczych w ramach domeny. Dla komputerów spoza domeny, instalacja oprogramowania wykonywana jest przez pracowników IT, a proces aktualizacji oprogramowania, jak i definicji, konfigurowany jest automatycznie.

W toku kontroli nie przekazano dokumentacji potwierdzającej przeprowadzenie ww. weryfikacji oraz nie wskazano, w jaki sposób zapewniono aby wszystkie komputery spoza domeny posiadały zainstalowane oprogramowanie antywirusowe.

W odniesieniu do systemu SMI dostęp do konsoli posiadają pracownicy Helpdesku. Aktualizacja definicji baz silników antywirusowych i antyspamowych wykonywana jest automatycznie.

W przypadku systemu SMI, wykryte nowe zagrożenia, które nie zostały zidentyfikowane, wysłane są (w postaci załącznika) do producenta oprogramowania w celu aktualizacji definicji baz silników antywirusowych i antyspamowych. W okresie objętym kontrolą wystąpiło 9 takich przypadków.

Przypadki szkodliwego oprogramowania GData wykryte na stacjach roboczych pracowników oraz serwerach są automatycznie rejestrowane w systemie Helpdesk. W systemie SMI pracownicy Helpdesk mają możliwość wglądu do statystyk przetworzonych danych przez zastosowane filtry antywirusowe i antyspamowe.

Poczta elektroniczna w MSP chroniona jest przed zagrożeniami przez zastosowane filtry antywirusowe i antyspamowe systemu SMI.

(dowód: akta kontroli Tom III str. 163-164, 182-194)

Umowa na dostawę i instalację Systemu monitorowania sieci, ochrony informacji poufnych (Fidelis) została zawarta w 2011 r. i obejmowała 36-miesięczny okres gwarancji na poprawne funkcjonowanie systemu. Ministerstwo podpisało w dniu 30 września 2013 r.[13] umowę wsparcia w ramach systemu Fidelis.

Dyrektor BDG podał, że po upływie okresu gwarancyjnego na system Fidelis nie odnotowano jego awarii, jest on nadal funkcjonalny i był aktualizowany. Ze względu na ograniczone środki budżetowe nie był rozbudowywany.

(dowód: akta kontroli Tom II str. 392-405, Tom III str. 165-166)

W dniu 28 października 2015 r. MSP zawarło z Eversys Sp. z o.o. umowę na usługi wsparcia technicznego i serwisowego dla systemu DLP opartego o platformę Fidelis Security. W ramach umowy wykonawca zobowiązał się m.in. do przeprowadzenia analizy obecnej konfiguracji architektury systemu, aktualizacji oprogramowania do najnowszej wersji, zaprojektowania i implementacji nowych polityk ochrony przed wyciekiem informacji przy współpracy z pracownikami Wydziału Systemów Teleinformatycznych oraz przeprowadzenia analiz incydentów w siedzibie MSP.

(dowód: akta kontroli Tom III str. 239-242)

Pracownicy Ministerstwa otrzymywali na skrzynki pocztowe informacje o zagrożeniach możliwych do wystąpienia w systemach teleinformatycznych użytkowanych w MSP.

(dowód: akta kontroli Tom II str. 526-551)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości

1.7. Bezpieczeństwo sieciowe

Opis stanu faktycznego

Ewidencja aktywów wspierających, dotycząca infrastruktury sieciowej, prowadzona jest w bazie danych systemu Optiest. W bazie tej ujęte są następujące dane: kod kreskowy, nazwa (np. serwer, macierz), nr inwentarzowy oraz wartość. Oprogramowanie nie posiada funkcjonalności umożliwiającej przyporządkowanie różnych poziomów ochrony dla poszczególnych aktywów.

(dowód: akta kontroli Tom II str. 516, Tom III str. 233-234)

Zadania związane z zarządzaniem (konfiguracją) sprzętem sieciowym realizowane są w ramach umowy z Betacom S.A. na świadczenie usług wsparcia technicznego sieci LAN w Ministerstwie. Zakres obowiązków wykonawcy obejmuje m.in. aktualizację firmware, przegląd logów, okresowe przeglądanie wykonanych kopii bezpieczeństwa, ciągły monitoring urządzeń sieci LAN. Zgodnie z postanowieniami umowy wykonawca przedkładał MSP miesięczne raporty z jej realizacji.

(dowód: akta kontroli Tom II str. 249-263 Tom III str. 198)

---

[13] MSP/FSP/140-00/2013.

Zastępca Dyrektora BDG podała m.in., że *„stosując dobre praktyki w przypadku wykonania kopii bezpieczeństwa po wykonywanych czynnościach administracyjnych związanych ze zmianą konfiguracji, wdrożono rozwiązanie systemowe (używanego przez MSP dedykowanego oprogramowania Cisco Works), które automatycznie wykonuje kopię bezpieczeństwa konfiguracji urządzeń sieciowych po każdej zmianie oraz cyklicznie (raz na dobę) sprawdza stan obecnej konfiguracji z ostatnią zapisaną."*

(dowód: akta kontroli Tom II str. 516-517)

W toku kontroli nie przedstawiono formalnej procedury w zakresie bezpieczeństwa dla systemów mobilnych. Według wyjaśnień BDG bezpieczeństwo takie zapewniane było poprzez :

a) przeprowadzenie przez pracowników Helpdesku procesu szyfrowania dysku w oparciu o Instrukcję dot. szyfrowania dysków twardych w notebookach (za pomocą dedykowanego oprogramowania „Safend"),
b) instalację oprogramowania antywirusowego w oparciu o Instrukcję dot. instalacji klienta oprogramowania antywirusowego,
c) blokowanie kont administracyjnych,
d) ustawienia hasła do BIOSu,
e) ustawieniu silnego hasła dla założonego konta użytkowania.

(dowód: akta kontroli Tom II str. 518, 552-557)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości

Ocena cząstkowa

W oparciu o stosowany w metodyce CobiT 4.1 Model dojrzałości, NIK ocenia poziom zarządzania procesem „zapewnienie bezpieczeństwa systemów informatycznych" w MSP jako „powtarzalne lecz intuicyjne". W kontrolowanej jednostce istnieje świadomość potrzeby zapewnienia bezpieczeństwa teleinformatycznego, jednak jest ona fragmentaryczna i ograniczona. Rozwijana jest polityka dotycząca bezpieczeństwa, ale nie towarzyszą jej adekwatne narzędzia. Bezpieczeństwo IT jest postrzegane głównie, jako przedmiot odpowiedzialności i domena działu IT, a nie zadanie leżące w gestii całego Ministerstwa. Na ocenę tę miały wpływ nieprawidłowości związane z całokształtem funkcjonowania MSP w zakresie zapewnienia warunków bezpieczeństwa systemów informatycznych. Zdaniem NIK nie jest to wystarczający i akceptowalny poziom zarządzania w badanym obszarze.

2. Wspieranie bezpieczeństwa na poziomie wybranego systemu

2.1. Zarządzanie tożsamością

Opis stanu faktycznego

Według informacji przekazanych przez Dyrektora BDG zarządzanie tożsamością w Ministerstwie oparte jest na:

a) zarządzeniu nr 27 Dyrektora Generalnego MSP z dnia 9 września 2015 r. z załącznikiem – Instrukcja Zarządzania Systemem Informatycznym w MSP,

b) procesie wnioskowania o nadanie uprawnień przez przełożonego pracownika,

c) weryfikacji wnioskowanych uprawnień („*w przypadku gdy nadanie pracownikowi wymaganych uprawnień może grozić naruszeniem standardów bezpieczeństwa systemów informowany jest wnioskodawca oraz Zespół ds. Bezpieczeństwa Teleinformatycznego o zagrożeniu i wstrzymywany jest proces nadawania uprawnień*"),

d) nadaniu uprawnień przez administratora systemu.

W wyniku analizy sprawozdań Zespołu ds. Bezpieczeństwa Teleinformatycznego stwierdzono, że w latach 2014-2015 kierownictwo MSP nie było informowane o przypadkach wskazanych w pkt. c).

(dowód: akta kontroli Tom II str. 231-248, Tom III str. 226)

System ZSI db co do zasady nie jest udostępniany na zewnątrz infrastruktury Ministerstwa, a dostęp do niego posiadają wyłącznie uwierzytelnieni użytkownicy w siedzibie MSP (posiadający konto w domenie MSP).

Dyrektor BDG podał, że „*mechanizm weryfikacji tożsamości podczas uzyskiwania dostępu do systemu ZSI w przypadku pracowników zdalnych, obejmuje pracowników zdalnego dostępu tj. wyłącznie administratora systemu ZSI db oraz pracowników serwisu – firmy Comarch. MSP nie konfiguruje zdalnego dostępu do systemu ZSI pracownikom urzędu.*"

Do udzielonych wyjaśnień nie załączono dokumentów określających sposób, w jaki dokonywana jest weryfikacja tożsamości pracowników zdalnego dostępu.

(dowód: akta kontroli Tom III str. 227-246)

W odniesieniu do odnotowywania działań użytkowników lub obiektów systemowych w dziennikach systemu ZSI Dyrektor BDG podał że: „*w historii błędów systemu ZSI odnotowywane są błędy krytyczne ZSI. Audyt aktywności użytkowników jest przeprowadzany tylko w ten sposób, że przy każdym zapisie danych jest zapisywana informacja, kto utworzył rekord, kiedy utworzył, kto modyfikował i kiedy modyfikował. To daje informacje o utworzeniu rekordu i o ostatniej modyfikacji. Dokładniejszy audyt nie jest prowadzony, ponieważ byłoby to zbyt kosztowne w przetwarzaniu.*"

(dowód: akta kontroli Tom III str. 228)

Zgodnie z § 16 Polityki Bezpieczeństwa, hasła kont administracyjnych systemów MSP były zdeponowane w zaklejonych kopertach, przechowywanych w sejfie. Dostęp fizyczny do istotnych dla bezpieczeństwa elementów systemów sieciowych ograniczony jest poprzez kontrolowany dostęp wyłącznie dla osób uprawnionych.

(dowód: akta kontroli Tom I str. 19,Tom II str. 517, Tom III str. 196)

BDG, tj. jednostka organizacyjna odpowiadająca za bezpieczeństwo systemów teleinformatycznych Ministerstwa nie posiada informacji na temat sposobu weryfikacji poprawności działania systemu ZSI.

Dyrektor BGD podał m.in., że „*w przypadku stwierdzonej nieprawidłowości pracownicy zgłaszają do administratora ZSI zdarzenie, które jest rejestrowane w zewnętrznym systemie zgłoszeń pn. IZGL (...) System zgłoszeń IZGL*

obsługiwany jest przez firmę (Comarch S.A.) realizującą zapisy umowy na świadczenie usług asysty technicznej, usług konsultacyjnych oraz serwisu Zintegrowanego Systemu Informatycznego dla Ministerstwa Skarbu Państwa."

Do wyjaśnień załączono przykładowe zgłoszenie dotyczące m.in. podejrzenia błędnego działania systemu, nie wskazano jednakże liczby takich zgłoszeń oraz działań podejmowanych przez Comarch S.A. w celu ich wyeliminowania.

(dowód: akta kontroli Tom III str. 227, 280-281)

W ocenie NIK brak wiedzy działu IT, a co za tym idzie kierownictwa Ministerstwa, o prawidłowości działania systemów m.in. z uwagi na powierzenie obsługi tego typu działalności podmiotowi zewnętrznemu powodować może zbytnie uzależnienie MSP od informacji przekazywanych przez dostawcę systemu. Na szeroki dostęp dostawców zewnętrznych do danych Ministerstwa wskazywał również raport audytora zewnętrznego.

Ustalone nieprawidłowości

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

W dziennikach systemu ZSI nie są odnotowywane obligatoryjnie działania użytkowników lub obiektów systemowych, polegające na dostępie do:
- systemu z uprawnieniami administracyjnymi,
- konfiguracji systemu, w tym konfiguracji zabezpieczeń,
- przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.

Tym samym Zintegrowany System Informatyczny MSP nie spełnia wymogów, o których mowa w § 21 ust. 1 rozporządzenia KRI, który stanowi, że rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach). Ponadto, zgodnie z pkt. 12.4 normy ISO/IEC 27002 zaleca się tworzenie, przechowywanie i systematyczne przeglądanie dzienników zdarzeń rejestrujących działania użytkowników, wyjątki, usterki oraz zdarzenia związane z bezpieczeństwem informacji.

(dowód: akta kontroli Tom III str. płyta logi)

Dyrektor BDG podał m.in., że „*w chwili obecnej, ze względu na aktualny standard aplikacji ZSI, uruchomienie szczegółowych logów wpłynęłoby negatywnie na wydajność systemu ZSI i w znaczący sposób obniżyłoby komfort pracy z systemem.*"

(dowód: akta kontroli Tom II str. 382)

2.2. Zarządzanie kontami użytkowników

Opis stanu faktycznego

Kontrola dostępu do systemu ZSI opiera się na identyfikacji użytkownika poprzez podanie indywidualnego identyfikatora i hasła dostępu. Hasło składa się minimalnie z 8 znaków, w tym z wielkich i małych liter oraz cyfr. Użytkownik ma obowiązek zmiany hasła co 30 dni, co jest automatycznie wymuszane przez system.

(dowód: akta kontroli Tom II str. 382)

W raporcie z audytu zewnętrznego, przeprowadzonego przez firmę Exatel wskazano, że system ZSI nie posiada włączonego mechanizmu polityki haseł, w tym

standardów przechowywania haseł dostępowych użytkowników, a w szczególności administratorów, co może doprowadzić do przejęcia kontroli przez osoby trzecie.

(dowód: akta kontroli Tom I str. 175)

Dyrektor BDG wyjaśnił, że *„obecnie system ZSI nie posiada włączonego mechanizmu polityki haseł. Logowanie do ZSI nie może się odbyć z pominięciem procesu logowania (uwierzytelnianie) uprawnionego pracownika do domeny MSP. System ZSI jest dostępny wyłącznie w siedzibie MSP z poziomu sieci lokalnej."*

(dowód: akta kontroli Tom III str. 166)

Zgodnie z § 14 Polityki Bezpieczeństwa nadawanie lub odbieranie uprawnień jest sformalizowane, tj. na podpisanym przez dyrektora komórki organizacyjnej wniosku lub formularzu uprawnień jednostkowych. W przypadku wygaśnięcia konta pracownika lub dla konta uprzywilejowanego, odnowienie uprawnień odbywa się wyłącznie na podstawie dostarczonego do BDG wniosku lub formularza.

Wnioski „Wydanie sprzętu informatycznego / założenie konta/uprawnienia konta użytkownika sieci komputerowej MSP" zawierały, zgodnie z ww. Instrukcją, w szczególności następujące dane: imię i nazwisko, komórkę organizacyjną i numer pokoju pracownika wraz z datą zatrudnienia. Dla poszczególnych pracowników, według zapotrzebowania, we wnioskach należało wskazać (tak/nie) odpowiednio: wydanie zestawu komputerowego, założenie konta w domenie MSP, Lotus Notes, poczta zewnętrzna, dostęp do aplikacji ZSI, uprawnienia do LEX, Internet.

(dowód: akta kontroli Tom III str. 133-145, 164)

Nadawanie lub odbieranie uprawnień danych użytkowników ZSI jest sformalizowane, tj. na podpisanym przez dyrektora komórki formularzu uprawnień jednostkowych. Weryfikacja i modyfikacja danych użytkowników ZSI dokonywana jest przez administratora systemu na podstawie informacji otrzymywanych drogą mailową z Biura Zarządzania Zasobami Ludzkimi.

(dowód: akta kontroli Tom I, str. 17-19, Tom III str. 215-216, 256-266)

W Ministerstwie nie określono formalnie zasad informowania Biura Dyrektora Generalnego MSP o absencjach pracowników. W toku kontroli stwierdzono, że odbywa się to drogą elektroniczną kilka razy w miesiącu.

(dowód: akta kontroli Tom III str. 27-28, 256-266)

Dyrektor Biura Zarządzania Zasobami Ludzkimi podała m.in., że *„stosownie do przyjętej przez MSP praktyki, informacje dot. m.in. długotrwałych absencji pracowników MSP, Biuro Zarządzania Zasobami Ludzkimi przekazuje na bieżąco i niezwłocznie drogą mailową. Co do zasady za absencję o trwałym charakterze przyjmuje się nieobecność powyżej miesiąca i są to urlopy bezpłatne, wychowawcze, urlopy związane z rodzicielstwem oraz świadczenia rehabilitacyjne".*

(dowód: akta kontroli Tom III str. 289)

Ustalone nieprawidłowości

Oceniając poziom zarządzania procesami zapewnienia bezpieczeństwa systemów teleinformatycznych z punktu widzenia stosowanego w metodyce CobiT 4.1 Modelu dojrzałości, biorąc pod uwagę minimalne wymagania dla systemów teleinformatycznych zawarte w rozporządzeniu KRI oraz dobre praktyki, w tym zalecenia zawarte w Polskich Normach w zakresie działań związanych

z zapewnieniem warunków bezpieczeństwa systemów informatycznych stwierdzono jak poniżej.

W logach systemu ZSI znalazło się m.in. 79 logowań użytkownika o nazwie „szkolenie". Zgodnie z protokołem uzgodnień z Comarch S.A. w dniach 3-4 marca 2014 r. w MSP odbyło się szkolenie z zakresu podstaw języka SQL.

(dowód: akta kontroli Tom III str. 217-222,290)

Zgodnie z wyjaśnieniami Dyrektora BDG konto to zostało utworzone i wykorzystane na potrzeby szkolenia z języka zapytań SQL, a użytkownik ten posiadał dane testowe oferowane przez firmę Oracle. Konto nie posiadało dostępu do danych zawartych w ZSI i zostało omyłkowo usunięte z systemu.

(dowód: akta kontroli Tom III str. 228)

Główny specjalista w BDG podała, że: *„konto „szkolenie" zostało fizycznie skasowane i w związku z tym nie można podać daty jego usunięcia. W dniu dzisiejszym nie da się potwierdzić osoby, która utworzyła i skasowała to konto, ale jedynie ja posiadam stosowane uprawnienia więc jestem pewna, że to ja jako administrator to konto utworzyłam i skasowałam."*

(dowód: akta kontroli Tom III str.215)

Ponadto, w logach systemu ZSIdb zarejestrowano 1439 logowań, w których w miejscu nazwy użytkownika domeny pojawiało się puste pole.

(dowód: akta kontroli Tom III str.290)

Dyrektor BDG podał, że *„połączenia odbyły się za pomocą jdbc – Java DataBase Connectivity – łącze do baz danych w języku Java (wykorzystywane w narzędziach oracle'a typu Oracle Universal Installer itp.). Część logowań z pustym polem dotyczy logowań użytkowników z uprawnieniami administratora zalogowanych na serwerze bazy danych."*

(dowód: akta kontroli Tom II str. 382)

Administrator eksploatowanych w MSP instancji Oracle RDBMS podała, że *„Takie przypadki mają miejsce jeżeli jest to logowanie bezpośrednio na serwerze bazy danych albo logowanie poprzez narzędzia, które nie przekazują danych o użytkowniku domenowym. Podstawowe dane o logującym się użytkowniku to jego nazwa w bazie danych i przy logowaniu do systemu nazwa ta zawsze musi być podana. Nie ma możliwości zalogowania się do bazy danych bez podania nazwy użytkownika bazodanowego."*

(dowód: akta kontroli Tom III str. 215)

W ocenie NIK ww. przypadki wskazują na nierzetelne prowadzenie dzienników systemowych skutkujące brakiem pełnej rozliczalności systemów teleinformatycznych MSP. Było to niezgodne z § 21 ust. 1 rozporządzenia KRI, który stanowi, że rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach). Ponadto, zgodnie z zaleceniem pkt. 9.2.1 normy ISO/IEC 27002 należy używać unikatowych identyfikatorów użytkowników, pozwalających na jednoznaczne przypisanie działań i odpowiedzialności za nie. Stosowanie identyfikatorów

grupowych powinno być ograniczone do szczególnych przypadków oraz zatwierdzone i udokumentowane.

2.3. Ochrona technologii zabezpieczeń

Opis stanu faktycznego

Historia zmian konfiguracji jest rejestrowana (zainstalowanie patchy). Informacje o instalacjach są odkładane w dzienniku instalacji.

(dowód: akta kontroli Tom III: str. 169-170)

Dyrektor BDG wyjaśnił, że *„ograniczony dostęp wynika z nadawanych uprawnień do ZSI przez administratora* (w przypadku gdy pracownik nie ma dostępu do pewnej funkcjonalności – nie zostanie ona wyświetlona w aplikacji ZSI lub dostępnym menu).

(dowód: akta kontroli Tom III: str. 165, 171-172)

W wyniku oględzin trzech losowo wybranych komputerów stacjonarnych w Ministerstwie stwierdzono, że przy starcie systemu operacyjnego pomijany jest port usb. Ponadto, wszystkie komputery były zabezpieczone plombami zabezpieczającymi przed fizycznym dostępem do ich podzespołów.

(dowód: akta kontroli Tom III: str. 195)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości

2.4. Wymiana wrażliwych danych

Opis stanu faktycznego

W badanym okresie w MSP był powołany Administrator Bezpieczeństwa Informacji[14] oraz obowiązywała dokumentacja dotycząca ochrony danych osobowych wymagana przepisem art. 36 i 36a uodo tj.:

- „Polityka bezpieczeństwa ochrony danych osobowych w Ministerstwie Skarbu Państwa" (dalej: Polityka Bezpieczeństwa lub PBI). W badanym okresie PBI była raz aktualizowana[15];
- „Instrukcja zarządzania systemem informatycznych w Ministerstwie Skarbu Państwa".
- „Polityka bezpieczeństwa Systemów Teleinformatycznych Ministerstwa Skarbu Państwa" (dalej Polityka Bezpieczeństwa Systemów Teleinformatycznych lub PBST).

(dowód: akta kontroli Tom I str. 10-99, Tom II: str. 75-172)

Stosownie do § 20 ust. 1 oraz ust. 2 pkt 1 rozporządzenia KRI podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji

---

[14] Na podstawie Zarządzenia Nr 34 Ministra Skarbu Państwa z dnia 21 lipca 2010 r. w sprawie ochrony danych osobowych w Ministerstwie SP, zastąpionego Zarządzeniem Nr 14 Ministra SP z dnia 23 kwietnia 2015 r. w sprawie ochrony danych osobowych w Ministerstwie SP.

[15] Do dnia 24 kwietnia 2015 r. obowiązywała PBI wprowadzona Zarządzeniem nr 3 Dyrektora Generalnego MSP z dnia 1 lutego 2011 r. w sprawie „Polityki Bezpieczeństwa ochrony danych osobowych w MSP". Została ona zastąpiona PBI wprowadzoną Zarządzeniem Nr 12 Dyrektora Generalnego MSP z dnia 24.04.2015 r. w sprawie wskazania zadań administratora danych, powołania administratora bezpieczeństwa informacji i ustalenia w MSP dokumentu „Polityka Bezpieczeństwa ochrony danych osobowych w MSP".

z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.

W badanym okresie w MSP nie opracowano kompleksowej dokumentacji dotyczącej ochrony przetwarzania innych danych niż osobowe, w szczególności nie opracowano dokumentacji dotyczącej Systemu Zarządzania Bezpieczeństwem Informacji. W PBI nie sporządzono ewidencji informacji i danych oraz nie dokonano klasyfikacji informacji, w tym nie zidentyfikowano danych, których ochrona nie jest prawnie wymagana, a mogłyby one zostać wykorzystane przeciwko MSP poprzez ujawnienie, zablokowanie lub zmanipulowanie. W badanym okresie w MSP trwały natomiast prace nad wprowadzeniem Systemu Zarządzania Bezpieczeństwem Informacji, który miałby określać m.in.:

Rodzaj zadania:	Termin realizacji
Zakres i granice SZBI w MSP	30.06.2015 r.
Terminy i definicje	30.06.2015 r.
Politykę Bezpieczeństwa Informacji	30.09.2015 r.
Standardy bezpieczeństwa informacji	30.09.2015 r.
Procedury bezpieczeństwa informacji	30.09.2015 r.
Regulamin bezpieczeństwa informacji	30.09.2015 r.
Klasyfikacja i ochrona informacji w MSP	31.03.2016 r.
Zasady bezpieczeństwa informacji	31.03.2016 r.
Wykaz informacji przetwarzanych w MSP	31.03.2016 r.
Struktura zarządzania bezpieczeństwem informacji	31.03.2016 r.
Proces Zarządzania Bezpieczeństwem Informacji w MSP	31.03.2016 r.
Szacowanie ryzyka bezpieczeństwa informacji	31.03.2016 r.
Plan postępowania z ryzykiem	31.03.2016 r.

(dowód: akta kontroli Tom I str. 480, Tom II str. 2-5)

Dyrektor Generalny wyjaśnił: „*W wyniku realizacji umowy nr MSP/FSP/165-00/2013 z dnia 20.11.2013 r. na wykonanie usługi przeprowadzenia audytu bezpieczeństwa infrastruktury sieciowej, audytu obecnego stanu zarządzania bezpieczeństwem informacji oraz ustanowienia i wdrożenia Systemu Bezpieczeństwa Informacji (SZBI) w MSP, w 2014 r. została sporządzona ewidencja informacji i danych (klasyfikacja i wartościowanie) tworzonych, gromadzonych i przetwarzanych w MSP. Obecnie trwają prace Zespołu ds. wdrożenia SZBI w MSP, powołanego Zarządzeniem nr 14 Dyrektora Generalnego z dnia 11 maja 2015 r., które obejmują swoim zakresem m.in. aktualizację klasyfikacji i wartościowania danych przetwarzanych w komórkach organizacyjnych. Zgodnie z przyjętym harmonogramem prac Zespołu, aktualizacja ta powinna zostać zrealizowana do dnia 31 marca 2016 r.*"

(dowód: akta kontroli Tom II str. 1-16)

Zespół ds. wdrożenia SZBI zakończył opracowywanie projektów dokumentów: Standardy bezpieczeństwa informacji, Procedury bezpieczeństwa informacji oraz Regulamin bezpieczeństwa informacji. W dniu 23 września 2015 r. dokumenty te

zostały przekazane komórkom organizacyjnym MSP w celu zapoznania się i zgłoszenia ewentualnych uwag.

(dowód: akta kontroli Tom II str. 588)

W kwestii określenia zasad korzystania z technik kryptograficznych w celu ochrony poufności, integralności i autentyczności informacji przekazywanych elektronicznie Dyrektor Generalny MSW wyjaśnił, że: *„W celu ochrony poufności, integralności i autentyczności informacji przekazywanych elektronicznie, obowiązujący w MSP system Elektronicznego Zarządzania Dokumentacją (EZD) umożliwia opatrzenie dokumentów podpisem kwalifikowanym. W toku procesu wdrażania systemu, pracownicy posiadający certyfikat kwalifikowany zostali przeszkoleni z zasad posługiwania się nim. Dodatkowo MSP planuje rozbudowę systemu PKI, mającą na celu wprowadzenie mechanizmu zapewnienia integralności i autentyczności korespondencji elektronicznej wysyłanej via e-mail jako podpisanej przy użyciu niekwalifikowanych certyfikatów elektronicznych w standardzie X.509, wydawanych przez wewnętrzne centrum CA (Certification Authority) Ministerstwa. Uruchomienie systemu planowane jest na pierwsze półrocze 2016 r. Elementem wdrożenia będzie również opracowanie procedur bezpieczeństwa oraz zasad postępowania z tym systemem wraz z przygotowaniem instruktażu dla pracowników.*"

(dowód: akta kontroli Tom II str. 1,3,23-24)

Ustalone nieprawidłowości

Oceniając poziom zarządzania procesami zapewnienia bezpieczeństwa systemów teleinformatycznych z punktu widzenia stosowanego w metodyce CobiT 4.1 Modelu dojrzałości, biorąc pod uwagę minimalne wymagania dla systemów teleinformatycznych zawarte w rozporządzeniu KRI oraz dobre praktyki, w tym zalecenia zawarte w Polskich Normach w zakresie działań związanych z zapewnieniem warunków bezpieczeństwa systemów informatycznych, zdaniem NIK w Ministerstwie Skarbu Państwa, na dzień zakończenia kontroli, nie uwzględniono następujących elementów, systemu wymiany danych wrażliwych:

1) Klasyfikacja i ochrona informacji w MSP:

- brak jest wykazu informacji przetwarzanych w MSP oraz nie dokonano ich podziału na informacje chronione i jawne,
- informacje i dane znajdujące się w ewidencji formalnie nie zostały przypisane ich właścicielom, tj. właściwym komórkom organizacyjnym zgodnie z obowiązującą strukturą organizacyjną MSP,
- nie ustalono właścicieli informacji odpowiedzialnych za nadanie im odpowiedniej klauzuli poufności, analizę wymagań i określenie wymaganego zakresu ich ochrony,
- nie określono zasad oznaczania danych i informacji (poza informacjami niejawnymi lub podlegającymi innej ochronie prawnej np. danych wrażliwych, o których mowa w art. 27 uodo).

(dowód: akta kontroli Tom II str. str. 2-22, 587-589)

NIK ocenia jako nierzetelne nieprzypisanie informacjom odpowiedniego poziomu ochrony, zgodnego z ich wagą dla Ministerstwa. Na konieczność dokonania klasyfikacji informacji z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację, a także na konieczność

opracowania zbioru procedur oznaczania informacji wskazuje pkt. 8 normy PN-ISO/IEC 27005.

2) Standardy Bezpieczeństwa Informacji: nie określono zasad dotyczących typu i siły algorytmów kryptograficznych dla poszczególnych poziomów ochrony danych i informacji.

3) Szacowanie ryzyka związanego z bezpieczeństwem informacji: MSP nie dokonywało analiz konsekwencji dla systemu zabezpieczeń przed złośliwym oprogramowaniem oraz pobierania i wysyłania danych w postaci zaszyfrowanej.

(dowód: akta kontroli Tom II str. str. 2-22, 587-589)

Zalecenie określenia wymaganego poziomu ochrony, opartego na szacowaniu ryzyka oraz biorącego pod uwagę typ, siłę i jakość wymaganych algorytmów kryptograficznych ujęte jest w pkt. 10.1.1. normy PN-ISO/IEC 27005.

4) Regulamin Bezpieczeństwa Informacji: w badanym okresie w MSP poza danymi osobowymi, nie określono zasad przesyłania innych wrażliwych (chronionych) danych i informacji przez sieć publiczną.

(dowód: akta kontroli Tom II str. str. 2-22, 587-589)

Wytyczne dotyczące procedur i zabezpieczeń stosowanych w celu ochrony informacji przesyłanych przy użyciu wszystkich rodzajów środków łączności ujęto w pkt. 13.2 normy PN-ISO/IEC 27005.

Według wyjaśnień Dyrektora Generalnego MSP elementy te zostaną uwzględnione w procesie wdrażania Systemu Zarządzania Bezpieczeństwem Informacji.

(dowód: akta kontroli Tom II str. str. 2-22, 587-589)

W przypadku użycia nośników przeznaczonych do transportu, które zawierać będą dane wrażliwe, IT zaleca pracownikom aby były chronione przed nieuprawnionym dostępem poprzez ich zaszyfrowanie. Instalowane w standardowej konfiguracji oprogramowanie na wszystkich komputerach pracowników pozwala na wykonanie ww. czynności.

(dowód: akta kontroli Tom. III str. 164)

W ocenie NIK, brak zasad regulujących postępowanie w przypadku transportu danych wrażliwych oraz ograniczenie się wyłącznie do zalecenia ich szyfrowania nie gwarantuje, że dane te będą w pełni chronione przed nieuprawnionym dostępem. Wytyczne ochrony nośników zawierających informacje przed nieuprawnionym dostępem, nadużyciem oraz utratą integralności podczas transportu sformułowano w pkt. 8.3.3. normy PN-ISO/IEC 27005.

Ocena cząstkowa

W oparciu o stosowany w metodyce CobiT 4.1 Model dojrzałości, NIK ocenia poziom zarządzania procesem „zapewnienie bezpieczeństwa systemów informatycznych" w MSP jako „powtarzalne lecz intuicyjne". Chociaż systemy dostarczają informacji dotyczących bezpieczeństwa, dane te nie są analizowane. Bezpieczeństwo IT jest postrzegane głównie, jako przedmiot odpowiedzialności i domena działu IT. Na ocenę tę miały wpływ przede wszystkim nieprawidłowości związane z zapewnieniem rozliczalności sytemu ZSI oraz braku klasyfikacji danych wrażliwych innych niż dane osobowe. Zdaniem NIK nie jest to wystarczający i akceptowalny poziom zarządzania bezpieczeństwem w badanym obszarze.

IV. Uwagi i wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny i uwagi wynikające z ustaleń kontroli, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[16], wnosi o:

1. Kontynuowanie działań związanych z wdrożeniem w MSP Systemu Zarządzania Bezpieczeństwem Informacji, w szczególności w zakresie przyjęcia kompletnej i spójnej polityki bezpieczeństwa systemów informatycznych.
2. Zapewnienie pełnej rozliczalności Zintegrowanego Systemu Zarządzania db.
3. Prowadzenie jednego kompletnego rejestru incydentów.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

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 Prezesa Najwyższej Izby Kontroli.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK proszę o poinformowanie Najwyższej Izby Kontroli, w terminie 14 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag i 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.

Warszawa, dnia 17 grudnia 2015 r.

Prezes
Najwyższej Izby Kontroli
Krzysztof Kwiatkowski

.....
Podpis

[16] Dz. U. z 2015 r., poz. 1096.