PREZES
NAJWYŻSZEJ IZBY KONTROLI
Krzysztof Kwiatkowski

KPB – 410.004.01.2015
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
Kontroler	Rafał Komorowski na podstawie upoważnienia nr 93494 z dnia 29 maja 2015 r. (dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Kasa Rolniczego Ubezpieczenia Społecznego Warszawa, ul. Niepodległości 190
Kierownik jednostki kontrolowanej	Artur Brzóska – Prezes Kasy Rolniczego Ubezpieczenia Społecznego od 5 stycznia 2012 r.
Okres objęty kontrolą	Od 1 stycznia 2014 do 23 października 2015 r.

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 informatycznych" w KRUS jako „zdefiniowany".

W kontrolowanej jednostce wprowadzono system bezpieczeństwa informacji w ramach Zintegrowanego Systemu Zarządzania, co zdaniem NIK świadczy o tym, że kierownictwo KRUS jest świadome potrzeby zapewnienia bezpieczeństwa. W ocenie Izby wdrożony system wymaga jednak poprawy i udoskonalenia.

W ramach ustalonego systemu zdefiniowano główne procedury bezpieczeństwa i – w ocenie NIK - są one wzajemnie kompatybilne, niemniej jednak NIK zauważyła, że opracowane procedury nie były w pełni czytelne i przejrzyste oraz stwierdziła brak niektórych procedur regulujących szczegółowe obszary bezpieczeństwa.

Zdaniem Izby przyjęta koncepcja powierzenia zasobów KRUS wykonawcy zewnętrznemu, może świadczyć o braku systemowego podejścia do zarządzania bezpieczeństwem informacji w szczególności w odniesieniu do systemów podstawowych dla realizacji ustawowych zadań KRUS. Dlatego też w ocenie NIK istnieje wysokie ryzyko, że usługi świadczone przez podmioty zewnętrzne mogą nie spełniać opracowanych w kontrolowanej jednostce wymagań dotyczących bezpieczeństwa.

W ustalonym systemie określono zasady oceny procedur i ich aktualizacji a proces zapewnienia bezpieczeństwa był monitorowany przez okresowe audyty. Stworzono system zbierania i analizy incydentów, jednak zdaniem NIK był on niekompletny.

W obszarze zarządzania kontami użytkowników systemu informatycznego objętego kontrolą stwierdzono nieprawidłowości, które w ocenie Izby obniżają jego bezpieczeństwo.

W trakcie kontroli podjęto działania zmierzające do systemowego usunięcia tych nieprawidłowości.

[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.

III. Opis ustalonego stanu faktycznego

1. Zarządzanie bezpieczeństwem IT, podstawowe dokumenty związane z bezpieczeństwem informacji

1.1 Podstawowe systemy funkcjonujące w KRUS oraz sposób zarządzania nimi

Opis stanu faktycznego

Najważniejsze systemy informatyczne służące statutowej działalności KRUS funkcjonujące w okresie objętym kontrolą to:

- FARMER – system emerytalno-rentowy zarządzany w modelu pełnego outsourcingu (zarówno usługi jak i infrastruktura została powierzona wykonawcy zewnętrznemu).
- nSiu[2] – system służący do obsługi ubezpieczenia społecznego rolników oraz świadczeń krótkoterminowych zarządzany w modelu pełnego outsourcingu.
- Kachna – system służący do obsługi ubezpieczeń zdrowotnych. System jest zarządzany przez KRUS.

Objęty badaniem system FARMER powstał w 2004 r. Jest on utrzymywany i administrowany w ośrodkach obliczeniowych wykonawcy (firmy Zeto i Unizeto), natomiast pracownicy KRUS mają do niego dostęp poprzez sieć WAN. Został on oparty na zapewnionym przez Wykonawcę środowisku mainframe[3].
System FARMER współpracował z systemem KRUSNAL-C (obecnie nSIU), który jest systemem centralnym i współpracuje z systemami instytucji zewnętrznych (NBP, PFRON oraz NFZ). System ten zapewnia centralne przechowywanie i przetwarzanie danych osobowych poprzez Centralny Zasób Danych Osobowych i współpracuje z pozostałymi systemami KRUS przez sieć WAN KRUS.
W okresie objętym kontrolą system FARMER utrzymywany i modyfikowany był na podstawie dwóch umów: nr 114/2011 z dnia 31 sierpnia 2011 r. z Bydgosko-Szczecińskim konsorcjum ZETO oraz nr 107/2015 z dnia 1 lipca 2015 r. z konsorcjum ZETO-ASSECO-UNIZETO, przy czym KRUS jest właścicielem praw majątkowych do tego systemu.

(Dowód: akta kontroli Tom II str. 217-537)

W KRUS funkcjonowały także systemy wspomagające m.in.:

- Archiwum – system do zarządzania dokumentacją wytworzoną i zgromadzoną w KRUS (outsourcing usług);
- Saturn HR – system do zarządzania kadrami KRUS (zarządzany przez KRUS);
- Remedy – system służący do ewidencji aktywnych zasobów IT (outsourcing usług);
- DGA Quality – system wspierający wdrożony w KRUS Zintegrowany System Zarządzania (outsourcing usług);
- Workflow – system stanowiący zbiór aplikacji realizujących różne funkcje biznesowe i IT - logowanie, dostęp do portalu (outsourcing usług).

(Dowód: akta kontroli Tom I str. 363-380)

1.2 Organizacja zarządzania procesem zapewnienia bezpieczeństwa systemów informatycznych.

Opis stanu faktycznego

W KRUS, w okresie objętym kontrolą, funkcjonował Zintegrowany System Zarządzania (ZSZ) składający się m.in. z systemu zarządzania bezpieczeństwem informacji. Polskie Centrum Badań i Certyfikacji przyznało KRUS (Centrali wraz

[2] System wdrożono w 2015 r. i zastąpił funkcjonujący w KRUS od 2000 roku system KRUSnal oraz system KRUSnal-C (od 2009 r.).
[3] Komputer główny.

z Oddziałami Regionalnymi) Certyfikat potwierdzający, iż obsługa ubezpieczonych i świadczeniobiorców w zakresie zadań wynikających z ustawy o ubezpieczeniu społecznym rolników[4] w odniesieniu do aktualnej wersji Deklaracji Stosowania[5] spełnia wymagania normy PN-ISO/IEC 27001:2007[6] (Norma).

(Dowód: akta kontroli Tom I str. 14-16, 710)

Zgodnie z informacjami uzyskanymi z Polskiego Centrum Badań i Certyfikacji Certyfikat systemu bezpieczeństwa informacji udzielony KRUS dotyczy całości zakresu działalności tej jednostki tzn. wszystkich zadań Kasy, realizowanych w Centrali, w wymienionych w certyfikacie Oddziałach Regionalnych (OR) oraz w podległych im Placówkach Terenowych.

(Dowód: akta kontroli Tom I str. 759-760)

1.3 Polityka Bezpieczeństwa Informacji oraz określenie celów bezpieczeństwa

W okresie objętym kontrolą w KRUS obowiązywała Polityka Bezpieczeństwa Informacji zatwierdzona przez Prezesa tej jednostki w dniu 8 marca 2012 r. oraz jej zaktualizowana wersja zatwierdzona w dniu 21 lipca 2015 r. W dokumentach tych określono zakres ochrony zasobów Kasy oraz rodzaj wsparcia dla procesów zmierzających do zapewnienia bezpieczeństwa informacji KRUS. Polityka bezpieczeństwa odnosiła się do wszystkich elementów określonych w pkt. 5.2[7] ww. Normy, a jej aktualność była potwierdzana w corocznych raportach z przeglądu Zintegrowanego Systemu Zarządzania sporządzanych przez Pełnomocnika Prezesa KRUS ds. ZSZ.

Zadeklarowane przez kierownictwo cele postawione przed systemem zarządzania bezpieczeństwem informacji to: zaangażowanie wszystkich pracowników w ochronę informacji, zapewnienie zgodności z obowiązującym prawem, zmniejszanie ryzyka utraty informacji.

(Dowód: akta kontroli Tom II str. 1, 146, Tom I str. 547)

Stwierdzona nieprawidłowość

W KRUS, planując jak osiągnąć cele w zakresie bezpieczeństwa informacji, nie określono jakie zasoby[8] będą wymagane dla ich osiągnięcia, celom tym nie przypisano miernika, nie określono również kiedy osiągnięcie tych celów jest oczekiwane. Do powyższych celów nie odnoszą się również procedury ZSZ.

Zgodnie z Normą organizacja powinna ustanowić cele bezpieczeństwa informacji dla odpowiednich funkcji i szczebli. Norma pkt. 6.2 stanowi, iż powinny one być m.in. spójne z polityką bezpieczeństwa, mierzalne i aktualizowane. Ponadto organizacja planując jak osiągnąć cele bezpieczeństwa powinna określić m.in. jakie zasoby będą wymagane do tego celu oraz kiedy to będzie zakończone.

(Dowód: akta kontroli Tom I str. 61-63, 187, 246-304, 630)

1.4 Określenie procesów zadań KRUS oraz przyjęty wskaźnik bezpieczeństwa

Opis stanu faktycznego

W KRUS zidentyfikowano procesy związane z realizacją kluczowych zadań instytucji, przypisano im procedury oraz określono ich właścicieli. Obecnie obowiązuje XV wydanie Księgi Procesów[9] zatwierdzonej 17 czerwca 2015 r. przez Prezesa KRUS. Opracowano 22 procedury związane z procesem zarządzania bezpieczeństwem[10]

---

[4] Ustawa z dnia 20 grudnia 1990 r. (Dz. U. z 2015 r., poz. 704).

[5] Obecnie obowiązuje VIII wydanie deklaracji stosowania z dnia 29 kwietnia 2015 r.

[6] W okresie objętym kontrola funkcjonowały dwa takie certyfikaty Nr. I-19/1/2014 wydany 21 listopada 2014 r. oraz Nr JKI - 2/2/2011 z dnia 22 listopada 2011 r.

[7] Zgodnie z pkt. 5.2 Normy Polityka powinna zwierać: cele bezpieczeństwa informacji, zobowiązanie do spełnienia mających zastosowanie wymagań dotyczących bezpieczeństwa informacji, zobowiązanie do ciągłego doskonalenia systemu zarządzania bezpieczeństwa.

[8] Np. zasoby finansowe i kadrowe.

[9] W okresie objętym kontrolą obowiązywały 5 wydań księgi procesów XI z 14 marca 2013 r. XII z 17 lutego 2014 r., XIII z 13 października 2014 r. XIV 5 listopada 2014 r. oraz XV 17 czerwca 2015 r.

[10] M.in. Procedura awaryjna na wypadek naruszenia lub utraty danych osobowych, Procedura awaryjna na wypadek dysfunkcji lub włamania do systemu informatycznego, Procedura zarządzania kontami użytkowników, Procedura zarządzania zmianami

(11 dla centrali i 11 dla oddziałów regionalnych). Jako miernik monitorujący proces zarządzania bezpieczeństwem przyjęto iloraz liczby incydentów bezpieczeństwa w roku bieżącym oraz liczby incydentów w roku poprzednim. Wskaźnik bezpieczeństwa w 2013 r. wyniósł 0,64 a w 2014 r. 0,68 przy wartości oczekiwanej <1.

(Dowód: akta kontroli Tom I str. 12, 30-83, 246-304, 658)

Stwierdzone nieprawidłowości

W ocenie NIK przyjęty miernik nie oddawał w sposób rzetelny rzeczywistego obrazu realizacji procesu zarządzania bezpieczeństwem informacji:

1. Zakładał on, że wszystkie zgłoszone incydenty mają taką samą wagę i nie uwzględniał innego ujęcia tj. nadania większego znaczenia np. incydentom zdefiniowanym w procedurach jako incydenty dużej wagi[11]. Zdaniem NIK algorytm wyliczania wskaźnika tego procesu powinien być sformułowany w taki sposób aby incydenty poważniejsze np. incydenty dużej wagi miały większy wpływ na jego wartość.
2. Zdaniem Izby przyjęcie takiego miernika może zwiększać ryzyko samoograniczania się pracowników w zakresie zgłaszania incydentów np. w celu uzyskania zakładanej wielkości wskaźnika.
3. Wzrastająca liczba incydentów, zdaniem NIK, nie musi świadczyć o mniejszej skuteczności systemu zarządzania bezpieczeństwem informacji, ponieważ wzrost ten może być związany z czynnikami zewnętrznymi np. ataki złośliwego oprogramowania, lub może być wynikiem uzyskanego wzrostu ich wykrywalności.
4. W przypadku „uszczelnienia" systemu zbierania incydentów (NIK wnioskuje o takie działanie w rozdziale IV Uwagi i wnioski) powyższy miernik nie będzie miarodajny, gdyż pomimo wprowadzenia działań naprawczych wykaże spadek poziomu bezpieczeństwa.

(Dowód: akta kontroli Tom I str. 278, 279, 344-358)

1.5 Kwestia odpowiedzialności za bezpieczeństwo informacji.

Opis stanu faktycznego

Zgodnie z Księgą Procesów zarządzanie bezpieczeństwem informacji przypisano Drugiemu Zastępcy Prezesa - w trakcie kontroli funkcję tę pełniła Krystyna Gdula. Procedury wprowadzone w ramach ZSZ określały podział zadań i odpowiedzialności w regulowanym zakresie. Do każdej procedury przyporządkowano właściciela procedury oraz osobę pełniącą nadzór nad przestrzeganiem procedury[12].

Stwierdzone nieprawidłowości

Zarówno analiza dokumentacji kadrowej (zakresy obowiązków, regulaminy organizacyjne) jak i uzyskane wyjaśnienia wskazują, że podział zadań z zakresu bezpieczeństwa teleinformatycznego nie był w Centrali KRUS jednoznaczny i precyzyjny.

W dniu 26 czerwca 2015 r. z upoważnienia Prezesa KRUS Zastępca Prezesa p. Krystyna Gdula wyjaśniła, że: *za bezpieczeństwo systemów teleinformatycznych Kasy odpowiada Biuro Informatyki i Telekomunikacji co wynika z regulaminu organizacyjnego Biura obowiązującego od dnia 1 lipca 2013 r.* Natomiast Zastępca dyrektora Biura Informatyki i Telekomunikacji wyjaśnił, że: *zadania w zakresie bezpieczeństwa teleinformatycznego zostały delegowane do Zespołu Ochrony Informacji i Spraw Obronnych na podstawie zarządzania nr 6 Prezesa KRUS z dnia 17 marca 2015 r. zmieniającego zarządzenie w sprawie nadania regulaminu KRUS.*

---

w systemach informatycznych, Procedura zgłaszania i obsługi incydentu, Procedura przeglądu urządzenia informatycznego, Procedura wykonywania kopii bezpieczeństwa.

[11] Zgodnie z Instrukcją podstawowych zasad bezpieczeństwa dla pracowników KRUS incydent dużej wagi np. kradzież danych osobowych, włamanie do systemu teleinformatycznego, nieuprawnione wejście) Dyrektor jednostki organizacyjnej zgłasza m.in. Prezesowi KRUS.

[12] Poszczególni właściciele procedur zostali określeni w księdze procesów natomiast nadzór nad realizacją procedur został określony w treści poszczególnych procedur.

Zdaniem NIK wyraźnie określona i egzekwowana odpowiedzialność jest sprawą kluczową dla bezpieczeństwa informacji.

(Dowód: akta kontroli Tom I str. 7, 116, 246-304, 718-751, 755)

1.6 Proces szacowania ryzyka

Proces szacowania ryzyka w KRUS uregulowany został w Metodyce szacowania ryzyka bezpieczeństwa informacji przyjętej w dniu 1 grudnia 2009 r.

(Dowód: akta kontroli Tom I str. 12, 20-28)

W okresie objętym kontrolą, funkcjonowała ocena ryzyka utraty informacji zatwierdzona przez Prezesa KRUS w dniu 16 maja 2014 r. Na jej podstawie sporządzono i wdrożono plan minimalizacji ryzyka w Centrali KRUS oraz 47 takich planów w Oddziałach Regionalnych.
W dniu 10 czerwca 2014 r. Prezes KRUS zatwierdził Plan minimalizacji ryzyka utraty informacji Centrali tej jednostki.

(Dowód: akta kontroli Tom I str. 324-333, 382-397)

Stwierdzone nieprawidłowości

W KRUS nie opracowano metody szacowania ryzyka utraty informacji w przypadku systemów outsourcowanych. Zdaniem NIK przekazanie zasobów KRUS związanych z jej ustawowymi obowiązkami w zarząd zewnętrznego wykonawcy powinno być połączone z adekwatnym zarządzaniem ryzykiem z tym związanym.
NIK dostrzegła działania podjęte w tym zakresie - ujęcie kwestii podziału ryzyka w treści nowej, obowiązującej od 1 września 2015 r., umowy na utrzymanie systemu FARMER. Niemniej jednak ze względu na to, że do dnia zakończenia kontroli powyższe postanowienia nie zostały jeszcze zrealizowane, nie mogły podlegać ocenie NIK. Niezależnie od powyższego, zdaniem Izby, KRUS winna wypracować systemowe podejście do zarządzania ryzykiem na styku KRUS – wykonawca w przypadku systemów outsourcowanych (dla modelu całkowitego i częściowego outsourcingu) i powiązane z tym stosowne narzędzia nadzoru nad bezpieczeństwem powierzonych zasobów oraz co za tym idzie, oszacować niezbędne dla sprawowania tego nadzoru zasoby po stronie KRUS (więcej w podrozdziale 2.2 *Nadzór nad wykonaniem umowy utrzymania systemu FARMER str. 11).*

(Dowód: akta kontroli Tom I str. 658; Tom II str. 376-536)

1.7 Podstawowe regulacje w zakresie zasad bezpiecznego przetwarzania informacji

Opis stanu faktycznego

Podstawowymi regulacjami w zakresie zasad bezpiecznego przetwarzania informacji wdrożonymi w KRUS były:

- Polityka Bezpieczeństwa w zakresie danych osobowych KRUS (Polityka DO);
- Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w KRUS (Instrukcja DO);
- Instrukcja podstawowych zasad bezpieczeństwa dla pracowników KRUS – dokument opracowany w ramach ZSZ (Instrukcja zasad bezpieczeństwa).

(Dowód: akta kontroli Tom I str. 344-358; Tom II str. 2-144)

W okresie objętym kontrolą obowiązywała Polityka DO wydana zarządzeniem Prezesa KRUS nr 8 z dnia 30 kwietnia 2012 r. w sprawie wprowadzenia w tej jednostce Polityki Bezpieczeństwa w zakresie ochrony danych osobowych oraz Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych. Zgodnie z § 1 ust. 2 pkt 2 zarządzenia dokumenty te podlegają bieżącej aktualizacji przez Centralnego Administratora Bezpieczeństwa Informacji, a każdorazowa ich zmiana wymaga zatwierdzenia przez Prezesa KRUS.
Obowiązek aktualizacji ww. dokumentacji został zawarty w § 4 Regulaminu Organizacyjnego Zespołu Ochrony Informacji Niejawnych i Spraw Obronnych,

zgodnie z którym Administrator Bezpieczeństwa Informacji sprawuje nadzór nad opracowaniem oraz aktualizacją dokumentacji dotyczącej przetwarzania danych osobowych w KRUS, w szczególności Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemami informatycznymi.

(Dowód: akta kontroli Tom I str. 321; Tom II str. 128-134)

Polityka DO KRUS określała m.in. zasady przetwarzania danych osobowych opis zdarzeń naruszających ochronę danych osobowych, organizację bezpieczeństwa w odniesieniu do danych osobowych wraz z podziałem zadań, oraz wykazy: obszarów, w których przetwarzane są dane osobowe; zbiorów danych wraz ze wskazaniem programów do ich przetwarzania; jak również określała środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozłączalności przetwarzania danych.

(Dowód: akta kontroli Tom II str. 2-101)

Instrukcja DO regulowała m.in.: zarządzanie hasłami użytkowników, sposób użytkowania systemów informatycznych, sposób przechowywania nośników informacji, usuwanie danych osobowych zapisanych na nośnikach informacji, metody i częstotliwość tworzenia kopii bezpieczeństwa, metody i częstotliwość sprawdzania obecności szkodliwego oprogramowania oraz metody jego usuwania, sposób dokonywania przeglądów i konserwacji systemu, sposób postępowania w zakresie komunikacji w sieciach komputerowych.

(Dowód: akta kontroli Tom I str. 102-127)

Stwierdzone nieprawidłowości

Analiza dokumentów związanych z bezpieczeństwem informatycznym wykazała następujące nieprawidłowości:

1) Polityka DO i Instrukcja DO nie obejmowały części systemów przetwarzających dane osobowe takich jak Centralny System Finansowo-Księgowy, system poczty elektronicznej oraz Workflow. Nie były one wyszczególnione w załączonym do Polityki DO wykazie systemów przetwarzających dane osobowe, jak również nie został wskazany sposób przepływu danych pomiędzy tymi systemami[13].

   (Dowód: akta kontroli Tom I str. 363-380; Tom II str. 58-61)

2) Wykaz budynków w których przetwarzane są dane osobowe – załącznik do Polityki DO - był niepełny. W wykazie tym nie umieszczono m.in. ośrodka zapasowego dla systemu FARMER w Szczecinie, oraz ośrodka zapasowego KRUS w Żyrardowie[14].

3) Instrukcja regulowała m.in. kwestie zabezpieczenia antywirusowego systemów, natomiast dla urządzeń mobilnych nie opracowano procedury dystrybucji oprogramowania antywirusowego. Zgodnie z wyjaśnieniami Prezesa KRUS każdy użytkownik urządzenia mobilnego zarządza oprogramowaniem antywirusowym we własnym zakresie. Ponadto Prezes wyjaśnił, że pracownicy KRUS bez zdalnego dostępu do sieci WAN KRUS uzyskują dostęp wyłącznie do poczty elektronicznej. NIK zauważa, że w chwili obecnej podstawowym źródłem instalacji złośliwego oprogramowania jest właśnie poczta elektroniczna. Powyższy stan rzeczy w połączeniu z brakiem nadzoru nad ochroną urządzeń mobilnych w ocenie NIK negatywnie wpływa na bezpieczeństwo informacji.

---

[13] Kontrola nie obejmowała zagadnień przestrzegania postanowień ww. dokumentacji w systemach CSFK, system poczty elektronicznej oraz Workflow.

[14] Zgodnie § 4 pkt 1 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 Polityka bezpieczeństwa zawiera w szczególności wykaz budynków i pomieszczeń w których przetwarzane są dane osobowe oraz wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

(Dowód: akta kontroli Tom I 140, 188, 189)

4) Opracowane procedury nie były w pełni czytelne i przejrzyste. Wiele zagadnień np. zarządzanie hasłami użytkowników czy tworzenie kopii bezpieczeństwa ujętych w Polityce DO i Instrukcji DO było powielonych w Procedurach ZSZ. Powstały więc obszary uregulowane równolegle w dwóch procedurach, przy czym kontrola nie wykazała niezgodności tych dokumentów. Jednocześnie Polityka i Instrukcja DO miały zastosowanie do systemów, w których nie przetwarza się danych osobowych m.in. WinSTP, DGA Quality. Zdaniem NIK rzetelnie opracowane procedury powinny być czytelne, a jednocześnie winny precyzyjnie, w sposób nie budzący żadnych wątpliwości, wskazywać jaki jest ich zasięg (np. jakie systemy są nimi objęte). Dla wskazanych wyżej systemów informatycznych nieprzetwarzających danych osobowych nie opracowano dotychczas szczegółowych zasad bezpieczeństwa z uwagi na wdrożony w Kasie Zintegrowany System Zarządzania. Jednakże procedury ZSZ nie obejmowały wszystkich obszarów ujętych w Polityce DO. Oznacza to, że niektóre zagadnienia ujęte tylko w Polityce DO i Instrukcji DO miały zastosowanie do wszystkich systemów KRUS. Przykładem mogą być uregulowania dotyczące polityki zabezpieczenia antywirusowego - pomimo, że praktycznie zostały wdrożone we wszystkich systemach - ujęte zostały jedynie w Polityce DO i Instrukcji DO.

(Dowód: akta kontroli Tom I str. 189, 194-206, 344-358; Tom II str. 2-134)

W trakcie kontroli[15] trwały prace nad nową wersją Polityki DO i Instrukcji DO wynikające m.in. z nowelizacji od 1 stycznia 2015 r. ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[16].

Jak wyjaśnił Pełnomocnik ds. Ochrony Informacji Niejawnych (pełnomocnik OIN) przy opracowaniu projektu ww. dokumentacji szczególną uwagę zwrócono na spójność zapisów w odniesieniu do obowiązujących procedur w zakresie danych osobowych. Dotyczy to również załączników funkcjonalnych jakimi są wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz wykaz budynków, w których przetwarzane są dane osobowe.

(Dowód: akta kontroli Tom I str. 184, 711)

1.8 Klasyfikacja informacji

W KRUS opracowano Klasyfikację Informacji[17] w ramach procedur ZSZ. Klasyfikacja ta była wspólna dla wszystkich jednostek organizacyjnych KRUS. Zgodnie z jej treścią celem wprowadzenia tej klasyfikacji było uporządkowanie postępowania z informacjami jawnymi tj. nieobjętymi ustawą o ochronie informacji niejawnych. Dla poszczególnych poziomów ochrony zdefiniowano sposoby postępowania z zawierającymi się w nich informacjami. Podstawowym elementem klasyfikacji były grupy informacji wyodrębnione w oparciu o Rzeczowy wykaz akt KRUS. W klasyfikacji informacji zdefiniowano dwa poziomy ochrony:

- Poziom I – informacje o podstawowym poziomie ochrony,
- Poziom II – informacje o podwyższonym poziomie ochrony.

Dla zdefiniowanych poziomów klasyfikacja nie wprowadziła wymogu oznaczania objętych nimi informacji. Zgodnie z tą klasyfikacją Grupie informacji dotyczącej „04

[15] Zgodnie z § 5 Zarządzenia nr 1 Prezesa Kasy Rolniczego Ubezpieczenia Społecznego z dnia 6 stycznia 2015 r. w sprawie realizacji ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych Administrator Bezpieczeństwa Informacji został zobowiązany do 27 lutego 2015 r. do zaktualizowania dokumentów regulujących przetwarzanie danych osobowych w KRUS w tym: Polityki bezpieczeństwa i instrukcji zarządzania systemami informatycznymi. W dniu 1 czerwca 2015 r. Zarządzeniem nr 14 zmieniającym ww. zarządzenie Pan Prezes uchylił ten obowiązek. Przyczyną tego stanu rzeczy wynikała ze zmian organizacyjnych i kadrowych.

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

[17] Obecnie obowiązuje wydanie V klasyfikacji z dnia 27 lipca 2015 r.

Informatyzacji" (w zespole „0 zarządzanie") przypisano podstawowy poziom ochrony. W grupie tej, zgodnie z Jednolitym wykazem akt[18] zawarte zostały m.in. dokumentacja związana z eksploatacją systemów teleinformatycznych i oprogramowania (w tym kody źródłowe, kopie bezpieczeństwa, dokumentacje z przeglądu urządzeń informatycznych) oraz dokumentacja związana z bezpieczeństwem systemów teleinformatycznych.

(Dowód: akta kontroli Tom I str. 84-110, 223-244, 641)

Stwierdzone nieprawidłowości

Zdaniem NIK informacje: kody źródłowe oraz kopie bezpieczeństwa systemów są przykładem danych wrażliwych, tj. danych, których ochrona nie jest prawnie wymagana, jednakże stanowią one zasoby krytyczne instytucji. Izba zwraca uwagę, że zgodnie z ww. klasyfikacją dane te powinny być objęte ochroną na najniższym poziomie. W dokumentacji związanej z klasyfikacją informacji nie zdefiniowano danych wrażliwych (zasobów krytycznych), ani nie uregulowano odpowiednio kwestii ich ochrony. W ocenie NIK świadczy to o tym, że opracowanie ww. klasyfikacji nie zostało poprzedzone oszacowaniem ryzyka nieuprawnionej modyfikacji, czy braku dostępności do takich zasobów. Co w konsekwencji prowadzi, do tego że część takich zasobów chronionych jest w sposób intuicyjny. Zauważyć należy, że kody źródłowe, czy kopie bezpieczeństwa systemu FARMER były – pomimo opatrzenia ich podstawowym poziomem ochrony - w praktyce przechowywane w sejfie, w zamkniętym i chronionym pomieszczeniu, co świadczy o świadomości co do znaczenia tych danych dla bezpieczeństwa teleinformatycznego.

(Dowód: akta kontroli Tom I str. 641, 763)

1.9 Wykaz aktywów wspierających

Opis stanu faktycznego

W KRUS funkcjonował system BMC Remedy w którym zwarte były informacje o sprzęcie i oprogramowaniu. System ten zawierał dane na temat sprzętu i oprogramowania funkcjonującego w całej KRUS (Centrala, Oddziały oraz podległe im placówki).
W ramach tych informacji każdemu urządzeniu przyporządkowano istotność (zakładka Priority).

(Dowód: akta kontroli Tom I str. 648-652)

W trakcie kontroli nie przedstawiono wykazu pracowników kluczowych dla bezpieczeństwa informacji. Zgodnie z wyjaśnieniami otrzymanymi w tej kwestii od Prezesa KRUS wszyscy pracownicy zostali przeszkoleni w trakcie wdrażania systemu zarządzania bezpieczeństwem informacji, podobnie zostają przeszkoleni nowozatrudnieni pracownicy.
W KRUS nie opracowano osobnych procedur naboru na stanowiska pracy kluczowe dla bezpieczeństwa informacji.

(Dowód: akta kontroli Tom I str. 186)

Wg NIK Norma PN-ISO/IEC 27001 nie określa jednoznacznie jaki zakres powinien obejmować wykaz aktywów wspierających. Jednakże zarówno norma PN-ISO/IEC 27005 jaki i literatura fachowa w tym zakresie[19] wskazują, że pełny wykaz aktywów wspierających powinien, oprócz sprzętu i oprogramowania, obejmować również organizację, siedzibę, procedury oraz personel (w tym wskazanie pracowników kluczowych dla bezpieczeństwa). Wszystkie te elementy powinny mieć przyporządkowaną istotność i dopiero takie opracowanie może stanowić podstawę zarządzania ryzykiem i wynikające z niego podwyższone wymagania odnośnie procedury naboru na stanowiska kluczowe dla bezpieczeństwa informacji.

---

[18] Jednolity wykaz akt Kasy Rolniczego Ubezpieczenia Społecznego przyjętym r. zarządzeniem Prezesa KRUS z dnia 25 czerwca 2014 w sprawie wprowadzenia instrukcji kancelaryjnej, jednolitego rzeczowego wykazu akt oraz instrukcji w sprawie organizacji i zakresu działań archiwów zakładowych.

[19] Jerzy Krawiec, Grażyna Ożarek System zarządzania bezpieczeństwem Informacji w praktyce Zabezpieczenie wyd. Polski Komitet Normalizacyjny Warszawa 2014 r.

Ocena cząstkowa

W badanym obszarze NIK ocenia - w oparciu o stosowany w metodyce CobiT 4.1 Model dojrzałości - poziom zarządzania procesami zapewnienia bezpieczeństwa systemów jako „zdefiniowany". Zdaniem NIK przyjęty w KRUS system bezpieczeństwa informacji wraz z wdrożonymi procedurami może stanowić podstawę do zarządzania bezpieczeństwem informacji, jednakże część przyjętych uregulowań wewnętrznych wymaga uzupełnienia i uszczegółowienia, jak również pogłębionych analiz (np. klasyfikacja informacji). Opracowanie i wdrożenie ZSZ w ocenie NIK świadczy o tym, że kierownictwo ma świadomość zagrożeń i zasad bezpieczeństwa teleinformatycznego.
Pozytywnie należy się odnieść do faktu, iż część prac naprawczych została podjęta jeszcze w trakcie kontroli. Oprócz przytoczonych wyjaśnień Pełnomocnika OIN, Wicedyrektor BIiT poinformował, że podjęto działania, których celem jest ujednolicenie i uspójnienie procedur z obszaru zarządzania bezpieczeństwem teleinformatycznym KRUS.

(Dowód: akta kontroli Tom I str. 756)

2. Testowanie, nadzorowanie i monitorowanie procesu zapewnienie bezpieczeństwa systemów informatycznych.

2.1 Audyty wewnętrzne

Opis stanu faktycznego

Jak wyjaśnił Prezes KRUS w związku ze spełnianiem przez tę jednostkę, wynikających z § 20 pkt 3 w zw. z § 20 ust. 2 pkt 14 Rozporządzenia KRI[20], minimalnych wymagań dla rejestrów publicznych i wymiany informacji elektronicznej oraz minimalnych wymagań dla systemów informatycznych, poprzez wdrożenie i certyfikowanie sytemu zarządzania bezpieczeństwem informacji zgodnego z Polską Normą PN-ISO/IEC 27001, uznaje się, że Kasa nie jest zobligowana do przeprowadzania corocznych audytów wewnętrznych w zakresie bezpieczeństwa informacji.
Zasady przeprowadzania audytów wewnętrznych systemu bezpieczeństwa informacji przeprowadzanych w ramach Zintegrowanego Systemu Zarządzania uregulowane zostały w Procedurze planowania i przeprowadzania audytów wewnętrznych.

(Dowód: akta kontroli Tom I str. 137, 144-171)

W ramach ww. audytów obszar zarządzania bezpieczeństwem podlega badaniom na zgodność z wymaganiami Normy we wszystkich jednostkach organizacyjnych KRUS.
Zadania audytu wewnętrznego w KRUS były realizowane przez Biuro Audytu na podstawie rocznego planu audytu, który był opracowany na podstawie analizy ryzyka. Na skutek tego w 2014 r. przeprowadzono zadanie „Ocena systemu bezpieczeństwa informacji".

(Dowód: akta kontroli Tom I str. 136-138)

W wyniku audytu wewnętrznego, przeprowadzonego w okresie wrzesień – grudzień 2014 r. sformułowano 7 zaleceń, w tym m.in.:

- Przegląd dokumentacji dotyczącej bezpieczeństwa przetwarzania danych osobowych (Polityka DO i Instrukcja DO) w celu zapewnienia jej zgodności z pozostałymi regulacjami ZSZ.
- Wprowadzenie regulacji wdrażającej obowiązek cyklicznych przeglądów uprawnień pod kątem ich adekwatności do wykonywanych zadań i określających częstotliwość i zakres przeglądów.

[20] Rozporządzenie Rady Ministrów z 12 kwietnia 2012 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2012 r. poz. 526 ze zm.)

– Rozważenie możliwości wdrożenia narzędzia dedykowanego do zarządzania incydentami bezpieczeństwa.

(Dowód: akta kontroli Tom I str. 548-600)

Zgodnie z informacją przekazaną kontrolerom NIK, według stanu na dzień 24 września 2015 r. zrealizowano 5 zaleceń pokontrolnych, w tym wprowadzono do aktualnej wersji procedury zarządzania kontami użytkowników oraz obowiązek przeprowadzania przez dyrektorów biur kierujących zespołami oraz dyrektorów OR przeglądów uprawnień nadanych pracownikom pod kątem ich adekwatności do wykonywanych przez nich zadań. Pozostałe zalecenia były w trakcie realizacji.

(Dowód: akta kontroli Tom I str. 639-640)

2.2 Nadzór nad wykonaniem umowy utrzymania systemu FARMER

Zgodnie z § 7 pkt. 8 Umowy z ZETO Bydgoszcz zawartej w dniu 31 sierpnia 2011 r audyt systemu FARMER był przeprowadzany przez audytora zewnętrznego raz w roku. Kasa każdorazowo była informowana o czasie oraz zakresie przeprowadzanego audytu, a plan audytu był przekazywany do zaopiniowania przez KRUS. Na podstawie ostatniego audytu w ZETO Bydgoszcz z dnia 15 listopada 2014 r. wykonanego przez Polskie Towarzystwo Informatyczne nie było zaleceń dotyczących poprawy bezpieczeństwa systemu FARMER.

(Dowód: akta kontroli Tom I str. 139, 601-624, 639)

Obowiązująca w okresie objętym kontrolą umowa (od 1 września 2015 r.) w § 8 wprowadziła dwa rodzaje audytów – audyt przeprowadzony przez KRUS z asystą podmiotu trzeciego lub przez podmiot trzeci wskazany przez KRUS z częstotliwością nie większą niż raz do roku.

Niezależnie od tych audytów wykonawca zobowiązany był co najmniej raz na 18 miesięcy wykonać audyt ośrodków obliczeniowych i łączy telekomunikacyjnych pod kątem spełnienia wymagań i standardów technicznych, organizacyjnych oraz weryfikacji poziomu bezpieczeństwa. Do dnia 20 października 2015 r. audyty te nie były jeszcze przeprowadzone.

(Dowód: akta kontroli Tom I str. 752; Tom II str. 378-388)

Stwierdzone nieprawidłowości

1. Żadna z zawartych umów (obecnie obowiązująca i poprzednia) nie nakładała na wykonawcę obowiązku przeprowadzania testów bezpieczeństwa systemu FARMER. Takich testów nie zlecała również KRUS. Wyjaśniając powyższą kwestię Prezes KRUS poinformował, iż spowodowane to było tym, że dokumentacja prowadzona przez wykonawcę, związana z dostępem do systemu, nie dawała ku temu podstaw oraz tym, że dostawca infrastruktury sieci WAN w raportach nie informował KRUS o konieczności podjęcia dodatkowych działań związanych z podniesieniem bezpieczeństwa infrastruktury. NIK nie podziela powyższej argumentacji. Zdaniem NIK przeprowadzanie takich testów jest w chwili obecnej standardem monitorowania bezpieczeństwa i istotnym elementem ciągłego doskonalenia procesu zapewnienia bezpieczeństwa. NIK zauważa, że system FARMER jest produktem unikatowym (jedynym w Polsce) co oznacza, że wynikający z pkt. A.12.6.1 Normy obowiązek zarządzania podatnościami technicznymi może zostać zrealizowany tylko przez zamawiającego lub wykonawcy[21], co oznacza, że KRUS nie może pozyskać takich informacji w inny sposób.

(Dowód: akta kontroli str. Tom I str. 639; Tom II str. 217-537)

[21] 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.

2. Zdaniem NIK na skutek wyznaczenia małych zasobów kadrowych do monitorowania i nadzoru nad wykonaniem umowy przez wykonawcę istnieje wysokie ryzyko zaniechań w tym zakresie. Zauważyć należy, że poprzednio obowiązująca umowa (w okresie od 2011 r. do września 2015 r.) zawierała zapisy[22] obligujące wykonawcę do zapewnienia dostępu do systemu monitorującego parametry jakości świadczenia usług, dla pięciu wyznaczonych pracowników KRUS. Tymczasem, ze względu na zasoby kadrowe uprawnienia zamawiającego w tym zakresie nie były wykorzystywane, a aspektami monitorowania systemu zajmowali się tylko jednoosobowo kolejni Kierownicy Projektów. Ponadto na dzień 7 października 2015 r., zgodnie z wyjaśnieniami otrzymanymi od Wicedyrektora BIiT Karola Tomczaka, zajmował się on jednoosobowo rozliczeniami miesięcznymi, rozwojem systemu oraz szeroko pojętym nadzorem nad poprawnością realizacji umowy. Przy czym należy podkreślić, iż ze szczegółowego zakresu czynności powierzonych temu pracownikowi w Karcie czynności wynika, że zadania te nie zostały ujęte w zakresie jego obowiązków. Zostały mu natomiast przypisane inne zadania dotyczące innych systemów np. administrowanie centralną aplikacją Portal dla Pracowników. Według analiz BIiT minimalny zespół zajmujący się utrzymaniem i rozwojem systemu FARMER, poza kierownikiem projektu, powinien obejmować 3 osoby (po jednej osobie zajmującej się utrzymaniem, rozwojem oraz biblioteką).

(Dowód: akta kontroli Tom I str. 755, 719; Tom II str. 287-293)

3. KRUS nie otrzymywała informacji o incydentach dotyczących bezpieczeństwa informacji systemu FARMER od firmy utrzymującej ten system. W umowie z wykonawcą nie zawarto takiego obowiązku. Na tę okoliczność Prezes KRUS wyjaśnił, że w trakcie audytów Wykonawca przedstawił rejestr incydentów bezpieczeństwa, który nie zawierał zapisów o ich naruszeniu. Powyższe dane stanowiły informację chronioną i były udostępnione do wglądu w siedzibie Wykonawcy.

W ocenie NIK nieuregulowanie kwestii testów bezpieczeństwa i faktyczne nieprzeprowadzanie ich dla systemu FARMER, w połączeniu z nieprzekazywaniem przez firmę ZETO Bydgoszcz informacji o incydentach istotnie ogranicza KRUS w sprawowaniu skutecznego nadzoru nad bezpieczeństwem zasobów informacyjnych przekazanych pod zarząd zewnętrznego wykonawcy, w tym zasobów szczególnie chronionych np. danych wrażliwych w rozumieniu ustawy o ochronie danych osobowych. Ww. nadzór, zdaniem NIK jest dodatkowo ograniczony przez niewystarczające zasoby kadrowe przeznaczone do realizacji umowy z Firmą ZETO (w tym monitoringu realizacji umowy).

(Dowód: akta kontroli Tom I str. 639)

2.3 Definicja incydentu związanego z bezpieczeństwem teleinformatycznym

Opis stanu faktycznego

Definicja incydentu bezpieczeństwa została określona w KRUS jako pojedyncze lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań i zagrażają bezpieczeństwu informacji.

(Dowód: akta kontroli Tom II str. 5)

Opis sposobu zgłaszania incydentu jak również procedury obsługi różnych typów incydentów zawarte zostały w dokumentach:

- Instrukcji analizy zgłoszonych incydentów bezpieczeństwa informacji (obecnie obowiązuje wydanie V[23])

[22] Pkt 5.6 Załącznika nr 6 do umowy pn. SLA oraz zasady obsługi technicznej.
[23] Zatwierdzonej przez Prezesa KRUS w dniu 26 czerwca 2014 r.

- Procedurze zgłaszania oraz analizy incydentów bezpieczeństwa w Oddziale Regionalnym[24].
- Procedurze zgłaszania oraz analizy incydentów bezpieczeństwa w Centrali KRUS[25]
- Procedurze zgłaszania i obsługi incydentu (dot. dysfunkcji infrastruktury – systemowej) dla Centrali[26] oraz dla Oddziałów Regionalnych[27].

Zgodnie z tymi dokumentami każdy z pracowników KRUS zobowiązany był do zgłaszania wszystkich wykrytych incydentów bezpieczeństwa. Incydenty, zgodnie z ww. uregulowaniami, dzielą się na teleinformatyczne oraz incydenty niezwiązane z infrastrukturą teleinformatyczną. W przypadku wystąpienia incydentu dużej wagi procedura (Instrukcja zasad bezpieczeństwa) obliguje właściwego dyrektora do niezwłocznego powiadomienia Zastępcy Prezesa oraz Prezesa KRUS.

(Dowód: akta kontroli Tom I str. 344-358, 765-803)

Zespołem analizującym incydenty związane z bezpieczeństwem systemów teleinformatycznych byli pracownicy service-desk Biura Informatyki i Telekomunikacji. Zespół składał się z 3 osób: Głównego Informatyka oraz dwóch starszych inspektorów. W przypadku wykrycia incydentów dużej wagi związanych z bezpieczeństwem systemów IT kierowane były one do administratorów w Biurze Informatyki i Telekomunikacji.

Wg wyjaśnień Prezesa KRUS w okresie objętym kontrolą nie doszło do żadnych naruszeń zasad bezpieczeństwa informacji przez pracowników.

(Dowód: akta kontroli Tom I str. 140, 141)

Stwierdzone nieprawidłowości

W KRUS nie stworzono definicji incydentu dużej wagi. Jak wyjaśnił Prezes KRUS wynika to z tego, że nigdy nie ma pewności, że stworzony katalog incydentów dużej wagi jest kompletny. Podzielić należy opinię Pana Prezesa, że stworzenie zamkniętego katalogu incydentów dużej wagi jest trudne, jednakże, zdaniem NIK, zbudowanie takiej definicji pozwoli na większą jednoznaczność w tej kwestii oraz jednolitość w interpretacji zaistniałych zdarzeń.

Ponadto, zdaniem NIK procedury nie precyzują pełnej ścieżki zgłaszania incydentów dużej wagi. Obowiązek poinformowania m.in. Prezesa KRUS nałożony na dyrektorów nie jest powiązany z obowiązkiem osoby zgłaszającej, lub przyjmującej zgłoszenie o incydencie, poinformowania o tym przełożonego. Nie jest również jednoznacznie wskazane, kto winien decydować, czy dany incydent jest incydentem dużej wagi. Zdaniem NIK incydenty powinny mieć przypisaną istotność i dla poszczególnych istotności przyporządkowaną ścieżkę postępowania.

(Dowód: akta kontroli Tom I str. 642)

Opis stanu faktycznego

Zgodnie z informacją uzyskaną w trybie art. 29 ust 1 pkt 2 lit f ustawy o NIK[28] od zespołu CERT.GOV.PL w Agencji Bezpieczeństwa Wewnętrznego zarejestrowano w KRUS 24 incydenty zgłoszone przez tę jednostkę, jak również zidentyfikowane przez zespół CERT. Spośród nich 23 incydenty zostały zakwalifikowane i zarejestrowane[29] jako „klient botnetu", natomiast jeden incydent zarejestrowany w dniu 24 listopada 2014 r. zakwalifikowano jako nieuprawniony dostęp lub nieuprawnione wykorzystanie informacji. Wszystkie wykryte zdarzenia były zgłaszane do KRUS przez Zespół CERT w ABW. KRUS wysyłała informację zwrotną do ABW o podjętych krokach.

(Dowód: akta kontroli Tom I str. 175-180, 340)

---

[24] Zatwierdzona przez Dyrektora Biura Strategii i Rozwoju w dniu 26 sierpnia 2014 r.
[25] Zatwierdzona przez Dyrektora Biura Strategii i Rozwoju w dniu 26 sierpnia 2014 r.
[26] Zatwierdzone przez Dyrektora Biura Informatyki i Telekomunikacji w dniu 15 lutego 2013 r.
[27] Zatwierdzone przez Dyrektora Biura Informatyki i Telekomunikacji w dniu 18 lutego 2013 r.
[28] Ustawa z dnia 23 grudnia 1994 r. (Dz. U. z 2015 r., poz. 1096),
[29] Daty rejestracji zgłoszenia 26 luty, 12 i 13 marca, 18 czerwca, 22, 26 i 30 września, 6 i 29 października, 10 i 24 listopada, 24, 30 i 31 grudnia 2014 r. oraz 5, 8, 12, 13 stycznia, 10 i 17 lutego, 9 i 17 marca, 16 kwietnia 2015 r.

W okresie objętym kontrolą KRUS otrzymała 5 rekomendacji od zespołu CERT dokonania zmian w infrastrukturze Kasy. Zmiany te polegały na zablokowaniu ruchu sieciowego do określonych adresów IP i zostały wdrożone w ciągu 1 dnia roboczego.
(Dowód: akta kontroli Tom I str. 139)

Stwierdzone nieprawidłowości

Rejestr incydentów był prowadzony nierzetelnie, a co za tym idzie sprawozdawczość dotycząca bezpieczeństwa była niekompletna. Analiza zgłoszeń incydentów teleinformatycznych przekazywanych do service-desk wykazała, że gromadzenie informacji o zgłoszeniach incydentów było prowadzone z naruszeniem zasad zawartych w procedurach ZSZ dotyczących m.in. konieczności zgłaszania wszystkich incydentów do service- desk:
- Rejestr incydentów nie obejmował systemu FARMER np. zgłaszanie usterek w pracy systemu FARMER, zablokowania użytkownika itp. Odbywało się to poprzez bezpośredni kontakt z wykonawcą poza systemem service–desk, a co za tym idzie incydenty takie nie były odnotowywane w rejestrze prowadzonym w ramach ZSZ,

- Incydenty obsługiwane przez administratorów systemu nie były zgłaszane do service-desk i nie były odnotowywane w rejestrze zgodnie z procedurą. Przykładowo nie ujęto w tej ewidencji trzech przypadków wykrycia złośliwego oprogramowania ujawnionego na podstawie informacji uzyskanej od zespołu CERT.gov.pl. Nie ujęto w tym rejestrze również incydentu dużej wagi, jakim była awaria systemu DGA na skutek uszkodzenia serwera[30]. Awaria taka miała miejsce w dniu 10 sierpnia 2015 r. i została usunięta w dniu 31 sierpnia 2015 r.
Jak wyjaśnił Z-ca Dyrektora BIiT incydenty bezpieczeństwa administratorów są prowadzone w osobnym rejestrze i nie były przekazywane ze względu na pomocniczy charakter tego rejestru.
Niezależnie od powyższego należy zauważyć, iż wszystkie okazane w trakcie kontroli dokumenty świadczyły o tym, że zarówno incydenty rejestrowane w ramach ZSZ jak i poza tym systemem były obsługiwane i analizowane.
(Dowód: akta kontroli Tom I str. 754)

Ocena cząstkowa

W badanym obszarze NIK ocenia poziom zarządzania procesami zapewnienia bezpieczeństwa systemów jako „powtarzalny, lecz intuicyjny", co zdaniem NIK nie jest wystarczającym i akceptowalnym poziomem zarządzania w badanym obszarze. W ocenie NIK Kierownictwo KRUS poprzez nierzetelną sprawozdawczość wynikającą z niekompletnego systemu rejestrowania incydentów jak i wadliwy miernik procesu zarządzania bezpieczeństwem pozbawione było podstawowego narzędzia monitorowania poziomu bezpieczeństwa informacji. Przyjęty przez KRUS model monitorowania i nadzoru nad realizacją umowy FARMER, w tym poziom bezpieczeństwa przekazanych danych należy uznać, za niewystarczający pod względem organizacyjnym i kadrowym, a co za tym idzie powoduje on wysokie ryzyko, iż usługi świadczone przez wykonawcę mogą nie spełniać wymagań KRUS dotyczących bezpieczeństwa. Zdaniem NIK, ustalony model zarządzania w badanym obszarze powinien powstać na podstawie przeprowadzonej analizy ryzyka i przyjęcia stosownych rozwiązań dostosowanych do akceptowalnego poziomu ryzyka rezydualnego. Pozytywnie należy natomiast ocenić to, że wszystkie zgłoszone incydenty były obsługiwane, analizowane oraz w ich konsekwencji podejmowano działania naprawcze.

3. Stosowanie narzędzi zabezpieczeń

3.1 Zarządzanie kluczami kryptograficznymi

Opis stanu faktycznego

[30] Uszkodzenie serwera było konsekwencją awarii systemu chłodzenia w serwerowni.

W ramach systemu FARMER zabezpieczenia kryptograficzne wykorzystywano w dwóch sytuacjach pomocniczych:

- dystrybucji plików danych dla jednostek KRUS (np. dane statystyczne, dane dla instytucji zewnętrznych) wykorzystywany był serwer „DRUZD" z użyciem protokołu transferu plików FTP,
- dystrybucji formularzy PIT-11 do Ministerstwa Finansów (reguły walidacji i dystrybucji określiło Ministerstwo Finansów).

Stwierdzone nieprawidłowości

Zgodnie z pkt. A.10.1.1 Normy należy opracować i wdrożyć politykę stosowania zabezpieczeń kryptograficznych do ochrony informacji.
W KRUS nie prowadzono analiz dotyczących możliwości wykorzystania zabezpieczeń kryptograficznych w ramach podstawowych danych (funkcjonalności) systemu FARMER. Jak wyjaśnił Prezes KRUS powyższe wynikało ze stosowania innych zabezpieczeń sprzętowych i sieciowych, które zapewniają poufność, autentyczność i integralność informacji.
W procedurach wewnętrznych KRUS nie określono polityki używania zabezpieczeń kryptograficznych oraz zarządzania kluczami kryptograficznymi. Zdaniem NIK powyższa nieprawidłowość pozbawia KRUS realnej możliwości oceny czy zakres stosowania mechanizmów kryptograficznych jest adekwatny do zagrożeń.

(Dowód: akta kontroli Tom I str. 140, 638)

3.2 Ochrona przed złośliwym oprogramowaniem, jego wykrywanie i wprowadzanie poprawek

Opis stanu faktycznego

Ochrona przed złośliwym oprogramowaniem dla wszystkich systemów oraz dla stacji roboczych i serwerów polegała na tym, że:

- Na styku łącza z Internetem funkcjonowały dedykowane systemy firewall w całości zarządzane przez dostawcę usługi WAN;
- Systemy pocztowe zabezpieczone były przed atakami oraz szkodliwymi i niechcianymi przesyłkami za pomocą zastosowania dwóch dedykowanych do tego urządzeń;
- Dostęp do zasobów internetowych dla pracowników zabezpieczony i nadzorowany był za pomocą urządzenia Barracuda Web Filter, które umożliwiało kontrolę zasobów do jakich pracownicy mają dostęp, jak również ochronę przed szkodliwym oprogramowaniem pochodzącym z Internetu;
- Wszystkie stacje robocze oraz serwery plików i aplikacji posiadały centralnie zarządzane oprogramowanie antywirusowe, zapewniające w czasie rzeczywistym bieżącą ochronę komputerów przed szkodliwym oprogramowaniem.

(Dowód: akta kontroli Tom I str. 114)

Sprawność procesu dystrybucji oprogramowania antywirusowego, uaktualnień i definicji była weryfikowana na podstawie przeglądu dziennika zdarzeń CSZO-AV[31]. Centralna konsola zarządzania oprogramowaniem AV obejmowała wszystkie komputery, w tym komputery przenośne. Przegląd taki odbywał się dwa razy w tygodniu. W przypadku wykrycia złośliwego oprogramowania sytuacja taka powinna być odnotowywana w dzienniku incydentów. W okresie objętym kontrolą nie stwierdzono takich zdarzeń. Przypadki automatycznego wykrycia i/lub usunięcia szkodliwego oprogramowania powinny być raportowane z częstotliwością miesięczną.

(Dowód: akta kontroli Tom I str. 115, 340, 629)

Zgodnie z § 44 Instrukcji DO administratorzy systemów informatycznych byli zobowiązani dokonywać okresowych kontroli antywirusowych całego systemu plików

[31] System Zarządzania Oprogramowaniem Antywirusowym

na serwerach poszczególnych systemów informatycznych. Kontrola taka była przeprowadzana raz na miesiąc. W przypadku wykrycia złośliwego oprogramowania fakt ten powinien być odnotowany w dzienniku incydentów. Jak wyjaśnił Prezes KRUS w okresie objętym kontrolą nie wystąpiły przypadki wykrycia złośliwego oprogramowania na serwerach poszczególnych systemów informatycznych.

(Dowód: akta kontroli Tom I str. 116, Tom II str. 102-127)

Zgodnie z § 52 Instrukcji DO Administratorzy systemów informatycznych odpowiedzialni za funkcjonowanie sieci lokalnych dbają o właściwy sposób monitorowania sieci. Do ich zadań należy m.in. systematyczne przeglądanie logów systemowych z serwerów w celu wychwycenia nietypowych zdarzeń.
W trakcie kontroli nie okazano dokumentacji z tych przeglądów. Jak wyjaśnił Prezes KRUS kontrola taka odbywa się nie rzadziej niż raz na miesiąc, a informacja o takim przeglądzie jest generowana tylko w przypadku wykrycia złośliwego oprogramowania, jako incydent w dzienniku incydentów.

(Dowód: akta kontroli Tom I str. 115-116, Tom II str. 124)

3.3 Bezpieczeństwo sieciowe

KRUS eksploatowała sieć w modelu usługowym obsługiwanym przez firmę Orange. Jak wyjaśnił Prezes KRUS, zarządzanie jej konfiguracją leży w gestii Operatora sieci we współpracy z administratorami KRUS na podstawie zawartej umowy na usługi operatorskie sieci WAN. Krytyczne elementy sieci KRUS były monitorowane przez systemy zabezpieczające tj. firewall. Dodatkowo dla usługi świadczonej w sieci publicznej Internet (Portal dla Rolników e-KRUS) uruchomiono usługę dedykowaną dla ochrony przed atakami typu DDoS.
Nieużywane gniazda logiczne w pomieszczeniach użytkowników oraz porty na switch'ach były fizycznie wyłączone. Główna infrastruktura sieciowa zlokalizowana była w dedykowanym pomieszczeniu pod nadzorem, do którego dostęp był ograniczony.
Zasady zarządzania sprzętem sieciowym, zarządzania istotnymi dla bezpieczeństwa elementami sieci nie zostały opracowane. Jak wynika z wyjaśnień Prezesa KRUS spowodowane to było świadczeniem usług operatorskich sieci WAN przez firmę zewnętrzną i uregulowaniem tej kwestii w umowie.

(Dowód: akta kontroli Tom I str. 185-186)

3.4 Ochrona technologii zabezpieczeń

Kopie konfiguracji systemu FARMER przechowywane były przez firmę ZETO na taśmach magnetycznych. W nagłówkach programów wpisywana była historia modyfikacji. Ostatnia wersja programu była oznaczana identyfikatorem programisty, który ją modyfikował oraz czasem zapisu.

(Dowód: akta kontroli Tom I str. 342-343)

Z analizy 4 umów zawartych w latach 2010- 2015[32] wynikało, że umowy z kontrahentami zawierały klauzule zobowiązujące wykonawcę do zachowania poufności informacji uzyskanych w ramach realizowanej umowy.

(Dowód: akta kontroli Tom I str. 635)

---

[32]Umowy: nr 299/2010 z dnia 30 lipca 2010 r. z TP S.A. na usługi operatorskie sieci WAN, nr 202/2014 z dnia 2 stycznia 2015 r. z Blue Energy Sp. z o.o. na usługę asysty technicznej dla oprogramowania DGA, nr 3/2014 z dnia 7 stycznia 2014 r. z firmą Nadikom na świadczenie usługi asysty technicznej dla wdrożonego i eksploatowanego przez Zamawiającego oprogramowania antywirusowego wraz z dwuletnim wsparciem technicznym, nr 114 /2011 z dnia 31 sierpnia 2011 r. z PI ZETO Bydgoszcz S.A. na świadczenie usług informatycznych dotyczących systemu FARMER.

Administratorzy systemu FARMER w ośrodku obliczeniowym mieli pełne uprawnienia do zasobów systemu (system operacyjny, baza danych, oprogramowanie narzędziowe, aplikacja), co oznacza, że mogli sami modyfikować swoje uprawnienia.
W przypadku instalacji nowego sprzętu korzystającego z zasobów sieciowych nie były wykorzystywane hasła domyślne. Login i hasło dla tego sprzętu były nadawane indywidualnie, w momencie uruchomienia włączenia do sieci przez administratorów i przechowywane w aplikacji Active Directory. Przy czym KRUS nie posiadał procedury zmiany domyślnych lub tymczasowych haseł na instalowanym sprzęcie.

(Dowód: akta kontroli Tom I str. 663)

Ocena cząstkowa

W badanym obszarze NIK ocenia poziom zarządzania procesami zapewnienia bezpieczeństwa systemów jako „zdefiniowany". Przy formułowaniu oceny wzięto pod uwagę, że część badanych zagadnień została przekazana wykonawcom w umowach outsourcingowych, a co za tym idzie nie mogła podlegać ocenie NIK. Niemniej jednak w badanym obszarze aktualne pozostają przedstawione w pkt. 1.6 uwagi NIK dotyczące zarządzania ryzkiem w zakresie bezpieczeństwa w przypadku powierzenia usług firmie zewnętrznej.

4. Zarządzanie tożsamością

4.1 Zobowiązanie pracowników do zachowania poufności

Opis stanu faktycznego

W KRUS wprowadzono obowiązek pracowników do złożenia oświadczenia o zachowaniu w poufności zdobytych informacji. Zobowiązania te nie obejmowały jednakże okresu po ustaniu zatrudnienia. Sprawdzono 10 pracowników Biura Informatyki i Telekomunikacji pod ww. kątem. Wszystkie skontrolowane teczki akt osobowych zawierały takie oświadczenia. Ponadto klauzula o zobowiązaniu do dochowania tajemnicy została we wszystkich przypadkach zawarta w podpisanej przez pracownika karcie czynności. Stwierdzono jeden przypadek złożenia oświadczenia 27 dni po uzyskaniu przez niego dostępu do zasobów KRUS.

(Dowód: akta kontroli Tom I str. 643)

4.2 Zarządzanie kontami użytkowników i przegląd uprawnień

Kwestie zarządzania kontami w tym wnioskowania, ustanawiania, wydawania i modyfikacji uprawnień uregulowane były w Procedurze zarządzania kontami użytkowników. Zawarto w niej również obowiązek dokonywania przez dyrektorów przeglądu aktualności nadanych podległym pracownikom uprawnień do systemów informatycznych. Informacje z tych przeglądów należało przesłać do Dyrektora BIiT w terminach 31 lipca (I półrocze) i 31 stycznia (II półrocze).

Stwierdzone nieprawidłowości

W okresie objętym kontrolą do dnia 16 czerwca 2015 r. brak było uregulowań w zakresie obowiązkowych przeglądów uprawnień. Do dnia 19 października 2015 r. przegląd, na podstawie nowych regulacji nie został przeprowadzony pomimo upływu wskazanego w procedurze terminu 31 lipca.
Jak wyjaśnił Prezes KRUS przeglądy uprawnień do pracy w systemach informatycznych KRUS wynikały z dobrych praktyk i były dokonywane średnio raz w miesiącu z wykorzystaniem Portalu dla pracowników w ramach systemu informatycznego Workflow. W trakcie kontroli nie okazano dokumentacji potwierdzającej przeprowadzanie tych przeglądów lub zawierającej ich wyniki.
Przyjmując przytoczone powyżej wyjaśniania należy zauważyć, że dokonywane w ramach systemu Workflow[33] przeglądy uprawnień nie mogły obejmować wszystkich systemów wykorzystywanych w KRUS, a jedynie systemy objęte zredukowanym logowaniem np. nSIU, Archiwum. W przypadku systemu FARMER KRUS nie miała

[33] Ustalono, że za pomocą systemu Workflow istnieje możliwość przeglądu uprawnień poprzez: raportowanie uprawnień dla konkretnego użytkownika, porównywanie uprawnień pary wybranych użytkowników, raportowanie uprawnień dla jednostki organizacyjnej.:

możliwości podglądu uprawnień nadanych w tym systemie, a w celu dokonania weryfikacji aktualności nadanych uprawnień musiała się zwrócić z wnioskiem do Wykonawcy. Możliwość przeglądu uprawnień systemu FARMER za pomocą systemu Workflow ma zostać wdrożona po integracji tych systemów, co planowe jest w ramach nowej (3 wersji) tego systemu.

(dowód: akta kontroli Tom I str. 194-221, 655, 657)

Opis stanu faktycznego

Kontrola zgodności przechowywania haseł administracyjnych z procedurami wewnętrznymi, w szczególności z Wytycznymi Dyrektora BliT dla Administratorów Systemów Informatycznych w sprawie przechowywania i prowadzenia Rejestru aktualizacji haseł administratorów, nie wykazała nieprawidłowości.

(Dowód: akta kontroli Tom I str. 192, 645-646)

4.3 Logowanie do systemów

Dostęp do systemu FARMER był dwuetapowy.

- W pierwszym etapie należało się zalogować do domeny. Utworzenie konta użytkownika w domenie następowała z wykorzystaniem oprogramowania do zarządzania tożsamością Oracle Identity Manager – aplikacja Portal dla pracowników systemu Workflow.

  Po zarejestrowaniu pracownika w systemie Saturn HR automatycznie tworzy się konto w domenie, która daje dostęp do poczty, aplikacji service-desk oraz DGA Quality. Poszerzenie uprawnień pracownika o automatyczny dostęp do systemów nSIU, Archiwum, KRH docelowo również dla FARMERA3 następowała na wniosek przełożonego.
  Powyższe rozwiązania powodowały, że bezpośrednio po ustaniu stosunku pracy, (co zostaje zaznaczone w systemie Saturn), blokowany był dostęp do domeny. Analiza 25 przypadków osób, które odeszły z pracy w okresie objętym kontrolą nie wykazała opóźnień w odbieraniu uprawnień do nSIU, Archiwum, KRH.

- W drugim etapie użytkownik logował się do systemu FARMER. Dostęp uwierzytelniany był przez login i hasło. Na potrzeby kontroli, zwrócono się o utworzenie loginu i przydzielenie hasła do systemu w celu weryfikacji wymuszania przez system narzuconych warunków na hasło. Sprawdzenia dokonano w dniu 2 października na komputerze pani Wicedyrektor Biura Świadczeń - Anny Grabowskiej.

(Dowód: akta kontroli Tom I str. 667-678)

Stwierdzone nieprawidłowości

Stwierdzono niezgodność przyjętej maski hasła dostępu do systemu FARMER z Instrukcją podstawowych zasad bezpieczeństwo dla pracowników KRUS (pkt. 5.5). Hasło dostępu do systemu FARMER jako przetwarzającego dane osobowe musi składać się z trzech grup znaków z grup: mała litera, wielka litera, cyfra, znak specjalny, a składało się z dwóch grup – litery i cyfry[34]. Ponadto stwierdzono, że po ośmiokrotnym wprowadzeniu błędnego hasła konto nie zostało zablokowane, pomimo, że hasło zgodnie z uzyskanymi informacjami powinno blokować się po pięciokrotnym błędnym wprowadzeniu. Zgodnie z wyjaśnieniami Dyrektora BliT *za blokowanie konta w systemie FARMER odpowiada moduł „Natural Security". W konfiguracji dotychczas implementowanej różnie interpretował on próbę nieudanego logowania. Po stwierdzeniu tego faktu zmieniono jego konfigurację tak, że w chwili obecnej konto użytkownika jest blokowane po trzech nieudanych próbach logowania.*
Powyższe wyjaśnienia - blokady konta po trzeciej, nieudanej próbie zalogowania - zostały potwierdzone przez Kontrolera w dniu 6 października 2015 r.

(dowód: akta kontroli Tom I str. 662, 682, 687)

[34] System nie rozróżniał wielkich i małych liter oraz znaków specjalnych.

Opis stanu faktycznego

Uprawnienia pozwalające na odczyt informacji z systemu FARMER miało w Centrali KRUS 8 osób - pracowników Biura Świadczeń. Terminowość odbierania uprawnień w tym systemie sprawdzono na przykładzie:

- Pracownika Centrali, który odchodził z pracy w okresie objętym kontrolą i posiadał uprawnienia do systemu FARMER – uprawnienia zostały odebrane po 4 dniach od odejścia z pracy.
- Listy 14 pracowników, którzy odeszli z pracy w okresie objętym kontrolą z Oddziału Regionalnego KRUS w Warszawie. Kontrola nie stwierdziła aktywnych kont[35].

Ponadto sprawdzono terminowość odbierania uprawnień do systemu Saturn (w całości utrzymywanego przez KRUS) na przykładzie dwóch osób, które odeszły z pracy w okresie objętym kontrolą oraz jednej osoby która była długotrwale nieobecna w pracy. Kontrola nie wykazała opóźnień.

(Dowód: akta kontroli Tom I str. 680, 684-688)

4.4 Zawieszanie uprawnień w przypadku dłuższej nieobecności.

W KRUS nie uregulowano kwestii zawieszania uprawnień w przypadku długotrwałych nieobecności. Uprawnienia w części takich przypadków nie były odbierane. Na przykładzie 4 osób długotrwale nieobecnych w pracy stwierdzono trzy przypadki aktywnego konta w systemie Workflow pomimo, absencji trwającej od 23 miesięcy, poprzez 13 miesięcy, do 3 miesięcy. W jednym przypadku pracownika BliT konto w tym systemie zostało zawieszone bez opóźnienia.

W trakcie kontroli sprawdzono także zawieszanie uprawnień w systemie Saturn HR (administrowane przez Biuro Kadr i Szkolenia). Konto zostało zawieszone bez opóźnienia.

(dowód: akta kontroli Tom I str. 681, 687, 668,715)

Stwierdzone nieprawidłowości

Taki stan rzeczy (aktywne konto pomimo blisko dwuletniej nieobecności) wynika, w ocenie NIK, z braku uregulowań w zakresie zawieszania uprawnień (w szczególności braku obowiązku informowania administratorów o długotrwałej nieobecności), jak również z braku wypracowania dobrych praktyk w tym zakresie. Zdaniem NIK ustalenia kontroli potwierdzają, że poszczególni administratorzy mieli świadomość istotności niezwłocznego zawieszania uprawnień (świadczy o tym bezzwłoczne zawieszanie uprawnień dla pracowników tej samej jednostki organizacyjnej co administratorzy systemów) i dokonywali tego w sposób intuicyjny. Wg NIK wskazany wyżej stan faktyczny potwierdza zasadność wprowadzenia uregulowań kwestii zawieszania uprawnień.

Ocena cząstkowa

Stwierdzone w ww. obszarze nieprawidłowości w istotny sposób obniżały bezpieczeństwo informacji KRUS, dlatego też w badanym obszarze NIK ocenia poziom zarządzania procesami zapewnienia bezpieczeństwa systemów jako „powtarzalny, lecz intuicyjny". NIK dostrzegła jednakże wprowadzane zmiany, w tym zmiany systemowe (centralizacja zasobów, integracja poszczególnych systemów z modułem OIM), zmierzające do wyeliminowania niektórych nieprawidłowości.

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 o NIK, wnosi o:

1. Przeprowadzenie kwerendy obowiązujących procedur zmierzającej do dalszego ich udoskonalenia, zwiększenia czytelności, integralności i kompletności.

[35] Jak wspomniano powyżej w KRUS nie ma możliwości podglądu uprawnień do systemu Farmer, dane w tym zakresie opierają się na informacjach uzyskanych od ZETO Bydgoszcz.

2. Podjęcie czynności zmierzających do wzmocnienia nadzoru nad realizacją umów w modelu outsourcingu w powiązaniu z rzetelną analizą ryzyka w tym obszarze.
3. Wypracowanie rzetelnego narzędzia monitorowania bezpieczeństwa informacji poprzez uszczelnienie i ujednolicenie systemu gromadzenia informacji o incydentach bezpieczeństwa przy jednoczesnej modyfikacji miernika procesu zarządzania bezpieczeństwem informacji.
4. Podjęcie skutecznych działań na rzecz systematycznego i rzetelnego przeprowadzania przeglądu adekwatności uprawnień.
5. Kontynuowanie działań zmierzających do zbudowania pełnego wykazu aktywów wspierających.

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 09.12.2015r.

Prezes
Najwyższej Izby Kontroli
Krzysztof Kwiatkowski

.....
podpis