PREZES
NAJWYŻSZEJ IZBY KONTROLI
Krzysztof Kwiatkowski

KPB – 410.004.02.2015
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. Katarzyna Kędzior-Rejner, główny specjalista kontroli państwowej, upoważnienie do kontroli nr 93504 z 9 czerwca 2015 r.
2. Katarzyna Kuzioła, inspektor kontroli państwowej, upoważnienie do kontroli nr 95756 z 9 czerwca 2015 r.
3. Adam Czugajewicz, specjalista kontroli państwowej, upoważnienie do kontroli nr 97713 z 28 września 2015 r.

Jednostka kontrolowana

Ministerstwo Spraw Wewnętrznych, ul. Batorego 5, 02-591 Warszawa, zwane w dalszej części niniejszego wystąpienia „MSW".

Kierownik jednostki kontrolowanej

Obecnie Ministrem Spraw Wewnętrznych i Administracji jest Mariusz Błaszczak, Ministrem Spraw Wewnętrznych od 22 września 2014 r. do końca okresu objętego kontrolą (od 1 stycznia 2014 r. do 1 października 2015 r.) była Teresa Piotrowska. Poprzednio, od 25 lutego 2013 r. Ministrem był Bartłomiej Sienkiewicz.

II. Ocena kontrolowanej działalności

Ocena ogólna

W oparciu o stosowany w metodyce CobiT 4.1 Model dojrzałości[1] NIK ocenia poziom zarządzania procesem „zapewnienie bezpieczeństwa systemów teleinformatycznych" w MSW jako „początkowy/doraźny".

W kontrolowanej jednostce istnieje świadomość potrzeby zapewnienia bezpieczeństwa teleinformatycznego, jednak jest ono zorganizowane w sposób nieskoordynowany, a zagadnienia bezpieczeństwa IT są rozproszone pomiędzy kilka komórek organizacyjnych i ciał, które odmiennie postrzegają swoją rolę, co prowadzi zarówno do luk kompetencyjnych, jak i zróżnicowanej oceny potencjalnych zagrożeń i braku jednoznacznego określenia podmiotów odpowiedzialnych za identyfikację tych zagrożeń i ich neutralizację.

Do zakończenia okresu objętego kontrolą (1 października 2015 r.) w MSW nie opracowano i nie wdrożono, zgodnego z powszechnie przyjętymi standardami, Systemu Zarządzania Bezpieczeństwem Informacji obejmującego politykę bezpieczeństwa informacji oraz plan zapewnienia bezpieczeństwa teleinformatycznego, zawierający uszeregowane hierarchicznie cele, pozwalające na osiągnięcia w określonym czasie oczekiwanych poziomów bezpieczeństwa informacji.

Działania dotyczące bezpieczeństwa IT albo nie zostały w sposób formalny określone w obowiązujących procedurach, albo były rozproszone w wielu odrębnych dokumentach.
Nie zidentyfikowano informacji istotnych dla realizowanych przez MSW zadań i nie określono wymaganych poziomów ochrony tych informacji (poza systemami wchodzącymi w skład infrastruktury krytycznej oraz ich komponentami chronionymi zgodnie z ustawą o ochronie

[1] 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.

informacji niejawnych). Nie dokonano oszacowania kosztów ewentualnego naruszenia bezpieczeństwa informacji. Nie wyznaczono formalnie komórki rekomendującej sposoby zapewnienia bezpieczeństwa IT. Nie określono jednolitej definicji incydentu bezpieczeństwa i procedur reagowania w przypadku jego wystąpienia.

Pomimo stosowania kaskadowego systemu antywirusowego stwierdzono liczne przypadki zawirusowania stacji roboczych, docierania do pracowników e-maili z odnośnikami do zagrożonych stron, przypadki nieaktualnego oprogramowania antywirusowego na stacjach roboczych lub jego brak, jak również 24 przypadki, w których komputery MSW były elementem sieci typu „botnet"[2].

Dla Centralnej Ewidencji Wydanych i Unieważnionych Dokumentów Paszportowych (dalej: CEWiUDP) przyjęto, związane z wymaganiami zapewnienia bezpieczeństwa, założenie, że system ten jest odseparowany od sieci publicznej. W świetle tego, że MSW nie posiada uprawnień i środków technicznych do zweryfikowania, czy stacje robocze użytkowników CEWiUDP faktycznie są odseparowane od tej sieci, jak też stwierdzenia przypadku utraty takiej separacji, założenie iż istnieje separacja jest w ocenie NIK nieuprawnione. Przestrzeganie przez użytkowników CEWiUDP zasad bezpieczeństwa systemu było poza nadzorem MSW. Logi systemowe CEWiUDP przechowywane były przez 30 dni, podczas gdy zgodnie z § 21 ust. 4 Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności[3] (dalej: KRI) powinny one być przechowywane przez 2 lata. Taśmy z kopią danych CEWiUDP nie były zabezpieczone kryptograficznie i przechowywane były w jednej lokalizacji.

Ustalenia i oceny NIK potwierdzają wyniki audytu wewnętrznego MSW w zakresie systemu zarządzania bezpieczeństwem informacji.

III. Opis ustalonego stanu faktycznego

1. Organizacja zarządzania procesem zapewnienia bezpieczeństwa systemów informatycznych MSW

Opis stanu faktycznego

W MSW zadania dotyczące działania systemów informatycznych leżały w gestii: Departamentu Teleinformatyki (dalej: DT), Departamentu Ewidencji Państwowych (dalej: DEP), Wydziału Informatyki i Łączności w Biurze Administracyjno-Finansowym (dalej: BAF) oraz Zespołu ds. Komunikacji Internetowej w Departamencie Komunikacji Społecznej (dalej: DKS).

Do zakresu działania **DT**, zgodnie z § 18b pkt 4 i 4a Regulaminu organizacyjnego MSW[4], należało m. in. prowadzenie spraw związanych z organizacją i koordynacją zadań w zakresie bezpieczeństwa teleinformatycznego i ochrony danych przekazywanych i przetwarzanych w sieciach i systemach teleinformatycznych MSW z uwzględnieniem KRI, w tym pełnienie funkcji Administratora Bezpieczeństwa Informacji, opracowanie i nadzorowanie planów ciągłości działania dla krytycznej infrastruktury teleinformatycznej, opracowanie i opiniowanie standardów i polityk bezpieczeństwa i innych dokumentów związanych z bezpieczeństwem informacji w MSW, prowadzenie spraw związanych z opracowaniem, ustanowieniem, wdrożeniem, eksploatowaniem, monitorowaniem, przeglądaniem oraz utrzymaniem i doskonaleniem[5] SZBI w MSW z uwzględnieniem KRI.

Dyrektor DT wyjaśnił, że w gestii DT leży bezpieczeństwo Systemu Rejestrów Państwowych, a informowanie pracowników MSW o zagrożeniach bezpieczeństwa teleinformatycznego leży w zakresie działania BAF.

---

[2] Sieć typu botnet - rodzaj złośliwego oprogramowania wytworzonego w celu przejmowania kontroli nad komputerami osobistymi i wykorzystywania ich do wykonywania założonych przez twórców celów np. kradzieży poufnych informacji, przeprowadzania ataków na inne systemy, propagacji infekcji złośliwym oprogramowaniem, rozsyłania niechcianej korespondencji itp.

[3] Rozporządzenie Rady Ministrów z 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 (Dz. U. poz. 526 ze zm.).

[4] Wprowadzonego zarządzeniem nr 4 Ministra Spraw Wewnętrznych z 9 grudnia 2011 r. (Dz. Urz. MSW Nr 1, poz. 3 ze zm.)

[5] Do 23 czerwca 2015 r. ww. przepis określał dla DT jedynie obowiązki związane z wdrożeniem i utrzymaniem SZBI. Pozostałe funkcje związane z SZBI zostały dodane do zakresu działania DT w wyniku realizacji zaleceń audytu wewnętrznego

Zgodnie z § 22 pkt 10 Regulaminu organizacyjnego MSW do zadań **BAF** należała m. in. obsługa komórek organizacyjnych Ministerstwa w zakresie informatyki i łączności, a w szczególności prowadzenie usług doraźnego serwisu technicznego sprzętu teleinformatycznego użytkowanego przez pracowników MSW oraz administratorski nadzór wewnętrznych sieci komputerowych, ich połączeń oraz opieka nad systemami informatycznymi w obiektach Ministerstwa, z wyłączeniem infrastruktury teleinformatycznej, będącej pod nadzorem Departamentu Teleinformatyki.

Dyrektor BAF wyjaśniła, że w gestii BAF leży bezpieczeństwo systemów zapewniających usługi sieci biurowej, serwerowej i klienckie, w tym kontrolery domeny serwery poczty, serwery plików, systemy elektronicznego obiegu dokumentów, serwery pomocnicze, oprogramowanie antywirusowe, kopie bezpieczeństwa, programy kadrowe, finansowo-księgowe. Z zakresu działania BAF wyłączona była infrastruktura sieciowa w budynku MSW przy ul. Pawińskiego w Warszawie.

W gestii **DKS** leżało bezpieczeństwo portalu internetowego i intranetowego MSW.

Do zadań **DEP** należał rozwój i obsługa systemów: Centralnej Ewidencji Wydanych i Unieważnionych Dokumentów Paszportowych, Systemu Rejestrów Państwowych (tj. rejestr PESEL, Rejestr Dowodów Osobistych, Rejestr Stanu Cywilnego, System Odznaczeń Państwowych i Centralny Rejestr Sprzeciwów) oraz Centralnej Ewidencji Pojazdów i Centralnej Ewidencji Kierowców. Zgodnie z Regulaminem organizacyjnym MSW do zakresu zadań DEP nie należały kwestie dotyczące bezpieczeństwa teleinformatycznego.

Do zakończenia okresu objętego kontrolą nie opracowano w MSW i nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji, Polityki Bezpieczeństwa Informacji i planu zapewnienia bezpieczeństwa IT.

(dowód: akta kontroli str. 238-264)

Nie wyznaczono uszeregowanych hierarchicznie celów dotyczących osiągnięcia w określonym czasie oczekiwanych poziomów bezpieczeństwa informacji. Nie wydzielono w planie finansowym MSW odrębnych środków finansowych na podnoszenie poziomu bezpieczeństwa informacji.

System bezpieczeństwa informacji budowany był siłami własnymi MSW.

Procesy związane z realizacją kluczowych zadań MSW zostały określone w kartach procesów operacyjnych, m.in.: „KPO-10/MSW - Prowadzenie rejestrów, ewidencji oraz przetwarzanie zbiorów danych", „KPO-11/MSW - Tworzenie, utrzymywanie i rozwój systemów informatycznych oraz komunikacji", „KPO-12/MSW - Nadzór nad utrzymaniem i rozwój infrastruktury". W kartach procesów nie określono zasobów niezbędnych do realizacji tych procesów.

Nie zidentyfikowano informacji istotnych dla realizowanych zadań. Nie określono wymaganych poziomów ochrony informacji, poza systemami wchodzącymi w skład infrastruktury krytycznej (systemy w gestii DEP), dla których poziom ochrony określono jako wysoki, oraz Centralnej Ewidencji Pojazdów Służbowych, chronionej na podstawie ustawy o ochronie informacji niejawnych[6]. Nie dokonano oszacowania kosztów ewentualnego naruszenia bezpieczeństwa informacji.

Nie było wyznaczonej komórki rekomendującej sposoby zapewnienia bezpieczeństwa IT. Funkcję tę pełniło BAF i zespół ds. bezpieczeństwa teleinformatycznego. Komórki MSW właściwe w sprawach IT odmiennie postrzegały istnienie procedur zgłaszania incydentów IT i komórki zobowiązanej do reakcji. W ocenie DEP procedura została opisana w polityce bezpieczeństwa, a incydenty zgłaszane były do DT. W ocenie DT i BAF procedura zgłaszania incydentów była w fazie projektu, a komórką zobowiązaną do reakcji był Zespół ds. bezpieczeństwa teleinformatycznego. Odmiennie postrzegana była przez komórki MSW również kwestia ciała lub zespołu służącego omawianiu i uzgadnianiu działań w zakresie bezpieczeństwa informacji. W ocenie DT był to Zespół ds. bezpieczeństwa teleinformatycznego. W ocenie administratorów systemów DEP funkcję taką pełnił

[6] Ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r., nr 182, poz. 1228)

Administrator Bezpieczeństwa Informacji. Nie istniała jedna komórka odpowiedzialna za zarządzanie bezpieczeństwem systemów teleinformatycznych. Zadanie to realizowane było przez Wydział Centrum Certyfikacji i Bezpieczeństwa Teleinformatycznego DT, Pełnomocnika ds. ochrony informacji niejawnych i Wydział Informatyki i Łączności BAF.

Kierownictwo MSW nie otrzymywało regularnych, okresowych raportów dotyczących stanu bezpieczeństwa informacji. W kontrolowanym okresie do kierownictwa MSW wpłynęło 10 pism dotyczących bezpośrednio lub pośrednio bezpieczeństwa informacji, opracowane przez DT, BAF i Administratora Bezpieczeństwa Informacji, w tym 4 sprawozdania okresowe dotyczące wybranych zagadnień związanych z bezpieczeństwem informacji i 1 notatką dotyczącą incydentu.

O bezpieczeństwie IT użytkownicy Systemu Rejestrów Państwowych informowani byli poprzez Politykę Bezpieczeństwa Systemu Rejestrów Państwowych, instrukcje użytkowania, a w przypadkach nagłych faksem i pocztą elektroniczną.

Szacowanie ryzyka w obszarze bezpieczeństwa IT, wynikające z wymagań Polityki Ochrony Cyberprzestrzeni RP, zostało przeprowadzone w 2014 r. na podstawie metodyki opracowanej przez Ministerstwo Administracji i Cyfryzacji.

Nie określono jednolitej definicji incydentu bezpieczeństwa i procedury reagowania. W okresie od 1 lutego 2014 r. do 6 lipca 2015 r. CERT.GOV.PL zarejestrował 55 incydentów dotyczących MSW, w tym 24 zidentyfikowanych jako „klient botnetu". W reakcji na powiadomienia w MSW dokonano w 24 przypadkach rekonfiguracji zagrożonego urządzenia, w 21 przypadkach – reinstalacji oprogramowania, a w 2 przypadkach – rekonfiguracji programu antyspamowego. W 8 przypadkach MSW nie było w stanie zidentyfikować incydentu i podać sposobu reakcji. Nie było możliwe uzyskanie przez MSW danych na temat tych incydentów z CERT ABW ze względu na brak w MSW numerów incydentów nadanych przez CERT ABW.

Nie był prowadzony rejestr incydentów zgłoszonych przez CERT. Pracownicy wyznaczeni do kontaktów z CERT przechowywali informacje o zagrożeniach i incydentach otrzymane z CERT w odrębnym folderze poczty elektronicznej.

Komórki MSW odpowiedzialne za kwestie IT odmiennie postrzegały kwestię istotności i poziomu bezpieczeństwa logów systemów teleinformatycznych. W ocenie DT i BAF logi te zawierają dane wrażliwe z punktu widzenia MSW, w związku z czym nie mogą być przekazane kontrolerowi na nośniku informatycznym, jednakże nie określono formalnie ich poziomu ochrony oraz wymaganych procedur zabezpieczenia. DEP nie czynił zastrzeżeń co do możliwości udostępnienia logów na nośniku informatycznym.

(dowód: akta kontroli str. 9-111, 131-392, 470-476, 490-501, 512-546)

Zgodnie z § 20 ust. 2 pkt 14 KRI zarządzanie bezpieczeństwem informacji realizowane jest m. in. poprzez zapewnienie nie rzadziej niż raz na rok okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji. W MSW w okresie od 4 listopada 2014 r. do 6 maja 2015 r. przeprowadzono audyt systemu zarządzania bezpieczeństwem informacji. Audytorzy stwierdzili m. in., że:

- pomimo wejścia w życie KRI z dniem 30 maja 2012 r. nie został w MSW wdrożony i utrzymywany system zarządzania bezpieczeństwem informacji (SZBI), co może skutkować utratą integralności, poufności i dostępności informacji w MSW, a w konsekwencji w MSW nie zarządza się bezpieczeństwem informacji w pełnym zakresie określonym w § 20 ust. 1 KRI;
- przez okres dwóch lat od wejścia w życie KRI nie została wskazana komórka organizacyjna odpowiedzialna za wdrożenie i utrzymanie SZBI;
- brak koncepcji w zakresie budowy i wdrażania SZBI
- w MSW funkcjonują niektóre elementy SZBI (np. polityki bezpieczeństwa informacji dla rejestrów państwowych, system kontroli dostępu), jednak szereg luk może wpływać na bezpieczeństwo informacji w MSW, np. brak spójnej wiedzy o wszystkich funkcjonujących w MSW systemach i zabezpieczeniach, nieaktualne oprogramowanie,

brak wiedzy i świadomości pracowników w zakresie incydentów informatycznych, brak polityki bezpieczeństwa informacji i innych procedur regulujących te zagadnienia (polityka czystego biurka, czystego ekranu, telepracy, itp.);
- brak analizy ryzyka utraty integralności, dostępności i poufności informacji;
- pracownicy MSW nie mają wiedzy i świadomości, czym jest incydent lub zdarzenie informatyczne;
- brak polityki postępowania z incydentami i zdarzeniami informatycznymi;
- projekt „Algorytmów komunikacji i działań na wypadek wystąpienia incydentów teleinformatycznych" jest niespójny z projektem „Procedury postępowania w przypadku wystąpienia incydentu informatycznego" oraz nie uwzględnia faktu, że członkowie Zespołu ds. Bezpieczeństwa Teleinformatycznego pracują tylko na jedną zmianę.

Zespół audytowy sformułował 15 zaleceń, które zostały zrealizowane w następujący sposób:

1. Udokumentowana analiza zasobów osobowych, kompetencji, uwarunkowań organizacyjno-funkcjonalnych niezbędnych do wdrożenia i utrzymywania SZBI – wykonano. **Jeden z wniosków analizy rekomenduje powołanie komórki organizacyjnej w zakresie bezpieczeństwa teleinformatycznego i cyberprzestrzeni na odpowiednio wysokim poziomie usytuowania w strukturze MSW, której kompetencje dotyczyłyby wszystkich komórek organizacyjnych;**
2. Analiza zasadności zwiększenia zasobu kadrowego Wydziału Centrum Certyfikacji i Bezpieczeństwa Teleinformatycznego DT – obsadzono stanowisko zastępcy dyrektora DT i 2 wakaty pracowników DT oraz skierowano na szkolenia 20 pracowników;
3. Wskazanie odpowiedzialnego za opracowanie, ustanowienie, eksploatację, monitorowanie i przeglądanie oraz doskonalenie SZBI – zadanie powierzono DT w wyniku zmiany regulaminu organizacyjnego MSW i wewnętrznego regulaminu DT;
4. Udokumentowana analiza i oszacowanie wydatków niezbędnych do wdrożenia i utrzymywania SZBI – zadanie planowane do realizacji. Przeprowadzono szacowanie kosztów realizacji zadań z zakresu ochrony cyberprzestrzeni w latach 2013-2015;
5. Określenie i zatwierdzenie harmonogramu wdrożenia kolejnych elementów SZBI - wykonane;
6. Szczegółowe określenie ról Wydziału Centrum Certyfikacji i Bezpieczeństwa Teleinformatycznego (dalej: WCC) DT i Zespołu ds. Bezpieczeństwa Teleinformatycznego (dalej: Zespół) w celu uniknięcia dublowania pracy oraz skutecznej realizacji zadań i wskazania osób odpowiedzialnych za realizację poszczególnych zadań – wykonano;
7. Zmiana decyzji w sprawie powołania Zespołu w celu określenia zasad nadzoru nad pracą Zespołu – nie wykonano. W ocenie Dyrektora Generalnego MSW zmiana ww. decyzji nie prowadziłaby do wyraźniej zmiany jakościowej prac Zespołu i nie miałby zasadniczego wpływu na zakres i sposób realizacji zadań Zespołu;
8. Uaktualnienie zakresów czynności pracowników WCC – wykonano;
9. Określenie indywidualnych programów rozwoju zawodowego pracowników WCC - wykonano;
10. Przegląd aktów prawnych w celu przygotowania podstaw do wdrożenia SZBI – wykonano;
11. Opracowanie szczegółowej koncepcji SZBI – wykonano;
12. Udokumentowanie sposobu monitorowania przez kierownictwo DT wdrażania SZBI - wykonano;
13. Określenie harmonogramu pracy Zespołu ds. Bezpieczeństwa Teleinformatycznego i dokonanie przeglądu dokumentów opracowywanych przez Zespół – wykonano;
14. Analiza stosowanego oprogramowania po kątem użytkowania systemu Windows XP i wymiany oprogramowania niewspieranego na aktualne – wymieniono część stacji

roboczych na stacje z nowym oprogramowaniem, pozostało ok. 450 stacji z systemem Windows XP;

15. Uporządkowanie i oznaczenie okablowania – uporządkowano okablowanie, odstąpiono od jego oznakowania.

(dowód: akta kontroli str. 9-44, 131-237)

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 MSW:

- Brak Systemu Zarządzania Bezpieczeństwem Informacji, brak polityki bezpieczeństwa informacji, brak planu zapewnienia bezpieczeństwa IT, brak skoordynowania ról i spory kompetencyjne pomiędzy komórkami MSW w zakresie bezpieczeństwa IT, co NIK ocenia jako działanie nierzetelne i wskazujące 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.
- Brak definicji incydentu i jednolitej procedury reagowania oraz jednoznacznego wskazania komórki odpowiedzialnej za reakcję, co 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 z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.
- Brak określenia uszeregowanych hierarchicznie celów dotyczących osiągnięcia w określonym czasie oczekiwanych poziomów bezpieczeństwa informacji i brak wydzielenia w planie finansowym odrębnych środków finansowych na podnoszenie poziomu bezpieczeństwa informacji. Norma PN-ISO/IEC 27001, w pkt. 5.1 i 5.2 zaleca kierownictwu jednostki między innymi określenie celów i zasad kierowania działaniami związanymi z bezpieczeństwem informacji oraz zabezpieczenie niezbędnych do tego zasobów. W ocenie NIK powyższe wskazuje na wysoki poziom ryzyka w zakresie zapewniania poufności, dostępności i integralności informacji w zarzadzaniu bezpieczeństwem informacji.
- Brak identyfikacji informacji istotnych dla realizowanych zadań. W ocenie NIK zdefiniowanie tych informacji jest niezbędne do adekwatnego określenia poziomów ich ochrony oraz opracowania planu zachowania ciągłości działania, którego zasadniczym elementem zalecanym w pkt 5.11 normy PN-ISO/IEC 24762 jest ustalenie priorytetów organizacji, ram czasowych, wymagań dotyczących odtworzenia po katastrofie.
- Nie określono wymaganych poziomów ochrony informacji w stosunku do wszystkich użytkowanych systemów, jak też nie oszacowano kosztów ewentualnego naruszenia bezpieczeństwa informacji, co w ocenie NIK jest jednym z elementów niezbędnych do określenia wymaganego poziomu ochrony. Norma PN-ISO/IEC 27002 w pkt. 8.2.1 zaleca, aby informacje były klasyfikowane z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację.
- Brak wyznaczenia komórki rekomendującej sposoby zapewnienia bezpieczeństwa IT, co w ocenie NIK powoduje luki i wątpliwości kompetencyjne w tym zakresie, a także brak regularnego raportowania kierownictwu MSW o stanie bezpieczeństwa informacji. Wskazuje to na nierzetelne ustanowienie struktury zarządzania mającej na celu zainicjowanie bezpieczeństwa informacji w Ministerstwie. Zalecenie określenia i przypisania

odpowiedzialności za bezpieczeństwo informacji zostało sformułowane w pkt. 6.1.1 Normy PN-ISO/IEC 27002.

- Brak procedury zgłoszeń incydentów i rzetelnego ich rejestru (odnotowywano jedynie zgłoszenia z CERT.GOV.PL), co nie pozwalało na rzetelną realizację działań zalecanych w pkt. 16.1.1 normy PN-ISO/IEC 27002, tj. określenia procedur związanych z odnotowywaniem działań związanych z incydentami bezpieczeństwa.
- Nie stworzono wykazu aktywów definiującego adekwatne poziomy ochrony dla poszczególnych rodzajów informacji, co stało się przyczyną rozbieżnego podejścia poszczególnych komórek MSW co do sposobu udostępnienia informacji zawartych w logach systemowych. Na potrzebę dokonania wartościowania aktywów wskazuje pkt B.1.1 normy PN-ISO/IEC 27005 i pkt 8.1.1 norny PN-ISO/IEC 27002.

Ocena cząstkowa

NIK ocenia - w oparciu o stosowany w metodyce CobiT 4.1 Model dojrzałości - poziom zarządzania procesem bezpieczeństwa systemów teleinformatycznych jako „początkowy/doraźny", tj. MSW dostrzega potrzebę zapewnienia bezpieczeństwa IT, jednakże jest ono zapewniane na doraźnych zasadach, zależy głównie od pojedynczych osób i nie podlega pomiarowi. Zdaniem NIK nie jest to wystarczający i akceptowalny poziom zarządzania bezpieczeństwem w badanym obszarze.

2. Bezpieczeństwo teleinformatyczne Centralnej Ewidencji Wydanych i Unieważnionych Dokumentów Paszportowych

Opis stanu faktycznego

Rozwój i obsługa CEWiUDP leżały w gestii DEP. W ocenie DEP kwestie bezpieczeństwa CEWiUDP należały co do zasady do zakresu zadań DT.

Dyrektor DT wyjaśnił, że DT utrzymuje techniczne działanie CEWiUDP, a za kwestie bezpieczeństwa danych odpowiada DEP. W odniesieniu do CEWiUDP, DT nie weryfikował prawidłowości działania, nie analizował nieskutecznych incydentów naruszenia bezpieczeństwa, nie prowadził cyklicznej kontroli bezpieczeństw i nie prowadził testów bezpieczeństwa CEWiUDP.

Prawidłowość wyników działania CEWiUDP przewidywała umowa utrzymaniowa z Centralnym Ośrodkiem Informatyki. Monitorowanie zgodności nie miało charakteru zautomatyzowanego. Nie stwierdzono przypadku naruszenia bezpieczeństwa CEWiUDP. Nie określono w sposób formalny obowiązku prowadzenia cyklicznej kontroli bezpieczeństwa CEWiUDP, obejmującej przestrzeganie polityki haseł, skuteczności zarządzania tożsamością, skuteczności zarządzania kontami użytkowników, niezmienności parametrów systemu istotnych dla bezpieczeństwa i niezmienności parametrów sieci istotnych dla bezpieczeństwa.

Użytkownikom zewnętrznym CEWiUDP uprawnionym do dostępu DEP wydawał certyfikaty do komunikacji danego punktu paszportowego z rejestrem CEWiUDP, zakładał konto użytkownika oraz nadawał login i hasło. Zmiana hasła nie była wymuszana. Dalszą obsługę zapewniało Centrum Personalizacji Dokumentów.

MSW nie było w posiadaniu wykazu aktywów CEWiUDP. Zasady zabezpieczeń kryptograficznych CEWiUDP zostały określone w Polityce Certyfikacji dla CEWiUDP.

W MSW przyjęto założenie, że CEWiUDP jest odseparowany od sieci publicznej. ABW stwierdziła jednak przypadek korzystania przez użytkownika Systemu Rejestrów Państwowych ze stacji podłączonej do sieci publicznej. Brak było możliwości zautomatyzowanego wykrywania przypadków braku separacji użytkownika systemów ewidencji i rejestrów od sieci publicznej. Dyrektor DEP wyjaśnił, że za bezpieczeństwo lokalnej infrastruktury sieciowej wykorzystywanej przez użytkowników do łączenia się z CEWiUDP odpowiadają ich lokalni administratorzy.

Rozliczalność CEWiUDP zapewniana była na podstawie logów aplikacyjnych zawierających datę, godzinę, nazwę użytkownika i dokonaną czynność. Dane, o których mowa w § 21 KRI, przechowywane były przez 30 dni.

W wyniku przeglądu aktualności danych użytkowników CEWiUDP w MSW stwierdzono dwa przypadki niewyrejestrowania nieaktywnych użytkowników, spowodowane brakiem zgłoszenia o cofnięciu upoważnienia do dostępu.

Rozdział uprawnień administracyjnych administratorów CEWiUDP dokonany był w opisach stanowisk.

Taśmy z kopiami danych CEWiUDP nie były zabezpieczone kryptograficznie. Były one przechowywane w jednej lokalizacji.

(dowód: akta kontroli str. 238-276, 283-284, 291, 467-469)

Ustalone nieprawidłowości

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

- Powstała rozbieżność opinii pomiędzy komórkami MSW co do zakresu odpowiedzialności za bezpieczeństwo CEWiUDP, co w ocenie NIK wskazuje na nieprawidłową organizację procesu bezpieczeństwa. Zgodnie z zaleceniem pkt. 6.1.2 normy PN-ISO/IEC 27002 obowiązki i odpowiedzialności pozostające w konflikcie ze sobą należy rozdzielić.
- Kopia danych CEWiUDP nie była zabezpieczana kryptograficznie, co było niezgodne z § 5 ust. 2b Polityki Bezpieczeństwa Zbioru Danych Osobowych CEWiUDP. Zalecenie takiego szyfrowania kopii zapasowych zawierających niektóre dane sformułowane jest w pkt. 12.3.1 normy PN-ISO/IEC 27002.
- Nie sporządzano drugiej kopii danych, która byłaby przechowywana w innej lokalizacji. W ocenie NIK działanie MSW nie zapewniało wystarczającej ochrony przed utratą danych. Zalecenie, aby kopia zapasowa danych była przechowywana w innej lokalizacji, w odległości pozwalającej uniknąć uszkodzenia spowodowane katastrofą, która dotknęła ośrodek podstawowy jest zawarte w pkt. 12.3.1 normy PN-ISO/IEC 27002.
- Zasady bezpieczeństwa CEWiUDP oparto na założeniu całkowitej separacji sieci systemu od sieci publicznej, w sytuacji braku realnych możliwości weryfikacji tej separacji, w sytuacji scedowania kwestii bezpieczeństwa i prawidłowości działania CEWiUDP na podmioty zewnętrzne przy jednoczesnym braku aktywnego nadzoru nad bezpieczeństwem tego systemu oraz stwierdzonego przypadku utraty takiej separacji.
- Przechowywanie danych wskazanych w § 21 ust. 1-3 KRI tj. informacji w dziennikach systemów przez 30 dni, podczas gdy okres ten powinien wynosić 2 lata, co zdaniem NIK jest niezgodne z § 21 ust. 4 KRI

(dowód: akta kontroli str. 238-276, 283-284, 291, 467-469)

Ocena cząstkowa

NIK ocenia - w oparciu o stosowany w metodyce CobiT 4.1 Model dojrzałości - poziom zarządzania procesem bezpieczeństwa systemu CEWiUP jako „nieistniejący", tj. organizacja nie dostrzega potrzeby zapewnienia bezpieczeństwa. Podstawowym powodem zastosowania powyższej oceny jest nieuprawnione - zdaniem NIK – założenie uzyskania oczekiwanego poziomu bezpieczeństwa jedynie dzięki całkowitej separacji sieci systemu od sieci publicznej i zapewnieniu dostatecznego bezpieczeństwa systemu przez podmioty zewnętrzne, odpowiedzialne za obsługę i użytkowanie CEWiUDP. Zdaniem NIK nie jest to wystarczający i akceptowalny poziom zarządzania bezpieczeństwem w badanym obszarze.

3. Bezpieczeństwo teleinformatyczne pozostałych systemów obsługujących ewidencje i rejestry będące w gestii MSW

Opis stanu faktycznego

W ocenie DEP i DT w MSW ustanowienie polityki zapobiegania złośliwemu oprogramowaniu, wykrywanie złośliwego oprogramowania i nadzorowanie aktualizacji oprogramowania

antywirusowego leżało w gestii BAF. W ocenie BAF do zakresu działania BAF nie należała nadzorowana przez DT infrastruktura sieciowa przy ul. Pawińskiego, obejmująca System Rejestrów Państwowych i Centralną Ewidencję Pojazdów i Kierowców.
Dokumentem regulującym kwestie bezpieczeństwa IT była Polityka Bezpieczeństwa Systemu Rejestrów Państwowych.

Dyrektor DT wyjaśnił, że przypadki zautomatyzowanego wykrycia i usunięcia szkodliwego oprogramowania są raportowane poprzez działanie programu Orion Solarwind. Logi programu są analizowane codziennie przez wyznaczonego pracownika. Obowiązek ten nie został uregulowany w formie procedury, ale został wpisany do zakresu obowiązków pracownika. W kontrolowanym okresie nie stwierdzono prób lub przypadków włamań do sieci w gestii DT, natomiast stwierdzono jeden przypadek zainfekowania komputera złośliwym oprogramowaniem.

Użytkownicy Systemu Rejestrów Państwowych i Centralnej Ewidencji Pojazdów i Kierowców zobowiązani byli do przestrzegania wymagań i zaleceń bezpieczeństwa określonych dla tych rejestrów i ewidencji, natomiast MSW nie weryfikowało przestrzegania tych wymogów ze względu na brak uprawnień.

W MSW nie była prowadzona ewidencja aktywów wspierających dotycząca infrastruktury sieciowej. Nie określono zadań i procedur dotyczących zarządzania sprzętem sieciowym. Odpowiedzialność personalną za funkcjonowanie sieci od odpowiedzialności za funkcjonowanie systemów oddzielono poprzez wyodrębnienie w DT Wydziału Utrzymania Sieci i Wydziału Utrzymania Systemów Teleinformatycznych.

Wytyczne dotyczące zarządzania istotnymi dla bezpieczeństwa elementami sieci były określone w dokumentach stworzonych na potrzeby infrastruktury krytycznej, które były przeglądane i aktualizowane w okresach 3-6 miesięcznych.

Określono politykę haseł administracyjnych dla urządzeń infrastruktury sieciowej.

Fizyczny dostęp do istotnych dla bezpieczeństwa elementów systemów sieciowych został ograniczony m. in. poprzez kontrolę dostępu, ograniczenie liczby osób uprawnionych do wejścia i rozliczalność wejść. Elementy sieci objęte były zarządzaniem konfiguracją.

Krytyczne dla MSW obszary sieci były monitorowane w zakresie bezpieczeństwa, jednak działania te nie zostały w sposób formalny opisane w zatwierdzonym dokumencie.

(dowód: akta kontroli str. 112-130, 244-262, 277-282, 466, 488-489)

Ustalone nieprawidłowości

Oceniając poziom zarządzania procesami zapewnienia bezpieczeństwa pozostałych systemów obsługujących ewidencje i rejestry będące w gestii MSW z punktu widzenia stosowanego w metodyce CobiT 4.1 Modelu dojrzałości oraz biorąc pod uwagę minimalne wymagania dla systemów teleinformatycznych zawarte w rozporządzeniu KRI i dobre praktyki, w tym zalecenia zawarte w Polskich Normach w zakresie działań związanych z zapewnieniem warunków bezpieczeństwa systemów informatycznych, zdaniem NIK, w MSW:

- Brak formalnego określenia zadań i procedur dotyczących zarządzania infrastrukturą sieciową, co wskazuje w ocenie NIK na brak rzetelnego zarządzania i nadzorowania siecią pozwalającego na właściwą ochronę przesyłanych nią informacji. Wytyczne ustanowienia procedur w zakresie zarządzania wyposażeniem sieciowym sformułowano w pkt. 13.1.1 normy PN-ISO/IEC 27002.
- Brak ewidencji aktywów wspierających dotyczących infrastruktury sieciowej, co wskazuje w ocenie NIK na nierzetelne zidentyfikowanie aktywów. Zdaniem NIK wiedza ta jest istotna z punktu widzenia dążenia do zapewnienia odpowiedniego poziomu bezpieczeństwa. Na potrzebę zidentyfikowania aktywów organizacji, obejmujących m. in. wszelkie urządzenia telekomunikacyjne używane do połączenia wielu fizycznie oddalonych komputerów wskazuje również pkt. B1 normy PN-ISO/IEC 27005.
- Istnieją rozbieżności pomiędzy komórkami MSW co do zakresu odpowiedzialności za wykrywanie złośliwego oprogramowania w odniesieniu do sieci dotyczących Systemu Rejestrów Państwowych i Centralnej Ewidencji Pojazdów i Kierowców, co wskazuje, w ocenie NIK, na nierzetelne określenie i ustanowienie odpowiedzialności za

bezpieczeństwo informacji. Na konieczność wyznaczenia podmiotów odpowiedzialnych za poszczególne procesy bezpieczeństwa informacji wskazuje również pkt. 6.1.1 normy PN-ISO/IEC 27002.

Ocena cząstkowa

NIK ocenia - w oparciu o stosowany w metodyce CobiT 4.1 Model dojrzałości - poziom zarządzania procesem bezpieczeństwa systemów obsługujących ewidencje i rejestry będące w gestii MSW jako „początkowy/doraźny", tj. organizacja dostrzega potrzebę zapewnienia bezpieczeństwa IT, jednakże jest ono zapewniane na doraźnych zasadach, zależy głównie od pojedynczych osób i nie podlega pomiarowi. Na ocenę tę miały wpływ nieprawidłowości związane z całokształtem funkcjonowania MSW w zakresie zapewnienia warunków bezpieczeństwa systemów informatycznych. Zdaniem NIK nie jest to wystarczający i akceptowalny poziom zarządzania w badanym obszarze.

4. Bezpieczeństwo pozostałych systemów teleinformatycznych wykorzystywanych w MSW

Opis stanu faktycznego

Bezpieczeństwo wykorzystywanych w MSW systemów teleinformatycznych innych niż CEWiUDP, System Rejestrów Państwowych, Centralna Ewidencja Pojazdów i Kierowców oraz portalu internetowego i intranetowego MSW leżało w gestii BAF (Wydziału Informatyki i Łączności). Do systemów będących w gestii BAF należały m. in. systemy usług biurowych, sieci serwerowej, serwery poczty i plików, systemy elektronicznego obiegu dokumentów, serwery pomocnicze, programy kadrowe i finansowo-księgowe, oprogramowanie antywirusowe.

Dokumentami dotyczącymi bezpieczeństwa IT były zarządzenia dyrektora generalnego: nr 28 w sprawie zasad przyznawania i korzystania ze służbowych urządzeń telekomunikacyjnych oraz rozliczania bezprzewodowych usług w zakresie połączeń głosowych i transmisji danych w MSW z 14 lipca 2014 r. oraz nr 1 w sprawie gospodarowania sprzętem informatycznym i łączności oraz zasad użytkowania tego sprzętu w komórkach organizacyjnych MSWiA z 14 stycznia 2009 r. Oba zarządzenia kwestie bezpieczeństwa IT regulowały w sposób marginalny.

Nie została w sposób formalny określona polityka zapobiegania złośliwemu oprogramowaniu. Polityka ta ma być zawarta w projektowanej Polityce Bezpieczeństwa Informacji.

W MSW funkcjonował kaskadowy system antywirusowy wybrany w drodze zamówienia publicznego, którego kryteria określili administratorzy BAF. Oprogramowanie było aktualizowane za pomocą centralnego systemu dystrybucji. Urządzenia mobilne pobierały aktualizacje automatycznie.

(dowód: akta kontroli str. 256-262)

W kontrolowanym okresie wystąpiły przypadki braku oprogramowania antywirusowego na stacjach roboczych pracowników MSW lub nieaktualność takiego oprogramowania. Z komunikatów BAF z lipca 2015 r. wynikało, że stwierdzono liczne przypadki zawirusowania komputerów z dostępem do internetu oraz otrzymywania e-maili zawierających wirusy, które jako podejrzane wiadomości zgłosili pracownicy MSW do Wydziału Informatyki i Łączności BAF.

Wykrycie i usunięcie szkodliwego oprogramowania były raportowane w odniesieniu do urządzeń, na których zainstalowany był program antywirusowy. Raporty były analizowane przez administratorów systemów.

Określenie zadań i procedur dotyczących zarządzania sprzętem sieciowym odbyło się poprzez zawarcie zadań związanych w zarządzaniem infrastrukturą sieciową w opisach stanowisk. Odpowiedzialność personalną za funkcjonowanie sieci od odpowiedzialności za funkcjonowanie systemów oddzielono poprzez określenie zadań w zakresach obowiązków pracowników.

Istotne dla bezpieczeństwa elementy sieci objęte były nadzorem zbierania logów systemowych za pomocą oprogramowania SIEM. Nie określono wytycznych dotyczących zarządzania istotnymi dla bezpieczeństwa elementami sieci. Polityka haseł administracyjnych

dla infrastruktury sieciowej była tożsama z polityką haseł serwerowych, określoną w „Zasadach korzystania z systemu teleinformatycznego MSWiA".

Fizyczny dostęp do istotnych dla bezpieczeństwa elementów systemów sieciowych został ograniczony poprzez umiejscowienie urządzeń sieciowych w wydzielonych pomieszczeniach zamykanych na zamek lub zabezpieczonych systemem kontroli dostępu. Elementy sieci objęte były zarządzaniem konfiguracją poprzez centralny system zarządzania urządzeniami sieciowymi.

Bezpieczeństwo systemów mobilnych zapewniane było poprzez wgrywanie przez administratora aplikacji nadzorującej zabezpieczenie za pomocą certyfikatów.

Za dokument polityki szczegółowej dotyczący zasad wykorzystywania urządzeń mobilnych przyjęto w MSW zarządzenie dyrektora generalnego nr 28 w sprawie zasad przyznawania i korzystania ze służbowych urządzeń telekomunikacyjnych oraz rozliczania bezprzewodowych usług w zakresie połączeń głosowych i transmisji danych w MSW z 14 lipca 2014 r., które nie regulowało kwestii bezpieczeństwa IT.

Krytyczne dla MSW obszary sieci były rutynowo monitorowane w zakresie bezpieczeństwa za pomocą oprogramowania typu SIEM.

Logi systemowe, antywirusowe i programu pocztowego były przeglądane codziennie przez administratorów, jednak obowiązek taki nie został sformalizowany. Logi systemu antywirusowego przechowywane były przez 1 miesiąc.

Nie określono w sposób formalny zasad bezpiecznego administrowania serwisem internetowym i intranetowym. Stacje robocze w budynku MSW przy ul. Batorego w Warszawie posiadały jednoczesny dostęp do zasobów MSW i internetu. Oba zasoby były odseparowane za pomocą kaskadowego systemu zabezpieczeń, składającego się z urządzeń typu firewall i oprogramowania. W budynku MSW przy ul. Pawińskiego w Warszawie zasoby te były fizycznie odseparowane.

Jako potrzeby w zakresie bezpieczeństwa IT, w tym wymagające modernizacji i usunięcia luk, BAF zidentyfikował: wymianę systemów Windows XP i Windows 2003 oraz pakietu MS Office 2003 na wyższą wersję, wymianę przełączników dostępowych, wymianę lub rozbudowę macierzy dyskowej do przechowywania plików, modernizację systemu zasilania awaryjnego dla infrastruktury IT i modernizację lub budowę nowej serwerowni.

(dowód: akta kontroli str. 238-264, 369-465, 470-481, 490-501)

Ustalone nieprawidłowości

W MSW stosowane były w praktyce niezatwierdzone zasady i procedury bezpieczeństwa IT, ponieważ kierownictwo nie dostrzegało potrzeby sformalizowania tych zasad. Prace w tym zakresie podjęto po zakończeniu audytu wewnętrznego. Zdaniem NIK, oceniając poziom zarządzania procesami zapewnienia bezpieczeństwa pozostałych systemów teleinformatycznych będących w gestii MSW z punktu widzenia stosowanego w metodyce CobiT 4.1 Modelu dojrzałości oraz biorąc pod uwagę minimalne wymagania dla systemów teleinformatycznych zawarte w rozporządzeniu KRI i dobre praktyki, w tym zalecenia zawarte w Polskich Normach, wskazać należy, że kierownictwo Ministerstwa w niedostatecznym stopniu zapewniało wytyczne i wsparcie dla działań na rzecz bezpieczeństwa informacji. Zalecenie, aby zbiór polityk bezpieczeństwa informacji został określony, zatwierdzony przez kierownictwo instytucji, opublikowany i zakomunikowany pracownikom i stronom zewnętrznym sformułowane jest w pkt. 5.1.1 normy PN-ISO/IEC 27002.

Ocena cząstkowa

NIK ocenia - w oparciu o stosowany w metodyce CobiT 4.1 Model dojrzałości - poziom zarządzania procesem bezpieczeństwa pozostałych systemów teleinformatycznych będących w gestii MSW jako „początkowy/doraźny", tj. organizacja dostrzega potrzebę zapewnienia bezpieczeństwa IT, jednakże jest ono zapewniane na doraźnych zasadach, zależy głównie od pojedynczych osób i nie podlega pomiarowi. Na ocenę tę miały wpływ nieprawidłowości związane z całokształtem funkcjonowania MSW w zakresie zapewnienia warunków bezpieczeństwa systemów informatycznych. Zdaniem NIK nie jest to wystarczający i akceptowalny poziom zarządzania w badanym obszarze.

Wnioski pokontrolne

IV. Uwagi i wnioski

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[7], wnosi o:

1. wprowadzenie zmian w organizacji MSW, w celu powierzenia całości zadań z zakresu bezpieczeństwa IT i odpowiedzialności za ich realizowanie jednej komórce;
2. opracowanie i wdrożenie, zgodnego z powszechnie przyjętymi standardami, Systemu Zarządzania Bezpieczeństwem Informacji.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach: jeden dla Pana Ministra, drugi do akt kontroli.

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK, przysługuje Panu Ministrowi 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, 9 grudnia 2015 r.

Prezes

Najwyższej Izby Kontroli

Krzysztof Kwiatkowski

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