PREZES
NAJWYŻSZEJ IZBY KONTROLI
Krzysztof Kwiatkowski

KPB.410.004.04.2015
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 Szymańska, specjalista kontroli państwowej, upoważnienie do kontroli nr 93498 z dnia 1 czerwca 2015 r.

(dowód: akta kontroli Tom I str. 1-2)

2. Anna Mach, główny specjalista kontroli państwowej, upoważnienie do kontroli nr 93499 z dnia 1 czerwca 2015 r.

(dowód: akta kontroli Tom I str. 3-4)

3. Łukasz Garbień, doradca prawny, upoważnienie do kontroli nr 95758 z dnia 4 sierpnia 2015 r.

(dowód: akta kontroli Tom I str. 5-6)

Jednostka kontrolowana

Narodowy Fundusz Zdrowia - Centrala (dalej: NFZ lub Fundusz)
ul. Grójecka 168, 02-300 Warszawa

Kierownik jednostki kontrolowanej

Prezesem Narodowego Funduszu Zdrowia od dnia 3 czerwca 2014 r. jest Tadeusz Jędrzejczyk. Uprzednio funkcję Prezesa NFZ pełnili Marcin Pakulski (od 23 grudnia 2013 r. do 28 lutego 2014 r.) oraz Wiesława Anna Kłos (od 1 marca 2014 r. do 2 czerwca 2014 r.).

(dowód: akta kontroli Tom I str. 9)

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 Centrali NFZ jako „powtarzalne lecz intuicyjne".

Uzasadnienie oceny ogólnej

W kontrolowanej jednostce istnieje świadomość potrzeby zapewnienia bezpieczeństwa teleinformatycznego, jednak jest ona fragmentaryczna i ograniczona. Rozwijana jest polityka dotycząca bezpieczeństwa, ale nie towarzyszą jej adekwatne narzędzia. Chociaż systemy dostarczają informacji dotyczących bezpieczeństwa, dane te nie są analizowane. Bezpieczeństwo IT jest postrzegane głównie, jako przedmiot odpowiedzialności i domena działu IT, a nie zadanie leżące w gestii całego Funduszu.

W ocenie NIK brak jednolitego i kompleksowego systemu zarządzania bezpieczeństwem informacji w Centrali NFZ utrudniał właściwą ich ochronę.

[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.

Nieaktualizowanie od 2010 r.[2] regulacji dotyczących bezpieczeństwa danych przetwarzanych w NFZ powodowało, że stosowane rozwiązania nie nadążały za zmianami w systemie prawnym, a w konsekwencji również mogły przyczyniać się do osłabienia tej ochrony. W tym kontekście Izba pozytywnie ocenia podjęte przez Fundusz działania w celu opracowania i wdrożenia[3] Zintegrowanego Systemu Zarządzania łączącego System Zarządzania Ryzykiem, System Zarządzania Bezpieczeństwem Informacji oraz System Zarządzania Ciągłością Działania.

Stwierdzone przez NIK nieprawidłowości dotyczyły również:

- braku zastępowalności na kluczowym dla bezpieczeństwa i monitoringu systemów teleinformatycznych stanowisku,
- braku jednego zcentralizowanego rejestru incydentów,
- niezgodnego z wewnętrznymi uregulowaniami przekazywania informacji o dłuższych absencjach do odpowiednich komórek organizacyjnych.

III. Opis ustalonego stanu faktycznego

1. Wspieranie bezpieczeństwa IT na poziomie całej organizacji

1.1. Zarządzanie bezpieczeństwem IT

Opis stanu faktycznego

1. Zgodnie z zarządzeniem Nr 15/2015/GPF Prezesa Narodowego Funduszu Zdrowia z dnia 24 marca 2015 r. w sprawie regulaminu organizacyjnego Centrali Narodowego Funduszu Zdrowia[4] Departamentowi Informatyki (dalej: DI) przypisano kompetencje i odpowiedzialność związaną z budową, utrzymaniem i rozwojem systemów informatycznych Funduszu oraz budową, utrzymaniem i rozwojem infrastruktury teleinformatycznej Centrali NFZ, a także promowaniem i wprowadzaniem nowych technologii teleinformatycznych.

Zgodnie z §35 ust. 2 pkt 24 załącznika nr 1 do zarządzenia Nr 15/2015/GPF do podstawowych zadań DI należy w szczególności zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, o którym mowa w § 20 ust. 2 pkt 12 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[5] (dalej: rozporządzenie KRI).

Zadania DI zostały doprecyzowane w wewnętrznym regulaminie organizacyjnym Departamentu Informatyki[6], zatwierdzonym przez Prezesa NFZ w dniu 2 października 2013 r.

(dowód: akta kontroli Tom IV str. 26-39)

Do dnia zakończenia kontroli w Centrali NFZ funkcjonowało samodzielne stanowisko ds. bezpieczeństwa systemów teleinformatycznych. Do jego zdań należało w szczególności: współpraca z Pełnomocnikiem Ochrony Informacji Niejawnych (dalej: POIN) i Administratorem Bezpieczeństwa Informacji (dalej: ABI),

---

[2] Wprowadzone Zarządzeniem Nr 12/2010/POIN Prezesa NFZ z dnia 29 stycznia 2010 r. w sprawie bezpieczeństwa danych przetwarzanych w Narodowym Funduszu Zdrowia.

[3] Zgodnie z harmonogramem projektu wdrożenia ZSZ przeprowadzenie pełnego wdrożenia ZSZ planowane jest do końca 2016 r.

[4] Uprzednio obowiązywało zarządzenie nr 36/2013/GPF Prezesa Narodowego Funduszu Zdrowia z dnia 2 lipca 2013 r.

[5] Dz. U. z 2012 r., poz. 526 ze zm.

[6] Szczegółowy zakres działania komórek organizacyjnych Centrali NFZ został określony przez Prezesa NFZ na podstawie § 2 ust. 1 zarządzenia Nr 36/2013/GPF.

ciągły przegląd i nadzór nad implementacją technicznej warstwy bezpieczeństwa systemów teleinformatycznych, zarządzanie obsługą bezpieczeństwa na poziomie DI, cykliczny audyt systemów dziedzinowych zabezpieczanie materiału dowodowego z incydentów w obszarze bezpieczeństwa ICT we współpracy z POIN oraz analiza techniczna zebranego materiału dowodowego. Pracownik posiadał uprawnienia m.in. do wydawania poleceń wstrzymania się od dalszych działań w systemach informatycznych NFZ pracownikowi Funduszu lub innej osobie faktycznie działającej w systemie informatycznym NFZ, jeśli dalsze działania mogłyby prowadzić do naruszenia bezpieczeństwa tych systemów lub umożliwić zatarcie dowodów znajdujących się w systemach informatycznych.

(dowód: akta kontroli Tom IV str. 37-38)

W przedłożonym projekcie nowego regulaminu organizacyjnego Departamentu Informatyki w strukturze organizacyjnej DI wyszczególniono Sekcję ds. Bezpieczeństwa i Audytu Systemów Teleinformatycznych. W dokumencie tym nie sprecyzowano składu ww. Sekcji.

(dowód: akta kontroli Tom IV str. 40-54)

W dniu 15 czerwca 2015 r. rozwiązano stosunek pracy z kierownictwem Departamentu Informatyki. W związku z powyższym od dnia 16 czerwca 2015 r. p.o. Dyrektora DI jest Marcin Grabowski, a od dnia 24 czerwca 2015 r. p.o. Zastępcy Dyrektora DI jest Adam Kiersnowski.

(dowód: akta kontroli Tom I str. 15-29)

2. W dniu 4 czerwca 2014 r. Centrala NFZ zawarła z konsorcjum firm Blue Energy Sp. z o.o. i DGA Sp. z o.o. umowę na doradztwo w zakresie opracowania oraz wdrożenia systemów: zarządzania bezpieczeństwem informacji (SZBI), zarządzania ryzykiem korporacyjnym (SZRK) oraz zarządzania ciągłością działania (SZCD). SZBI zgodny z normą ISO/IEC 27001 – ujęty w modelu PDCA obejmującym etapy planowania, wykonywania, sprawdzenia oraz doskonalenia – będzie wdrażany (zgodnie z harmonogramem projektu ZSZ oraz równolegle z SZCD, zgodnym z normą ISO/IEC 22301), pilotażowo w Centrali NFZ oraz ośmiu oddziałach wojewódzkich w III i IV kwartale 2015 r. oraz I kwartale 2016 r., a następnie w całej organizacji.

(dowód: akta kontroli Tom I str. 41-64, 208)

W ramach projektu ZSZ została opracowana metodyka analizy ryzyka oraz zostało zapewnione wsparcie narzędzia informatycznego klasy BMP. Jak wyjaśnił p.o. dyrektora Departamentu Informatyki NFZ analiza ryzyka utraty atrybutów informacji (poufności, dostępności oraz integralności oraz ryzyka utraty ciągłości działania) zostanie przeprowadzona w IV kwartale 2015 r.

(dowód: akta kontroli Tom I str. 35, 305-340, 362-481)

W Raporcie z oceny ryzyka w Centrali Narodowego Funduszu Zdrowia z dnia 6 lipca 2015 r. zidentyfikowano 309 ryzyk[7], które wpływają lub mogą negatywnie wpłynąć na realizację działań poszczególnych komórek organizacyjnych NFZ. Wśród zidentyfikowanych ryzyk wskazano m.in. ataki hackerskie, spamerskie i typu DDoS, brak zastępowalności i braki kadrowe, nieefektywny przepływ informacji między komórkami organizacyjnymi, nieuprawniony dostęp do informacji, a także niezgłaszanie incydentów lub niepoprawne zarządzanie incydentami.

(dowód: akta kontroli Tom I str. 362-481)

[7] 239 ryzyk o niskiej wartości, 57 ryzyk o średniej wartości i 13 ryzyk o wysokiej wartości.

P.o. dyrektora DI NFZ podał, że *„W ramach zadań Gabinetu Prezesa Funduszu pracownicy informowani są o zagrożeniach wynikających z dużej ilości danych osobowych przetwarzanych w ramach systemów informatycznych Funduszu, kładzie się przy tym nacisk na rodzaj informacji przekazywanych przy wykorzystaniu poczty elektronicznej oraz rozmów telefonicznych"*.

Każdemu z pracowników przekazano Regulamin ochrony danych osobowych oraz każdy pracownik podpisał zobowiązanie do zachowania w tajemnicy danych przetwarzanych przez NFZ wraz ze sposobami ich zabezpieczenia.

(dowód: akta kontroli Tom I str. 133, 207, 210)

3. W NFZ funkcjonuje m.in. Centralny Wykaz Ubezpieczonych, w ramach którego funkcjonują następujące systemy:

1) CWU – Centralny Wykaz Ubezpieczonych,
2) CWPOZ – Centralny Wykaz POZ,
3) SIMP – System Informatyczny Monitorowania Profilaktyki,
4) SMPT – System Monitorowania Programów Terapeutycznych,
5) eWUŚ – Elektroniczna Weryfikacja Uprawnień Świadczeniobiorców.

(dowód: akta kontroli Tom I str. 244)

Ustalone nieprawidłowości

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

1. W Centrali NFZ nie dokonano oszacowania kosztów (w tym również niematerialnych) ewentualnego naruszenia bezpieczeństwa informacji istotnych dla realizowanych przez NFZ zadań, tj. ich poufności, integralności i dostępności. Ponadto, w Centrali NFZ nie jest prowadzona klasyfikacja aktywów, w związku z powyższym nie mają one przyporządkowanych parametrów istotności i poziomów ochrony.

(dowód: akta kontroli Tom I str. 523-528, Tom II str. 3)

Prezes NFZ wyjaśnił, że przyczyną powyższego było wstrzymanie do marca 2014 r.[8] prac związanych z realizacją postępowania o zamówienie publiczne mające na celu wyłonienie podmiotu zewnętrznego, który świadczyłby na rzecz Narodowego Funduszu Zdrowia usługę doradztwa eksperckiego w zakresie opracowania i wdrożenia w Funduszu Zintegrowanego Systemu Zarządzania obejmującego między innymi System Zarządzania Bezpieczeństwem Informacji.

Prezes NFZ podał, że *„Proces szacowania kosztów (w tym niematerialnych) ewentualnego naruszenia bezpieczeństwa informacji, musi zostać poprzedzony co najmniej identyfikacją aktywów informacyjnych, klasyfikacją i wartościowaniem informacji oraz oceną ryzyka utraty podstawowych atrybutów informacyjnych tj. poufności, integralności i dostępności. Wymienione działania stanowią bardzo istotny element, czy wręcz kluczowy element systemu Zarządzania Bezpieczeństwem Informacji. W świetle wstrzymania prac związanych z wdrożeniem [ZSZ] w Narodowym Funduszu Zdrowia, przeprowadzenie tego typu*

[8] Tj. do czasu upoważnienia przez Ministra Zdrowia Pani Wiesławy Kłos do zastępowania Prezesa Narodowego Funduszu Zdrowia. Pani Wiesława Kłos zastępująca Prezesa NFZ podjęła decyzję o kontynuowaniu projektu ZSZ.

działań oznaczałoby, że albo zakres przedmiotowy określony w Specyfikacji Istotnych Warunków Zamówienia (Szczegółowy Opis Przedmiotu Zamówienia) został zdefiniowany nadmiarowo ponieważ zasoby własne Funduszu pozwalają na przeprowadzenie klasyfikacji informacji i oceny ryzyka utraty bezpieczeństwa informacji albo, że doszłoby do niezgodnego z ustawą prawo zamówień publicznych podziału zamówienia publicznego (...) W związku z powyższym nie było możliwości oszacowania kosztów utraty bezpieczeństwa informacji nie kontynuując bądź nie unieważniając trwającego postępowania o zamówienie publiczne."

(dowód: akta kontroli Tom IV str. 511-512)

Nieprzypisanie informacjom odpowiedniego poziomu ochrony, zgodnego z ich wagą dla Centrali NFZ NIK ocenia jako nierzetelne. Na konieczność dokonania klasyfikacji informacji z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację, a także opracowania zbioru procedur oznaczania informacji wskazuje pkt. 8.2 normy PN-ISO/IEC 27005.

2. Zgodnie z przedłożonym zakresem obowiązków, pan Mariusz K. pracujący na samodzielnym stanowisku ds. bezpieczeństwa systemów teleinformatycznych był zastępowany przez pana Macieja G. - od dnia 1 października 2015 r nie będącego pracownikiem Centrali NFZ.

(dowód: akta kontroli Tom IV str. 64-69)

Prezes NFZ podał m.in., że „*Przyczyną nie zaktualizowania zakresu obowiązków pana Mariusza [K.] od 1 października 2015 r., odnośnie wskazania innej osoby zastępującej były prace koncepcyjne nad zmianami organizacyjnymi Departamentu Informatyki i niejasna sytuacja co do kształtu struktury organizacyjnej. Ostatecznie w dniu 30.10.2015 r. powstała nowa struktura organizacyjna, zgodnie z którą zakres obowiązków pana Mariusza [K.] zostanie niezwłocznie przygotowany.*"

(dowód: akta kontroli Tom IV str. 524)

Zgodnie z przedłożonym zakresem obowiązków dla Macieja G. do zakresu jego zadań należało przede wszystkim:

- instalacja i administrowanie serwerami platformy Windows wraz z urządzeniami peryferyjnymi, administracja profilami dostępowymi użytkowników w środowisku Windows, administracja ośrodkami przetwarzania danych;
- administrowanie systemami bezpieczeństwa i monitoringu w obszarze środowiska serwerów Windows wraz z urządzeniami peryferyjnymi oraz zapewnienie wymaganej dostępności aplikacji użytkowych oraz właściwego poziomu bezpieczeństwa w obszarze środowiska serwerów Windows, zgodnie regulacjami wewnętrznymi NFZ, regulacjami instytucji nadzorczych oraz standardami IT;
- rozwiązywanie problemów i usuwanie awarii, jakie wystąpiły w administrowanym przez pracownika obszarze oraz pomoc w rozwiązywaniu problemów użytkowników, jako druga linia wsparcia dla Sekcji Monitoringu i Wsparcia Informatycznego.

(dowód: akta kontroli Tom IV str. 64-69)

Zdaniem NIK brak zastępowalności pracownika na jednym z kluczowych stanowisk dla bezpieczeństwa i monitoringu systemów teleinformatycznych Centrali NFZ mógł w istotny sposób przyczynić się do obniżenia poziomu bezpieczeństwa. Pozytywnie należy ocenić w tym kontekście powołanie Sekcji ds. Bezpieczeństwa i Audytu Systemów Teleinformatycznych, dzięki czemu w przypadku wystąpienia zagrożenia

bezpieczeństwa systemów informatycznych zminimalizowane zostanie ryzyko nieobecności osoby władnej do podjęcia stosownych działań.

1.2. Plan zapewnienia bezpieczeństwa IT

Opis stanu faktycznego

Stosownie do § 20 ust. 2 pkt 1 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań, obejmujących zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.

Obowiązujące w badanym okresie zasady dotyczące bezpieczeństwa danych przetwarzanych w NFZ zostały wprowadzone zarządzeniem Nr 12/2010/POIN Prezesa NFZ z dnia 29 stycznia 2010 r. w sprawie bezpieczeństwa danych przetwarzanych w Narodowym Funduszu Zdrowia. Załącznik nr 1 do ww. Zarządzenia stanowiła Polityka Bezpieczeństwa NFZ (dalej: PB), zaś Załącznik nr 2 – Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w NFZ (dalej: Instrukcja). Regulacje te nie były aktualizowane.

Z wyjątkiem ww. zarządzenia Nr 12/2010/POIN w Centrali NFZ nie wdrożono żadnych procedur w zakresie bezpieczeństwa systemów teleinformatycznych dla całej organizacji.

(dowód: akta kontroli Tom I str. 79-123)

W Instrukcji ujęto w szczególności:

- procedury nadawania i rejestrowania uprawnień do przetwarzania danych w systemie informatycznym,
- stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem,
- procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników,
- procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,
- przechowywanie i niszczenie nośników danych w formie papierowej i elektronicznej,
- sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
- procedury wykonywania przeglądów i konserwacji, usuwania awarii systemów oraz nośników danych służących do przetwarzania danych.

(dowód: akta kontroli Tom III str. 19-55)

W Centrali NFZ stosowano również Księgę Procedur Departamentu Informatyki, która nie została zatwierdzona formalnie. Księga obejmowała następujące procedury (wraz z instrukcjami): zarządzanie uprawnieniami i zmianami haseł (PDI-01), wykonywanie kopii zapasowej i archiwów danych (PDI-02), zarządzanie helpdeskiem (PDI-03), zarządzanie serwerami (PDI-04), zarządzanie sieciowymi elementami aktywnymi i pasywnymi (PDI-05), zabezpieczenie i monitorowanie sieci wewnętrznej i zewnętrznej przed atakami (PDI-06), polityki antywirusowe i antyspamowe (PDI-07), używanie skrzynek pocztowych i aliasów (PDI-08), korzystanie z urządzeń mobilnych (PDI-09), zasady dostępu użytkowników do Internetu (PDI-10), dostęp do sieci wewnętrznej z Internetu (PDI-11), zakup licencji dla oprogramowania zakupionego na potrzeby Centrali i Oddziałów Wojewódzkich

NFZ (PDI-12) i komunikacja w przypadku wystąpienia awarii systemów informatycznych (PDI-13).

(dowód: akta kontroli Tom IV str. 1-4)

Pracownikom Centrali NFZ przekazywano drogą elektroniczną skany pism dotyczące pouczeń o obligatoryjnym przestrzeganiu zarządzenia nr 12/2010/POIN oraz regulaminu organizacyjnego w zakresie odpowiedzialności poszczególnych pracowników komórek organizacyjnych.

(dowód: akta kontroli Tom I str. 511-512)

Ustalone nieprawidłowości

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

1. W NFZ brak jest całościowej polityki bezpieczeństwa informacji. Zarządzenie nr 12/2010/POIN przyjęte zostało w celu zapewnienia bezpieczeństwa informacji zgodnie z wymaganiami:

1) ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[9],
2) 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[10],
3) ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych[11],
4) Generalnego Inspektora Ochrony Danych Osobowych,
5) Polskich Norm PN-ISO/IEC 27001 i PN-I-13335-1:1999[12].

W § 2 ust. 3 pkt. 2 zarządzenia Nr 12/2010/POIN zawarto zapis, że w sprawach nie uregulowanych w zarządzeniu mają zastosowanie zasady zarządzania bezpieczeństwem informacji ujęte w Polskiej Normie PN-ISO/IEC 27001:2007.

W ocenie NIK zarządzenie 12/2010/POIN jest, poza obszarem bezpieczeństwa danych osobowych, niezgodne z wymogami § 20 ust. 1 rozporządzenia KRI.

(dowód: akta kontroli Tom I str. 79-134)

Księga Procedur Departamentu Informatyki oraz ujęte w niej procedury i instrukcje nie zostały zatwierdzone przez Prezesa NFZ, tym samym obowiązują jedynie Departament Informatyki.

(dowód: akta kontroli Tom IV str. 1-4)

Jak wyjaśnił p.o. Dyrektora DI *„Księga Procedur powstała w okresie, w którym obecny pion aplikacji* [DI] *znajdował się w strukturze Departamentu Świadczeń Opieki Zdrowotnej, w związku z czym została wdrożona tylko w pionie eksploatacji. Po ponownym przyłączeniu pionu aplikacji do* [DI] *postanowiono, że w związku z realizowanym projektem wdrożenie* [ZSZ] *pozostałe procedury zostaną wdrożone w trakcie projektu tak aby zawrzeć w nich wytyczne powstałe podczas prac projektu. Pozostałe, istniejące już procedury będą modyfikowane zgodnie z ww. wytycznymi oraz w związku ze zmianami regulaminu organizacyjnego Centrali NFZ. W ramach projektu ZSZ wdrożone zostanie System Zarządzania Bezpieczeństwem Informacji,*

---

[9] W brzmieniu Dz. U. z 2002 r. Nr 101 poz. 926 ze zm.

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

[11] W brzmieniu Dz. U. z 2008 r. Nr 164, poz. 1027 ze zm..

[12] Systemy zarządzania bezpieczeństwem informacji oraz Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych.

który obejmie cały [NFZ], *dlatego wymagane w nim procedury również będą obejmowały cały Fundusz."*

(dowód: akta kontroli Tom I str. 230-231)

Ponadto, obowiązujące w badanym okresie ww. zasady dotyczące bezpieczeństwa danych przetwarzanych w NFZ nie były aktualizowane, co stanowiło naruszenie wymogów określonych w § 20 ust. 2 pkt 1 rozporządzenia KRI. Zgodnie z cyt. przepisem zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.

(dowód: akta kontroli Tom I str. 79-134)

W Centrali NFZ, zdaniem NIK, brak skutecznie działającego systemu zarządzania bezpieczeństwem informacji, co należy ocenić jako działanie nierzetelne i wskazujące na niespełnienie wymogu określonego w § 20 ust. 1 KRI według którego podmiot realizujący zadania publiczne opracowuje i ustanawia, utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji.

1.3. Testowanie nadzorowanie i monitorowanie bezpieczeństwa

Opis stanu faktycznego

1. W dniu 8 marca 2013 r. zakończył się audyt bezpieczeństwa systemu eWUŚ przeprowadzony przez IMMUSEC Sp. z o.o. Celem audytu była ocena bezpieczeństwa systemu informatycznego eWUŚ wykorzystywanego przez NFZ oraz wskazanie luk bezpieczeństwa, które mogą stanowić zagrożenie dla bezpieczeństwa informacji przetwarzanych przez Fundusz. Zakres prac audytowych obejmował analizę bezpieczeństwa i odporności systemu eWUŚ na ataki z wewnątrz oraz z zewnątrz sieci informatycznej oraz analizę podatności oraz testy penetracyjne systemu.

Przeprowadzone testy wykazały, że aplikacja eWUŚ jest podatna na znane błędy bezpieczeństwa oraz ujawniły istnienie ryzyk w obszarze bezpieczeństwa informacji.

W dniu 18 czerwca 2013 r. IMMUSEC Sp. z o.o. przeprowadziła powtórny audyt systemu eWUŚ, którego celem była weryfikacja wdrożenia rekomendacji przedstawionych w dokumencie z dnia 8 marca 2013 r.

Weryfikacji poddano 25 podatności w zakresie ich usunięcia poprzez wdrożenie rekomendacji z audytu. Na podstawie wykonanych prac stwierdzono, że w całości usunięto 28% podatności systemu, częściowo usunięto 32% podatności a nie usunięto 40% podatności.

(dowód: akta kontroli Tom I str. 344-352, Tom III str. 228-227)

W sporządzonym przez DI zestawieniu wskazano, że po przeprowadzeniu analizy wskazanych podatności i po otrzymaniu uwag dostawcy systemu uznano, że przyjęte w Centrali NFZ mechanizmy ochrony systemów informatycznych są wystarczające do zapewnienia ich bezpieczeństwa.

(dowód: akta kontroli Tom I str. 353-356)

W odniesieniu do weryfikowania prawidłowości wyników działania systemu eWUŚ Prezes NFZ podał m.in., że *„w aplikacji zaimplementowana jest funkcjonalność automatycznych blokad, które uruchamiane są w przypadku 5 nieudanych prób logowań lub po przekroczeniu limitu logowań w jednostce czasu (500 na godzinę). Rejestr udanych/nieudanych prób logowania oraz uruchomionych blokad użytkowników stanowią logi systemu. Analiza logów została wdrożona bezpośrednio w aplikacji w celu natychmiastowego zablokowania dostępu do systemu*

użytkownikom, których działania sklasyfikowano jako potencjalne zagrożenie. Doraźnych analiz udanych/nieudanych prób logowania dokonuje Dostawca oprogramowania po otrzymaniu zlecenia na podstawie otwartej konsultacji."

W toku kontroli nie przedłożono dokumentów potwierdzających udzielone wyjaśnienia.

(dowód: akta kontroli Tom IV str. 513)

W Centrali NFZ prowadzone są przez DI analizy rejestrów zapytań eWUŚ, w celu zidentyfikowania nieprawidłowości niektórych programów świadczeniodawców. Na stronie internetowej Narodowego Funduszu Zdrowia zamieszczane są informacje o sposobie prawidłowego korzystania z usługi oraz działania, jakie podjęte zostaną przez Fundusz w celu wyeliminowania stwierdzonych nieprawidłowości. W 2014 r. w wyniku działań NFZ wyeliminowano masowy problem błędnej konstrukcji oprogramowania świadczeniodawców, które wielokrotnie w ciągu dnia dokonywało pytań o uprawnienia tego samego pacjenta.

(dowód: akta kontroli Tom IV str. 525-531)

2. W ramach wdrażania systemu ZSZ Blue Energy Sp. z o.o. przeprowadziła audyt zerowy w Centrali NFZ w zakresie weryfikacji spełnienia wymagań zawartych w normach ISO/IEC 27001:2013, PN-ISO 31000:2012 i ISO 22301:2012[13]. W wyniku audytu stwierdzono, że Centrala NFZ spełnia jedynie część wymagań określonych przez dwie pierwsze wymienione normy, natomiast stopnień spełnienia wymagań zawartych w standardzie ISO 22301:2012 dotyczącym zarządzania ciągłością działania jest znikomy. Za największy problem w omawianym obszarze audytor zewnętrzny uznał brak wdrożonych narzędzi systemowych takich jak klasyfikacja informacji, analiza ryzyka pod kątem utraty bezpieczeństwa informacji czy agregacja i analiza zgłoszonych incydentów.

(dowód: akta kontroli Tom III str. 605-660)

3. Audytorzy zewnętrzni przeprowadzili w Centrali NFZ, w okresie objętym kontrolą, m.in. testy bezpieczeństwa systemu ZIP, testy bezpieczeństwa systemów informatycznych (w zakresie systemów dostępnych w Internecie, w tym styków sieci wewnętrznych z siecią Internet oraz wybranych aplikacji webowych).

(dowód: akta kontroli Tom III str. 278-604)

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

W Centrali NFZ za planowanie i realizację audytów wewnętrznych w tym audytów dotyczących obszaru IT odpowiada Departament Kontroli/Wydział Audytu Wewnętrznego.

W okresie objętym kontrolą zespół audytorów wewnętrznych przeprowadził następujące zadania audytowe w zakresie bezpieczeństwa systemów teleinformatycznych:

[13] ISO/IEC 27001:2013 Bezpieczeństwo informacji, PN-ISO 31000:2012 Zarządzanie ryzykiem – zasady i wytyczne oraz ISO 22301:2012 System zarządzania ciągłością działania.

Okres przeprowadzenia audytu	Jednostka audytowana	Temat zadania audytowego	Rodzaj zadania audytowego
2014 - II-III kw.	Centrala NFZ / OW NFZ	Bezpieczeństwo informacji	zapewniające
2014 - IV kw.	Centrala NFZ	Ocena procesu wdrożenia Zintegrowanego Informatora Pacjenta	Doradcze
2015 - I kw.	Centrala NFZ	Ocena procesu planowania, utrzymania i rozwoju zasobów aplikacyjnych (w tym SI) oraz sprzętowych w odniesieniu do zidentyfikowanych potrzeb	zapewniające
2015 - III kw. Zadanie w trakcie realizacji	Centrala NFZ	Realizacja procesu opracowania oraz wdrożenia na poziomie Centrali NFZ systemów: SZBI, SZRK oraz SZCD	zapewniające

(dowód: akta kontroli Tom III str. 61-135)

Prezes NFZ wyjaśnił m.in., że „*audyty wewnętrzne realizowane w celu zapewnienia informacji dotyczących tego, czy system zarządzania bezpieczeństwem informacji jest zgodny z wewnętrznymi wymogami Funduszu dotyczącymi systemu zarządzania bezpieczeństwem informacji oraz wymogami normy międzynarodowej i czy system został skutecznie wdrożony i jest efektywnie utrzymywany* będą *realizowane w ramach utrzymania samego SZBI. W ramach projektu ZSZ przewidziano również konieczność pozyskania zasobów osobowych zdolnych do prowadzenia audytów wewnętrznych w tym zakresie. W ramach projektu zapewniono szkolenia dla Audytorów Wewnętrznych ISO/IEC 27001 oraz Audytorów Wiodących ISO/IEC 27001 przy założeniu, że szkolenia realizowane będą przez trenerów organizacji akredytowanej do certyfikacji systemów zarządzania bezpieczeństwem informacji.*"

(dowód: akta kontroli Tom IV str. 517-518)

Ustalone nieprawidłowości

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

1.4. Definicja incydentu związanego z bezpieczeństwem

Opis stanu faktycznego

Stosownie do § 20 ust. 2 pkt 13 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

W obowiązującym w Centrali NFZ zarządzeniu nr 12/2010/POIN przyjęto definicję naruszenia bezpieczeństwa systemu informatycznego w brzmieniu „*jakiekolwiek naruszenie poufności, integralności, dostępności do systemu informatycznego spowodowane w szczególności przez ludzi, oddziaływanie sił przyrody, katastrofy cywilizacyjne*".

(dowód: akta kontroli Tom I str. 81)

Rejestry incydentów w Centrali NFZ prowadzone są odrębnie przez Gabinet Prezesa Funduszu i Departament Informatyki.

(dowód: akta kontroli Tom I str. 233-235, 239-243)

Centrala NFZ na bieżąco współpracuje z Zespołem Reagowania na Incydenty Komputerowe CERT.GOV.PL. Departament Informatyki otrzymuje zalecenia co do blokowania ruchu z/do niebezpiecznych adresów oraz domen, jak również informacje na temat wykrytych zagrożeń bezpieczeństwa, zaleceń co do konfiguracji urządzeń itp. W ramach współpracy z Agencją Bezpieczeństwa Wewnętrznego

(dalej: ABW) w dniu 4 października 2006 r. w Centrali NFZ została wdrożona sonda systemu ARAKIS-GOV (bezterminowo).

W odpowiedzi na zgłaszane przez CERT zagrożenia (52) każdorazowo podejmowano stosowne działania, obejmujące aktualizacje systemów, blokady adresów na firewallach oraz wyłączanie zbędnych usług.

(dowód: akta kontroli Tom I str. 227, 239-243, Tom IV str. 93)

Pracownicy pionu IT w NFZ rozpowszechniali informacje o potencjalnych zagrożeniach, ich przyczynach i metodach uniknięcia (opis ataku hakerskiego wycelowanego w polskie samorządy, fałszywe powiadomienia o niedostarczonych przesyłkach z Poczty Polskiej i DHL, ostrzeżenia przed próbą wyłudzenia hasła do poczty, informacje pozyskane od Rządowego Zespołu Reagowania na Incydenty o możliwości wystąpienia ataków na rządowe systemy teleinformatyczne, w szczególności systemy pocztowe) poprzez przesyłanie pracownikom Centrali NFZ korespondencji mailowej.

(dowód: akta kontroli Tom IV str. 500-508)

Prezes NFZ wyjaśnił, że *„w okresie objętym kontrolą nie wykryto przypadków naruszenia bezpieczeństwa danych, w tym w szczególności danych wrażliwych."*

(dowód: akta kontroli Tom I str. 227)

Ustalone nieprawidłowości

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

- Gabinet Prezesa Funduszu – w rejestrze incydentów za 2014 r. ujęto 9 zdarzeń, a w 2015 r. – 5 zdarzeń. Incydenty dotyczyły m.in. wykorzystania danych do celów niezgodnych z prawem, umieszczenia danych kadrowych na dysku publicznym, pozostawienia na drukarce kopii dokumentów zawierających dane osobowe, przesłania na prywatną skrzynkę wiadomości zawierającej dane PESEL.
- Departament Informatyki – w rejestrze ujęto łącznie 52 zdarzenia dotyczące przede wszystkim informacji uzyskanych z CERTu, a także wiadomości email podszywających się pod NATO lub wiadomości typu phising (zawierających w załącznikach złośliwe oprogramowanie) oraz ostrzeżeń o kampanii cyberszpiegowskiej ukierunkowanej na administrację publiczną.

(dowód: akta kontroli Tom I str. 233-235, 239-243)

Prezes NFZ podał, że *„W chwili obecnej w ramach procedowania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z ISO/IEC 27001, opracowywana jest procedura zarządzania incydentami wraz z załącznikiem „Przykładowe zdarzenia mogące mieć wpływ na bezpieczeństwo informacji" oraz z załącznikiem „Rejestr incydentów". Procedura zastąpi obecny system ewidencjonowania incydentów."*

W przedłożonym dokumencie ujęto m.in. definicje incydentu, zgłaszanie, rejestrowanie incydentów, analizę zdarzeń i sposób zarządzania incydentami oraz wzajemne informowanie o incydentach.

(dowód: akta kontroli Tom IV str. 281-288, 402)

Ponadto, w Centrali NFZ, w okresie objętym kontrolą, nie zdefiniowano mierników pozwalających na identyfikację powtarzających się rodzajów incydentów i klasyfikację ich istotności.

Prezes NFZ podał, że *„klasyfikacja i ocena incydentów stanowi cześć aktualnie opracowywanego procesu zarządzania incydentem w ramach Systemu Zarządzania Bezpieczeństwem Informacji. Do tego czasu identyfikacja powtarzających się rodzajów incydentów i klasyfikacja ich istotności była oparta na regulacjach opisanych w załączniku do Polityki Bezpieczeństwa to „instrukcja postępowania w przypadku naruszenia ochrony danych osobowych". Dotyczy to także przypadku naruszenia przepisów prawa/regulacji wewnętrznych oraz gromadzenia dowodów."*

(dowód: akta kontroli Tom IV str. 402)

Ponadto, Dyrektor Gabinetu Prezesa Funduszu podała m.in., że *„zakwalifikowanie danego zdarzenia jako incydent oparte jest na wiedzy i doświadczeniu pracowników Departamentu Informatyki."*

(dowód: akta kontroli Tom IV str. 498)

W ocenie NIK regulacje przywołane w wyjaśnieniach Prezesa NFZ dotyczą głównie przypadków naruszenia ochrony danych osobowych. Kategoria ta nie obejmuje takich zdarzeń jak np. atak wirusowy lub ataki innego złośliwego oprogramowania, sabotaż systemów zabezpieczeń technicznych lub teleinformatycznych, nieautoryzowane usunięcie/dodanie/modyfikacja danych. Takie przykładowe zdarzenia mające wpływ na bezpieczeństwo informacji ujęte są w projekcie dokumentu „Procedura zarządzania incydentami bezpieczeństwa".

Brak jednego, zcentralizowanego rejestru incydentów, w ocenie NIK, uniemożliwia kierownictwu NFZ stworzenie odpowiednich warunków do monitorowania stanu bezpieczeństwa jednostki, reagowania na incydenty oraz ich analizowania w celu doskonalenia sytemu zabezpieczeń, a także realizację działań zalecanych w pkt. 16.1.1. normy PN-ISO/IEC 27002 obejmujących określenie procedur związanych z odnotowywaniem działań związanych z incydentami bezpieczeństwa.

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

1.5. Zarządzanie kluczami kryptograficznymi

Opis stanu faktycznego

Zgodnie z §20 ust. 2 pkt 12 lit. d) rozporządzenia w sprawie KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez stosowanie mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa.

Wymagania technicznie i organizacyjne dla tworzenia i stosowania certyfikatów klucza publicznego wydawanych przez Centrum Certyfikacji NFZ określone są w Polityce Centrum Certyfikacji NFZ (dalej: PCC) wydanej w dniu 21 kwietnia 2011 r. przez ISCG Sp. z o.o. w Warszawie.

Centrum Certyfikacji NFZ działa w ramach systemu infrastruktury klucza publicznego (dalej: PKI). PCC reguluje podstawowe prawa i obowiązki stron: Centrum Certyfikacji NFZ i Subskrybentów (użytkowników tego systemu) oraz stron

ufających. Sposób zapewnienia gwarantowanego przez PCC poziomu zaufania określony jest w Kodeksie Postępowania Certyfikacyjnego.

(dowód: akta kontroli Tom II str. 28-135)

Dla certyfikatów wydawanych przez urząd NFZCAe, w zależności od poziomu certyfikatu, stosowane są następujące zasady generowania kluczy:

a) Poziom 1: klucze są generowane przy pomocy software CSP. Klucze prywatne przechowywane są w lokalnym magazynie certyfikatów systemu.

b) Poziom 2: klucze prywatne są generowane przy pomocy software CSP. Klucze prywatne przechowywane są w lokalnym magazynie certyfikatów użytkownika chronionym hasłem w postaci pliku chronionego hasłem.

c) Poziom 3: klucze prywatne są generowane przy pomocy hardware CSP. Klucze prywatne są chronione przy pomocy modułów sprzętowych HSM lub za pomocą kart inteligentnych (Smartcard).

(dowód: akta kontroli Tom II str. 136-461)

W Centrali NFZ od końca 2013 r. wydanych zostało około 1600 certyfikatów (związanych z kluczami użytkowników umieszczonymi na kartach kryptograficznych) dla wskazanych pracowników Funduszu w Centrali oraz oddziałach wojewódzkich. Są one wykorzystywane do potwierdzania czynności w systemie e-faktury oraz zapewnienia rozłączalności elektronicznego obiegu dokumentów księgowych.

(dowód: akta kontroli Tom II str. 400)

Dostęp zewnętrzny do systemu eWUŚ jest zabezpieczony przy pomocy certyfikatu SSL dostarczanego przez zewnętrzny urząd certyfikacji (Thawte). Certyfikat ten ważny jest do dnia 1 listopada 2017 r.

(dowód: akta kontroli Tom I str. 482-483)

Zastępca Dyrektora Di podał m.in., że *„usługa eWUŚ wykorzystuje podpisy cyfrowe w odpowiedzi na zapytanie o dany numer PESEL do zapewnienia autentyczności i integralności przekazywanych zwrotnie informacji – każda odpowiedź dla świadczeniodawcy i lekarza z systemu jest podpisywana cyfrowo."*

(dowód: akta kontroli Tom II str. 6)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości

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

Opis stanu faktycznego

1. Rozwiązaniem zapobiegającym użytkowaniu szkodliwego oprogramowania na stacjach roboczych (komputery, laptopy) oraz na zasobach udziałów sieciowych w Centrali NFZ jest Intel Security[14].

Definicje sygnatur są aktualizowane codziennie poprzez wbudowany mechanizm aktualizacji oraz stosowana jest również możliwość aktualizacji wykonywanej „ręcznie" (na żądanie) dla specyficznej konfiguracji.

Oprogramowanie jest dystrybuowane z centralnego serwera zarządzającego ePolicy Orchestrator (ePO). W centralnym serwerze zarządzającym jest również tworzona polityka zabezpieczeń. Agent jest instalowany na komputerach , które mogą być używane poza siedzibą NFZ. Polityki bezpieczeństwa pobierane są z centralnego

[14] Dawniej McAfee.

serwera. Aktualizacja sygnatur wirusów odbywa się automatycznie, w przypadku odłączenia od sieci firmowej jest możliwość ręcznej aktualizacji sygnatur.

P.o. dyrektora DI NFZ podał, że *„Produkt spełnia najbardziej istotne dla nas kryteria, tj. możliwość centralnego zarządzania oraz wysoki poziom wykrywania zabezpieczeń."*

Ponadto, w Centrali NFZ stosowane jest oprogramowanie, za pomocą którego automatycznie wdrażane są polityki, których zadaniem jest zabezpieczenie jednostki przed złośliwym oprogramowaniem. Przykładem takiej polityki jest NFZ Cipher blokowanie, której składnikiem jest kategoria User-defined Rules. Kategoria zawiera zasady, które są sprawdzane w momencie otrzymywania dostępu do plików.

(dowód: akta kontroli Tom I str. 262, Tom IV str. 385-386)

W odniesieniu do ochrony służbowych urządzeń mobilnych Prezes NFZ podał m.in., że *„jeżeli za urządzenia mobile uznajemy wyłącznie komputery przenośne, to podlegają one takim samym restrykcjom jak urządzenia stacjonarne. Mają one ponadto możliwość aktualizacji zabezpieczeń poza siecią firmową bezpośrednio ze stron producenta oprogramowania. Po ponownym podłączeniu do sieci firmowej na urządzeniu automatycznie aktualizowane są polityki oraz aktualne sygnatury. Urządzenia mobilne typu smartfon wykorzystywane do pracy służbowej (obsługa poczty elektronicznej) są zabezpieczone poprzez wymuszenie w momencie konfiguracji usługi ustawienie kodu PIN. W momencie skasowania zabezpieczenia typu PIN użytkownik automatycznie traci dostęp do konta pocztowego, informacje dotyczące danych konta są kasowane."*

(dowód: akta kontroli Tom IV str. 514)

Od strony sieci nad bezpieczeństwem systemów NFZ czuwają urządzenia typu firewall i IPS. Centrala NFZ w dostępie do firewall stosuje zasadę najmniejszego uprzywilejowania (dostęp do systemów jest domyślnie zabroniony, a możliwa jest tylko komunikacja zdefiniowana jako niezbędna do działania danego systemu).

Do korelacji logów i wykrywania anomalii w sieci NFZ służy system do monitorowania bezpieczeństwa „ArcSight"[15].

(dowód: akta kontroli Tom I str. 210, 276-289)

System ochrony przed wyciekiem Fidelis – moduł sieciowy - służy do identyfikacji potencjalnych zdarzeń, w wyniku których mógł nastąpić wyciek danych osobowych z sieci NFZ, jak również posiada funkcję Anti-Malware.

P.o. dyrektora DI NFZ podał, że *„Na bieżąco przekazywane są informacje systemu Fidelis, o zablokowaniu przesyłek zawierających dane osobowe w postaci numeru pesel. Tego typu incydenty wycieku danych są na bieżąco sprawdzane. Pracownicy centrali posiadają wiedzę o tych działaniach, stąd też w bieżącym roku nie odnotowano wycieku informacji."*

(dowód: akta kontroli Tom I str. 210, 266-275, 491-501)

Do dnia zakończenia kontroli trwały prace Komisji Przetargowej powołanej do przeprowadzenia postępowania o udzielenie zamówienia publicznego na „Rozbudowę systemu DLP Fidelis wraz z usługą utrzymania (maintenance) oraz wsparciem technicznym.

(dowód: akta kontroli Tom I str. 530-577)

---

[15] System klasy SIEM – Security Information & Event Management.

System eWUŚ oraz inne systemy aplikacyjne oraz bazodanowe są chronione przez ww. rozwiązania sieciowe, poprzez umieszczenie ich w odpowiednych strefach dostępu. Serwery bazodanowe i aplikacyjne, które nie mają styku z Internetem, są umieszczane w sieci LAN z całkowitym brakiem dostępu do Internetu (w obie strony). Serwery aplikacyjne, które są dostępne z Internetu są umieszczane w strefie DMZ i są udostępniane w Internecie tylko w niezbędnym do funkcjonowania zakresie, same nie komunikując się z Internetem.

(dowód: akta kontroli Tom I str. 264)

Wszyscy pracownicy Centrali NFZ są informowani o zagrożeniach związanych z bezpieczeństwem teleinformatycznym za pośrednictwem poczty elektronicznej (otrzymują przesyłkę e-mail na konto imienne).

Śledzeniem zagrożeń zajmują się administratorzy (dwie osoby) oprogramowania antywirusowego. Zagrożenia śledzone są na podstawie informacji publikowanych w mediach elektronicznych[16], informacji otrzymywanych od firmy świadczącej usługę wsparcia oraz informacji dotyczących bezpieczeństwa otrzymywanych od agencji ABW. Aktualizacja doraźnych zmian prowadzona jest na bieżąco w chwili pozyskania informacji o zagrożeniu. W latach 2014-2015 wystąpiły dwa przypadki doraźnej interwencji związanej ze zmasowanym atakiem na polskie instytucje publiczne.

Przychodzące wiadomości są filtrowane za pomocą urządzenia IronPort, tj. weryfikowana jest reputacja nadawcy oraz odfiltrowywane są informacje uznawane za SPAM. Filtrowaniu podlegają słowa kluczowe oraz załączniki.

Prezes NFZ podał, że *„Przypadki automatycznego wykrycia zagrożenia są wizualizowane w formie graficznej na ekranie startowym aplikacji do zarządzania i monitoringu (Dashboards), śledzonym na bieżąco przez administratorów systemu. Każde odnotowane wykrycie analizują administratorzy. Wszystkie zdarzenia systemu antywirusowego rejestrowane są w dedykowanej bazie danych. W przypadku raportowania znacznej ilości zagrożeń, rejestrowane jest zgłoszenie w systemie zgłoszeniowym oraz wysłana jest prośba do użytkownika o wyjaśnienie zaistniałej sytuacji."*

(dowód: akta kontroli Tom IV str. 387-389, 403-412, 413-420)

Zdarzenia wykrycia niebezpiecznych wiadomości pocztowych system raportuje w formie graficznej na ekranie startowym aplikacji do zarządzania. Zaimplementowane automaty odrzucają niepożądane oraz niebezpieczne wiadomości. Dodatkowo prowadzona jest analiza wszystkich wiadomości pocztowych, które wpływają do systemu antyspamowego. W przypadku uznania za niepożądaną wiadomość, która nie została odrzucona przez zaimplementowane reguły, dokonuje się ich ręcznej aktualizacji. Ogólna liczba wykrycia niepożądanej treści oraz szkodliwego oprogramowania występuje średnio w ilości ok 230 000 dziennie.

System Intel Security automatycznie wykonuje zadane polityki bezpieczeństwa. Zdarzenia wykrycia szkodliwego oprogramowania, system raportuje w formie graficznej na ekranie startowym aplikacji do zarządzania i monitoringu. Informacje wyświetlane w raportach analizowane są na bieżąco przez administratorów. Zdarzeniem wykrycia szkodliwego oprogramowania jest wykrycie np. skryptów które uruchamiane są w momencie przeglądania stron WWW (np. *.js), aplikacje typu „makro" dołączone do arkuszy Excel lub dokumentów Word, wirusy, aplikacje, biblioteki DLL, itp. W szczególnych przypadkach wykrycia szkodliwego

[16] Np. biuletyny informacyjne: https://community.mcafee.com, niebezpiecznik.pl itp.

oprogramowania, po wstępnej analizie, rejestrowane jest zgłoszenie w systemie zgłoszeniowym oraz wysyłana jest prośba do użytkownika końcowego o wyjaśnienie zaistniałej sytuacji. Ogólna liczba zdarzeń wykrycia szkodliwego oprogramowania wymienionego wcześniej występuje średnio w ilości ok 60 dziennie.

(dowód: akta kontroli Tom IV str. 518-519, 543-546)

W wyniku oględzin trzech losowo wybranych komputerów stacjonarnych w Centrali NFZ stwierdzono, że podłączenie i użycie pamięci przenośnej typu pendrive możliwe jest wyłącznie w przypadku logowania upoważnionego pracownika. Pracownik bez nadanych uprawnień nie mógł podłączyć tego typu pamięci. W Centrali NFZ prowadzona jest ewidencja osób uprawnionych do użycia pamięci typu pendrive.

(dowód: akta kontroli Tom IV str. 55-57)

Prezes NFZ podał m.in., że *„Dyrektorzy komórek organizacyjnych Centrali Funduszu chcąc wyposażyć podległych sobie pracowników w pamięć przenośną typu pendrive, występują do Gabinetu Prezesa Funduszu o zgodę na ich użytkowanie. Pracownik zostaje wpisany do Ewidencji Pendrive oraz przekazana zostaje informacja zwrotna do Wnioskodawcy o odpowiedzialności pracownika za znajdujące się na pendrive dane oraz konieczności zachowania szczególnej ostrożność podczas jego transportu, przechowywania i użytkowania jak również stosowania środków ochrony kryptograficznej wobec danych na nim zapisanych."*

(dowód: akta kontroli Tom IV str. 516)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości

1.7. Bezpieczeństwo sieciowe

Opis stanu faktycznego

W Centrali NFZ prowadzona jest ewidencja urządzeń sieciowych. Infrastruktura sieciowa eWUŚ jest infrastrukturą dzieloną z innymi systemami i w związku z powyższym nie jest prowadzona odrębna ewidencja dla tych aktywów. Wszystkie krytyczne urządzenia sieciowe i serwery znajdują się w wydzielonych serwerowniach i punktach dystrybucyjnych z kontrolą dostępu zarówno fizycznego, jak i zdalnego zarządzania.

(dowód: akta kontroli Tom I str. 523-528, Tom II str. 3)

Procedury zarządzania sieciowymi elementami aktywnymi i pasywnymi przyjęte zostały w dniu 23 kwietnia 2013 r. przez dyrektora DI (PDI-05). Procedury te nie zostały zatwierdzone, do dnia zakończenia kontroli, przez Prezesa NFZ i tym samym obowiązują jedynie pracowników DI.

Procedura ta określa zasady włączania, wyłączania i obsługi aktywnych i pasywnych elementów sieciowych, a także opisuje działania w przypadku wystąpienia problemów lub incydentów bezpieczeństwa[17]. W procedurze ujęto działania dotyczące: przygotowania i instalacji urządzeń sieciowych oraz ich włączania, harmonogram pielęgnacji urządzeń, zarządzanie siecią LAN i WAN, wyłączania i resetowania urządzeń sieciowych, działania w przypadku wystąpienia problemów incydentów bezpieczeństwa, konserwacji i serwisu urządzeń sieciowych, zarządzania konfiguracją, inwentaryzacje, zarządzanie zmianą, zabezpieczanie urządzeń sieciowych oraz opieka nad umowami.

(dowód: akta kontroli Tom II str. 16-22)

[17] W przypadku wystąpienia incydentu bezpieczeństwa Administrator podejmuje działania mające na celu minimalizację skutków zagrożenia, zgodnie z dokumentem „Instrukcja postępowania w sytuacji naruszenia ochrony danych w NFZ".

W NFZ oddzielono odpowiedzialność personalną za funkcjonowanie sieci od odpowiedzialności za funkcjonowanie systemów korzystających z tej sieci. Zarządzaniem siecią zajmuje się wydzielona sekcja (Sekcja Sieci Teleinformatycznych w Wydziale Eksploatacji DI). Pracownicy tej sekcji nie zarządzają innymi systemami niż te, które są powiązane z funkcjonowaniem usług sieciowych.

Urządzenia sieciowe znajdują się w serwerowniach oraz punktach dystrybucyjnych z kontrolą dostępu. Dostęp do pomieszczeń ma ograniczone grono osób w Centrali NFZ – zdefiniowanych w systemie kontroli dostępu. Polityka haseł dla urządzeń infrastruktury sieciowej została określona w systemie uwierzytelniania administratorów infrastruktury sieciowej (ACS – Cisco Secure Access Control Server).

(dowód: akta kontroli Tom II str. 4)

Zgodnie z pkt 4.10. Procedury PDI-05 Zarządzanie konfiguracją tworzone są kopie konfiguracji urządzeń oraz odnotowywane zmiany w dzienniku administratora. Zmiany w konfiguracji urządzeń wymagają zatwierdzenia przez przełożonego.

(dowód: akta kontroli Tom III str. 20)

Urządzenia mobilne[18] w NFZ zabezpiecza się zgodnie z Procedurą korzystania z urządzeń mobilnych (PDI-09). Użytkownik korzystający z urządzenia mobilnego nie ma uprawnień administratora lokalnego, odstępstwem jest nadanie uprawnień tylko niektórych ustawień konfiguracyjnych np. wi-fi, szyfrowany jest dysk twardy za pomocą hasła, tzw. DriveLog – bez podania prawidłowo hasła komputer się nie uruchomi, instalacja oprogramowania antywirusowego z automatyczną aktualizacją. Procedura ta nie ma zastosowania do urządzeń typu smartphone, gdyż w centrali NFZ nie dopuszcza się stosowania tych urządzeń do przetwarzania danych. Wyjątkiem od tej zasady jest dopuszczenie wybranych pracowników, po uzyskaniu zgody ADO oraz Prezesa NFZ, do służbowych kont pocztowych. Na dzień 16 września 2015 r. pięciu pracowników posiadało dostęp do poczty służbowej centrali NFZ za pomocą usługi Active Sync.

(dowód: akta kontroli Tom I str. 484, 502-503, Tom II str. 23-24)

Zastępca Dyrektora DI podał m.in., iż *„przyjęto również zasadę, że w momencie konfiguracji połączenia do konta pocztowego narzucana jest polityka zabezpieczenia telefonu pinem. Jeśli użytkownik będzie chciał wyłączyć uwierzytelnienie pinem, będzie musiał wcześniej usunąć połączenie do konta pocztowego."*

(dowód: akta kontroli Tom III str. 3)

Krytyczne dla NFZ obszary sieci, tj. praca urządzeń sieciowych oraz urządzeń bezpieczeństwa jest monitorowana w zakresie przeglądu stanu urządzeń, alarmów, logów systemowych, dostępności, obciążenia. Stale monitorowany jest także ruch sieciowy na styku z Internetem. Pomieszczenia w których znajdują się urządzenia są monitorowane za pomocą monitoringu wizyjnego, a dostęp do nich ma ograniczone grono osób w Centrali NFZ.

W systemie monitoringu wykorzystuje się platformę ZABIX (umożliwiającą tworzenie systemów raportowania), platformę Cacti (monitorowanie w trybie rzeczywistym) oraz usługę Monit24.pl (monitorowanie działania systemów zewnętrznych, w tym eWUŚ).

---

[18] Poprzez urządzenia mobilne rozumie się komputery przenośne (laptopy) wykorzystywane do przechowywania i przetwarzania informacji w postaci elektronicznej, które mogą zostać wykorzystane poza siedzibą Centrali NFZ.

(dowód: akta kontroli Tom I str. 513-529)

Ustalone nieprawidłowości

Oceniając poziom zarządzania procesami zapewnienia bezpieczeństwa systemów teleinformatycznych z punktu widzenia stosowanego w metodyce CobiT 4.1 Modelu dojrzałości, biorąc pod uwagę minimalne wymagania dla systemów teleinformatycznych zawarte w rozporządzeniu KRI oraz dobre praktyki, w tym zalecenia zawarte w Polskich Normach w zakresie działań związanych z zapewnieniem warunków bezpieczeństwa systemów informatycznych stwierdzono, że w NFZ nie jest prowadzona klasyfikacja aktywów, w związku z powyższym nie mają one przyporządkowanych parametrów istotności i poziomów ochrony.

(dowód: akta kontroli Tom I str. 523-528, Tom II str. 3)

Nieprzypisanie informacjom odpowiedniego poziomu ochrony, zgodnego z ich wagą dla Funduszu NIK ocenia jako nierzetelne. Na konieczność dokonania klasyfikacji informacji z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację, a także na konieczność opracowania zbioru procedur oznaczania informacji wskazuje pkt. 8 normy PN-ISO/IEC 27005.

Ocena cząstkowa

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

2. Wspieranie bezpieczeństwa na poziomie wybranego systemu

2.1. Zarządzanie tożsamością

Opis stanu faktycznego

Zgodnie z ustawą z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych[19] użytkownikami usługi eWUŚ są świadczeniodawcy lub niebędące świadczeniodawcami osoby uprawnione w rozumieniu art. 2 pkt 14 ustawy z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych[20].

System eWUŚ został zaprojektowany w sposób umożliwiający zarządzanie (administrację) użytkownikami z poziomu świadczeniodawcy. Świadczeniodawcy na podstawie aktualnej umowy z NFZ otrzymują konta administratora umożliwiające zakładanie i administrowanie użytkownikami. Jak wyjaśnił p.o. Dyrektora DI *„w obecnej chwili na podstawie analiz wykonanych w środowisku autoryzacyjnym ustalono liczbę upoważnionych kontrahentów w wysokości 22 693 kont oraz sumaryczną liczbę wszystkich upoważnionych operatorów wszystkich świadczeniodawców i lekarzy z indywidualną praktyką na 142 241 kont."*

[19] Dz. U. z 2015 r., poz. 581 ze zm.

[20] Dz. U. z 2015 r., poz. 345.

(dowód: akta kontroli Tom I str. 212)

Dostęp na prawach administratora do serwerów aplikacyjnych eWUŚ ma pracowników Centrali NFZ, a do serwerów bazodanowych eWUŚ kolejnych 4 pracowników Centrali NFZ[21]. Ponadto, 6 pracowników Centrali Funduszu ma uprawnienia do przeglądania historii zapytań w systemie eWUŚ z poziomu Centralnego Wykazu Ubezpieczonych (informacje wykorzystywane są przy weryfikacji uprawnień do świadczeń opieki zdrowotnej finansowanych ze środków publicznych).

(dowód: akta kontroli Tom I str. 219, 224)

W Centrali NFZ nie ma odrębnej procedury nadawania uprawnień dla administratorów systemu eWUŚ, który jest jednym z elementów Systemu Informatycznego NFZ. Dostęp do SINFZ jest nadawany przez administratora systemu w oparciu o Wniosek o założenie/modyfikację/usunięcie konta użytkownika Systemu Informatycznego NFZ oraz przydział czynności, nadawane w momencie przyjmowania pracownika do pracy lub zmiany zakresu jego zadań (np. w przypadku zmiany komórki organizacyjnej). Wniosek ten jest każdorazowo akceptowany przez kierownika komórki merytorycznej oraz Dyrektora DI.

(dowód: akta kontroli Tom IV str. 548)

W dziennikach systemu eWUŚ odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegających na dostępie do systemu z uprawieniami administracyjnymi oraz konfiguracji systemu, w tym konfiguracji zabezpieczeń. W ramach publicznego systemu dostępowego eWUŚ dla świadczeniodawców i lekarzy, realizowany jest również dostęp dla lokalnego administratora świadczeniodawcy lub lekarza w celu zarządzania lokalnymi operatorami oraz ich upoważnieniami, koniecznymi do wykonywania zapytań o uprawnienie do świadczeń danego świadczeniobiorcy. Operacje wykonywane w tym trybie są składowane w logach systemowych.

Wszystkie działania użytkowników, zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu są zapisywane w logach systemowych serwera aplikacyjnego lub bazodanowego bez rozróżnienia z jakimi uprawnieniami zostały one wykonane. Rozróżnienie wynika z nadanych uprawnień dla danego systemu i jest zapisywane w oddzielnych plikach konfiguracyjnych systemu.

(dowód: akta kontroli Tom I str. 223, 257-258, Tom IV str. 446)

Dostęp do części publicznej usługi eWUŚ zabezpieczony jest mechanizmem uwierzytelniania w oparciu o login i hasło. Dodatkowo, każdy z operatorów korzystających z systemu eWUŚ musi, oprócz odpowiednych uprawnień, zyskać upoważnienie lokalnego administratora po stronie świadczeniodawcy lub lekarza. Każda próba uwierzytelnienia dostępu do publicznej części usługi eWUŚ za pośrednictwem aplikacji www lub usługi sieciowej jest logowana w systemie z określeniem daty i czasu operacji, rodzaju dostępu, adresu wywołania, danych operatora oraz wyniku operacji (pozytywna/negatywna). W systemie logowane są również próby uzyskania dostępu dla operatorów, którzy nie posiadają konta w systemie – w takim przypadku logowany jest również ciąg znaków wprowadzony jako login operatora.

(dowód: akta kontroli Tom I str. 223, 258-259)

[21] Według stanu na dzień 21 lipca 2015 r.

W odniesieniu do weryfikacji tożsamości podczas uzyskiwania dostępu do usługi eWUŚ przez użytkowników końcowych – nadawanie uprawnień operatora i administratora lokalnego odbywa się na podstawie dokumentu „Zasady korzystania z Elektronicznej Weryfikacji uprawnień Świadczeniobiorców – usługa eWUŚ" wdrożonym na podstawie rozporządzenia Ministra Zdrowia z dnia 20 grudnia 2012 r. w sprawie warunków występowania o sporządzenie dokumentu elektronicznego potwierdzającego prawo do świadczeń opieki zdrowotnej[22]. Weryfikacja tożsamości osoby, której powierza się korzystanie z usługi eWUŚ następuje podczas wydawania upoważnienia do korzystania z usługi eWUŚ.

(dowód: akta kontroli Tom IV str. 458-466)

Prezes NFZ podał m.in., że *„w przypadku serwerów bazodanowych i aplikacyjnych wszystkie dostępy do systemu eWUŚ odnotowywane są w logach systemowych i nie ma znaczenia jaki proces, użytkownik czy usługa uzyskuje dostęp do systemu. Dostęp do systemu eWUŚ może mieć jedynie użytkownik/proces, który ma zdefiniowane konto na tym systemie z odpowiednimi uprawnieniami. Weryfikacja dostępu do systemu eWUŚ pod kątem czy dostęp nastąpił zdalnie lub „z domu" lub inny sposób nie jest prowadzona na poziomie systemu operacyjnego Linux. Takie rozróżnienie jest możliwe w powiązaniu z weryfikacją logów dostępu VPN."*

(dowód: akta kontroli Tom IV str. 520)

Dostęp do przetwarzanych w systemach danych, udostępnianych poprzez usługę eWUŚ odbywa się za pośrednictwem przeglądarki internetowej z wykorzystaniem aplikacji webowej. Dostęp do aplikacji odbywa się poprzez uwierzytelnienie użytkownika poprzez wybór oddziału i wprowadzenie identyfikatora oraz hasła. Logowanie do aplikacji webowej eWUŚ zabezpieczone jest za pomocą kryptograficznej ochrony danych SSL. Możliwy jest również dostęp do przedmiotowych danych poprzez usługi. W tym przypadku wykorzystywany jest interfejs dostępowy z wykorzystaniem usług sieciowych w oparciu o mechanizm WSBroker.

Wszelkie zapytania o uprawnienia osoby ubiegającej się o świadczenia, odpowiedzi na te zapytania oraz data i oznaczenie użytkownika zadającego zapytanie są zapisywane w logach eWUŚ.

(dowód: akta kontroli Tom IV str. 446, 479-496)

Prezes NFZ podał, że „średnio dokonywanych jest około 3,4 mln zapytań w dni robocze i około 1 mln zapytań w dni wolne".

(dowód: akta kontroli Tom IV str. 398)

Dostęp do części usługi eWUŚ realizowany jest w oparciu o jeden profil użytkownika, wykorzystywany przez serwery aplikacyjne do dostępu do baz danych. P.o. Zastępcy Dyrektora DI podał m.in. że *„Podstawowym zabezpieczeniem jest stosowanie list dostępu do usługi, na podstawie których z systemu mogą korzystać tylko zaufane serwery z wewnętrznej sieci [NFZ]. Listy te nadzorowane są przez logikę aplikacji. Drugim zabezpieczeniem jest wykorzystywanie systemowych mechanizmów autentykacji i autoryzacji użytkowników. Dlatego też profil użytkownika wykorzystywany w aplikacji ma minimalne uprawnienia i dostęp tylko do obiektów stricte wymienionych, jako te do których ma autoryzację. Ponadto dane o dostępnie do usługi eWUŚ z serwerów zewnętrznych są stale monitorowane i nadzorowane. Zbierane dane dotyczą zarówno ruchu sieciowego, jak i operacji logowania i niektórych akcji podejmowanych przez użytkowników w systemie."*

[22] Dz. U. z 2012 r. poz. 1500

(dowód: akta kontroli Tom I str. 259)

W wyniku analizy przekazanych logów systemu eWUŚ oraz logów VPN nie stwierdzono nieprawidłowości.

(dowód: akta kontroli Tom I str. 223, 253, Tom IV str. 446)

Hasła kont administracyjnych systemów Centrali NFZ były zdeponowane w zaklejonych bezpiecznych kopertach, przechowywanych w sejfie.

(dowód: akta kontroli Tom IV str. 59-63)

W umowach na zakup lub serwis sprzętu komputerowego lub oprogramowania widniały zapisy gwarantujące zabezpieczenie poufności informacji uzyskanych w związku z ich realizacją przez wykonawców, tj. zgodnie z § 20 ust. 2 pkt 10 rozporządzenia KRI.

(dowód: akta kontroli Tom I str. 42, 270, 277, 283, 287)

Stwierdzono, że Centrala NFZ nie dokonała aktualizacji listy kontaktowej w bazie RIPE dla adresacji NFZ (tj. 194.50.61.0/24).

P.o. Zastępcy Dyrektora DI podał, że dwukrotnie – w latach 2009 i 2013 podejmowano próby aktualizacji danych w bazie RIPE poprzez zgłoszenia kierowane do LIR (Local Internet Registry). Działania te były nieskuteczne. *„Problem ten został rozwiązany wewnętrznie – adres kontaktowy podany w RIPE został przypisany na naszych serwerach pocztowych do nowej skrzynki pocztowej i otrzymujemy całą korespondencję wysyłaną na ten adres."*

(dowód: akta kontroli Tom I str. 261)

W wyniku kontroli NIK ponownie podjęto działania, których skutkiem była aktualizacja danych w bazie RIPE.

(dowód: akta kontroli Tom III str. 669)

Ustalone nieprawidłowości

Oceniając poziom zarządzania procesami zapewnienia bezpieczeństwa systemów teleinformatycznych z punktu widzenia stosowanego w metodyce CobiT 4.1 Modelu dojrzałości, biorąc pod uwagę minimalne wymagania dla systemów teleinformatycznych zawarte w rozporządzeniu KRI oraz dobre praktyki, w tym zalecenia zawarte w Polskich Normach w zakresie działań związanych z zapewnieniem warunków bezpieczeństwa systemów informatycznych stwierdzono, że w logach systemu eWUŚ, w okresie objętym kontrolą, ponad 180 razy pojawiał się użytkownik „root".

(dowód: akta kontroli Tom IV str. 446)

Prezes NFZ wyjaśnił, że *„dla systemów opartych o platformę Linux użytkownik „root" był używany wyłącznie przez administratorów pracujących w Centrali NFZ w celach instalacyjnych, konfiguracyjnych. Rozliczalność była zapewniona poprzez odpowiednie wpisy w logach systemowych, jednak dla pełnej identyfikacji niejednokrotnie należało korelować logi z kilku źródeł, co w znacznym stopniu komplikowało taką weryfikację.*

Obecnie w celu lepszej kontroli i rozliczalności działań administratorów wdrażany jest system IPA, który uniemożliwi korzystanie bezpośrednie z konta „root". Po pełnym wdrożeniu tego systemu wszelkie zmiany konfiguracyjne będą wykonywane wyłącznie przez administratorów (użytkowników) imiennych z nadanymi odpowiednimi uprawnieniami."

(dowód: akta kontroli Tom IV str. 397)

W ocenie NIK ww. przypadki wskazują na brak pełnej rozliczalności systemów teleinformatycznych Funduszu, co było niezgodne z § 21 ust. 1 rozporządzenia KRI, który stanowi, że rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach). Ponadto, zgodnie z zaleceniem pkt. 9.2.3 normy ISO/IEC 27002 należy utworzyć i utrzymywać szczególne procedury w celu uniknięcia nieautoryzowanego użycia typowych identyfikatorów użytkowników administracyjnych.

2.2. Zarządzanie kontami użytkowników

Opis stanu faktycznego

Zasady dotyczące założenia profilu użytkownika, nadania i modyfikacji uprawnień użytkownika centralnych baz danych zarządzanych z poziomu Centrali NFZ określono w § 3 i 4 Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w narodowym Funduszu Zdrowia, stanowiącej załączniki nr 2 do zarządzenia nr 12/2010/POIN.

Zarządzanie uprawnieniami uprzywilejowanymi następuje zgodnie z § 6 Instrukcji.

(dowód: akta kontroli Tom I str. 102-105)

Wnioski o przyznanie stacji roboczej dla użytkownika systemów informatycznych oraz o założenie/modyfikację/usunięcie konta użytkownika Systemu Informatycznego NFZ zawierały, zgodnie z ww. Instrukcją, w szczególności następujące dane: imię i nazwisko, stanowisko służbowe i nazwę komórki organizacyjnej pracownika, termin ważności, numer upoważnienia do przetwarzania danych osobowych, przedmiot wniosku oświadczenie pracownika o przeszkoleniu z zakresu ochrony danych osobowych wraz ze zobowiązaniem do ich przestrzegania, upoważnienie ABI oraz akceptację przełożonego pracownika oraz upoważnionego pracownika Departamentu Informatyki.

(dowód: akta kontroli Tom IV str. 16-25)

Szczegółowe zasady przyznawania uprawnień do systemów teleinformatycznych NFZ oraz zarządzania hasłami zostały określone w Procedurze zarządzania uprawnieniami i zmiany haseł (PDI-01).

W wyniku badania dokumentacji dwóch pracowników Centrali NFZ, z którymi rozwiązano stosunek pracy w trybie określonym w art. 52 § 1 pkt 1 Kodeksu pracy[23] stwierdzono, że DI niezwłocznie zablokował konta użytkowników i wykonał kopie bezpieczeństwa ich skrzynek pocztowych.

(dowód: akta kontroli Tom III str. 223-227, Tom IV str. 1-4)

Stosownie do § 5 pkt 9 Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w narodowym Funduszu Zdrowia, stanowiącej załączniki nr 2 do zarządzenia nr 12/2010/POIN *„komórka właściwa do spraw pracowniczych informuje kierownika komórki organizacyjnej właściwej do spraw informatyki i administratora bezpieczeństwa informacji (ABI) o dłuższej nieobecności pracowników w pracy (powyżej 30 dni kalendarzowych)."*

(dowód: akta kontroli Tom I str. 106)

Prezes NFZ wyjaśnił, że *„W okresie od stycznia 2014 r. do czerwca 2015 r. lista pracowników Centrali, którzy przebywają na przekraczających 30 dni absencjach była przekazywana w formie elektronicznej do komórki organizacyjnej odpowiedzialnej za administrowanie bezpieczeństwem informacji. Od lipca 2015 r.*

[23] Ustawa z dnia 26 czerwca 1974 r. (Dz. U. z 2014 r., poz. 1502 ze zm.

sytuacja uległa zmianie i informacja przesyłana jest bezpośrednio do Gabinetu Prezesa Funduszu (wykonującego w imieniu Prezesa zadania ABI) oraz do wskazanych pracowników Departamentu Informatyki." Ponadto, Prezes podał m.in., że „*W związku z przejęciem z dniem 1 kwietnia 2015 r. zadań w zakresie ochrony danych osobowych, Gabinet Prezesa Funduszu zwrócił się do Biura Kadr i Szkoleń o przesyłanie raportów o stanie zatrudnienia w Centrali Funduszu począwszy od czerwca 2015 r. na utworzoną skrzynkę mailową ado@nfz.gov.pl. Gabinet Prezesa Funduszu – zgodnie z ww. zarządzeniem - w zakresie swoich zadań, nie posiada obowiązku przekazywania raportów o stanie zatrudnienia do Departamentu Informatyki.*"

(dowód: akta kontroli Tom IV str. 87, 90-91)

Ustalone nieprawidłowości

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

Dane dotyczące absencji pracowników Centrali NFZ (przekraczających 30 dni kalendarzowych) przekazywane były do Departamentu Informatyki wybiórczo w okresach miesięcznych, głównie drogą elektroniczną. Stwierdzono, że:

a) nie przekazano informacji w miesiącach: luty, marzec, maj, czerwiec, wrzesień i październik 2014 r. oraz od stycznia do lipca 2015 r.

Prezes NFZ wyjaśnił: „*potwierdzam, że we wskazanych miesiącach wystąpiły przypadki absencji pracowników trwającej ponad 30 dni. Raporty za wszystkie miesiące w badanym okresie były sporządzane na bieżąco. Wszystkie raporty przekazane były drogą elektroniczną do komórki POIN. Natomiast Departament Informatyki dane o absencjach pracowników otrzymał z opóźnieniem.*"

b) w 24 przypadkach zgłoszenie nastąpiło w czerwcu 2014 r., pomimo że absencje pracowników miały miejsce w kwietniu 2014 r.

Prezes NFZ wyjaśnił, że absencje pracowników we wskazanych przypadkach miały miejsce przed kwietniem 2014 r. (nieobecność ciągła) i „*były również wykazywane we wcześniejszych raportach zgodnie ze stanem faktycznym.*"

(dowód: akta kontroli Tom IV str. 70-80, 91)

Działanie Biura Kadr i Szkoleń było niezgodne z § 5 pkt 9 Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Narodowym Funduszu Zdrowia, zgodnie z którym dane te przekazywać należy zarówno do Departamentu Informatyki jak i do ABI. Zaniechanie poinformowania działu IT o zmianach kadrowych niesie za sobą powstanie ryzyka dostępu osób nieuprawnionych do wewnętrznych baz danych Centrali NFZ.

2.3. Ochrona technologii zabezpieczeń

Opis stanu faktycznego

Historia zmian konfiguracji sprzętowej systemu eWUŚ rejestrowana jest zarówno w dziennikach administratora jak również w dokumentach pomocniczych stworzonych przez administratorów na potrzeby zarządzania infrastrukturą. W dziennikach administratora zawarta jest informacja kto i kiedy dokonał modyfikacji. Kopie konfiguracji są zachowywane podczas wykonywania codziennych kopii zapasowych.

(dowód: akta kontroli Tom IV str. 446)

Zgodnie z wyjaśnieniami Prezesa NFZ aktualne wersje aplikacji wraz z konfiguracją przekazywane są przez dostawcę zgodnie z zawartą umową.

(dowód: akta kontroli Tom IV str. 392)

Na poziomie użytkowników końcowych systemu eWUŚ, dla których udostępniane są informacje czy świadczeniobiorca zidentyfikowany poprzez nr PESEL posiada lub nie uprawnienia do korzystania ze świadczeń opieki zdrowotnej zaimplementowano automatyczne blokady, które uruchamiane są w przypadku 5 nieudanych prób logowań lub po przekroczeniu limitu logowań w jednostce czasu (500 na godzinę). W przypadku zbliżającego się terminu ważności hasła automatycznie generowany jest komunikat, że należy zmienić hasło. Jeżeli nie zostanie zmienione, to konto zostanie zablokowane.

Rejestr udanych/nieudanych prób logowania oraz uruchomionych blokad użytkowników stanowią logi systemu. Analiza logów została wdrożona bezpośrednio w aplikacji ze względu na wolumen danych i dokonywana jest na bieżąco w celu natychmiastowego zablokowania dostępu do systemu użytkownikom, których działania sklasyfikowano jako potencjalne zagrożenie.

W przypadku serwerów bazodanowych jak również serwerów aplikacyjnych nieudane próby logowania jak i inne zdarzenia systemowe rejestrowane są w logach systemowych poszczególnych serwerów. Analiza logów sprzętowych i systemowych przeprowadzana jest przez administratorów danego systemu.

(dowód: akta kontroli Tom IV str. 392-393, 446)

Zarządzanie uprawnieniami na poziomie aplikacji eWUŚ, w której występuje pojęcie „administratora systemu eWUŚ" następuje zgodnie z rozporządzeniem Ministra Zdrowia z dnia 20 grudnia w sprawie warunków występowania o sporządzenie dokumentu elektronicznego potwierdzającego prawo do świadczeń opieki zdrowotnej oraz Zasadami korzystania z eWUŚ wdrożonymi na podstawie przedmiotowego rozporządzenia.

(dowód: akta kontroli Tom IV str. 458-466)

Prezes NFZ podał m.in., że „*Po otrzymaniu upoważnienia do korzystania z usługi eWUŚ świadczeniodawca, bądź lekarz posiadający umowę z NFZ na wystawianie refundowanych recept lekarskich występuje z wnioskiem do oddziału NFZ o przyznanie wskazanemu użytkownikowi uprawnień lokalnego administratora. Po uzyskaniu takich uprawnień użytkownik może sam dokonywać weryfikacji prawa do świadczeń świadczeniobiorcy, może również nadać uprawnienia do dokonywania takiej weryfikacji swym pracownikom.*"

(dowód: akta kontroli Tom IV str. 394)

Funkcjonujące w Centrali NFZ systemy zabezpieczające (antywirus Intel Security, system antyspamowy IronPort) automatycznie generują raporty wizualizowane na stronach startowych (Dashboards) aplikacji do zarządzania i monitorowania. Strony te są na bieżąco monitorowane i analizowane przez administratorów.

(dowód: akta kontroli Tom IV str. 467-478)

Zgodnie z wyjaśnieniami Pełnomocnika ds. Ochrony Informacji Niejawnych w systemach kontroli dostępu oraz włamania i napadu jak również w systemie BMS są generowane alarmy. W przypadku wystąpienia przedmiotowych alarmów następuje reakcja ochrony fizycznej osób i mienia oraz administratorów systemu BMS. Wszystkie zdarzenia są automatycznie zapisywane w bazie danych systemu. Z bazy danych można wydrukować historię zdarzeń

(dowód: akta kontroli Tom IV str. 395)

Ustalone nieprawidłowości

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

Uwagi dotyczące badanej działalności

W toku kontroli stwierdzono, że w związku z uruchomieniem w Centrali NFZ systemu DLP Fidelis główny specjalista ds. bezpieczeństwa systemów teleinformatycznych już w lipcu 2014 r. zgłaszał potrzebę monitorowania protokołu HTTPS. W wyniku uzgodnień Departamentu Informatyki, Biura Prawnego oraz ABI ustalono, że kwestie te będą podlegały rozpatrzeniu w ramach projektu ZSZ.

(dowód: akta kontroli Tom I str. 578-582)

Prezes NFZ podał, że „*w ramach Projektu ZSZ zostanie przygotowana jedynie rekomendacja dotycząca monitoringu HTTPS natomiast sama decyzja o uruchomieniu monitoringu musi zapaść na szczeblu kierowniczym Narodowego Funduszu Zdrowia. Jednocześnie zauważyć trzeba, że Projekt ZSZ uwzględni już podjętą decyzję o uruchomieniu/nieuruchamianiu monitoringu HTTPS poprzez przygotowanie stosownych regulacji w ramach dokumentacji SZBI.*"

(dowód: akta kontroli Tom IV str. 514)

NIK pozytywnie ocenia fakt podjęcia działań zmierzających do monitorowania protokołu HTTPS i uznania ich za czynnik podniesienia poziomu bezpieczeństwa informacji w Centrali NFZ. Jednakże, do dnia zakończenia kontroli, nie przedłożono dokumentów potwierdzających podjęte działania w powyższym zakresie, co zdaniem NIK, uwzględniając fakt zgłoszenia problemu w lipcu 2014 r., świadczy o przewlekłości procesu decyzyjnego. W ocenie NIK ewentualne wprowadzenie analizy szyfrowanego ruchu sieciowego wymaga podjęcia przez kierownictwo Funduszu działań uświadamiających pracowników, ponieważ powyższe rozwiązanie wiąże się z potencjalnym naruszeniem ich prywatności.

2.4. Wymiana wrażliwych danych

Opis stanu faktycznego

Stosownie do art. 36a ust. 2 pkt. 1 lit. b ustawy o ochronie danych osobowych ABI, a jeśli nie został powołany to Administrator Danych, zobowiązany jest do zapewnienia przestrzegania przepisów o ochronie danych osobowych, w szczególności do nadzorowania opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2.

Obowiązujące w badanym okresie zasady dotyczące bezpieczeństwa danych przetwarzanych w NFZ wprowadzone zarządzeniem Nr 12/2010/POIN nie były aktualizowane, co opisano w punkcie 1.2. niniejszego wystąpienia pokontrolnego.

P.o. Zastępcy Dyrektora DI podał m.in., że „*zmiany w ustawie o ochronie danych osobowych, które weszły w życie 1 stycznia 2015 r. dotyczą w przeważającym zakresie nowej roli administratora bezpieczeństwa informacji (ABI), któremu powierzony został większy zakres obowiązków. Część obowiązków realizowanych do tej pory przez Generalnego Inspektora Danych Osobowych przeniesiona została na administratorów danych osobowych (ADO) i w konsekwencji na powołanych przez nich ABI. Na mocy postanowień Regulaminu Organizacyjnego Centrali Funduszu, z dniem 1 kwietnia 2015 r. nastąpiła likwidacja stanowiska ABI. Stanowisko takie wynika w szczególności ze Statutu NFZ stanowiącego załącznik do rozporządzenia Ministra Zdrowia z dnia 11 grudnia 2014 r. w sprawie nadania statutu NFZ, który nie wymienia ABI wśród komórek organizacyjnych zarówno centrali jak i oddziałów wojewódzkich Funduszu. Dotychczasowe zadania ABI związane z ochroną danych osobowych wykonuje Prezes Funduszu lub osoby przez niego upoważnione na podstawie imiennego upoważnienia do określonych zadań. W związku z powyższym nie było konieczności zmiany zapisów treści Polityki bezpieczeństwa w związku z wejściem w życie w dniu 1 stycznia 2015 r. przepisów znowelizowanej ustawy o ochronie danych osobowych. Nie mniej jednak w związku ze zmianami organizacyjnymi w Centrali Funduszu konieczne było podjęcie działań*

zmierzających do zmiany Zarządzenia 12/2010/POIN z dnia 29 stycznia 2010 r. w sprawie bezpieczeństwa danych przetwarzanych w NFZ. Jednocześnie do czasu zakończenia prac nad nowym zarządzeniem został opracowany Regulamin Ochrony Danych Osobowych w Centrali NFZ.

(dowód: akta kontroli Tom III str. 15)

W Centrali NFZ, w zarządzeniu Nr 12/2010/POIN, określono zasady postępowania z danymi wrażliwymi w rozumieniu ustawy o ochronie danych osobowych.

Zarządzenie w sposób ogólny określa zasady korzystania z technik kryptograficznych w celu ochrony poufności, integralności i autentyczności informacji przekazywanych elektronicznie. Przepisy § 20 ust. 1 – 2 Instrukcji wymagały, aby dostęp użytkowników do sieci Internet za pomocą urządzeń był zabezpieczony co najmniej przy użyciu urządzeń typu zapory sieciowe (firewall) i system detekcji włamań (IDS) lub systemów prewencji włamań (IPS). Do zabezpieczenia sieci LAN i stacji roboczych zalecano stosowanie skanerów antywirusowych zarządzanych centralnie z danej lokalizacji; do zabezpieczenia serwerów poczty elektronicznej – skanerów antywirusowych oraz antyspamowych zarządzanych centralnie w danej lokalizacji; zalecano również szyfrowanie połączeń w sieci informatycznej Funduszu. Zgodnie z § 20 ust. 3 Instrukcji przekazywanie danych mogło nastąpić wyłącznie za pośrednictwem bezpiecznego (szyfrowanego) kanału przesyłu danych, udostępnianego przez komórki właściwe ds. informatyki. W § 20 ust. 4 Instrukcji określono obowiązek utworzenia przez komórki właściwe ds. informatyki procedur korzystania z poczty elektronicznej wg. wytycznych zawartych w Instrukcji.

(dowód: akta kontroli Tom III str. 11, 19-57)

W badanym określenie w Centrali NFZ określono ogólne zasady przesyłania danych i informacji przez sieć publiczną. Kwestia ta została uregulowana w opisanym wyżej § 20 Instrukcji oraz w PBI.

(dowód: akta kontroli Tom III str. 19-49)

P.o. Zastępcy Dyrektora DI podał m.in., że: „*dokumenty wewnętrzne zawierające dane osobowe, w tym sensytywne, przekazywane w postaci elektronicznej pomiędzy jednostkami organizacyjnymi przekazuje się za pomocą bezpiecznego kanału przesyłu danych z autoryzowanym dostępem lub w postaci zaszyfrowanych plików na zabezpieczonych przed nadpisaniem nośnikach elektronicznych*".

(dowód: akta kontroli Tom III str. 14)

W trakcie kontroli NIK, w dniu 14 września 2015 r. Dyrektor Gabinetu Prezesa NFZ, w celu ujednolicenia postępowania z danymi osobowymi w Centrali Funduszu i Oddziałach, zwróciła się do dyrektorów Oddziałów Wojewódzkich NFZ o przekazanie pozostałym pracownikom Funduszu informacji o konieczności przestrzegania określonych w niniejszym piśmie zasad ochrony danych osobowych tj. m.in. o: zwrócenie szczególnej uwagi w przypadkach przekazywania jakichkolwiek danych osobowych za pośrednictwem poczty elektronicznej, by dane były zabezpieczone kryptograficznie; bezwzględne szyfrowanie danych będących na komputerach przenośnych i nośnikach danych typu pendrive.

(dowód: akta kontroli Tom III str. 56)

Według wyjaśnień Prezesa NFZ nośniki zawierające wrażliwe dane (taśmy backupowe systemów) są transportowane w opakowaniach ochronnych pomiędzy lokalizacjami ośrodków przetwarzania danych Centrali NFZ z wykorzystaniem samochodów służbowych NFZ z kierowcą będącym pracownikiem NFZ, pod opieką uprawnionego pracownika Departamentu Informatyki.

(dowód: akta kontroli Tom IV str. 93)

Ustalone nieprawidłowości

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

1. W zarządzeniu 12/2010/POIN poza ogólnymi zapisami, że w NFZ przetwarzane są dane osobowe (w tym wrażliwe) oraz inne dane prawnie chronione, w szczególności: medyczne, finansowe i kadrowe nie uregulowano zasad postępowania z danymi innymi niż osobowe. W praktyce regulacje te określały przede wszystkim przetwarzanie danych osobowych, nie regulowały zaś szczegółowo informacji chronionych rozumianych jako, informacje nie podlegające obligatoryjnemu obowiązkowi ochrony, ale które powinny być chronione ze względu na dobrze pojęty interes NFZ, pracowników NFZ lub podmiotów i instytucji, z którymi NFZ współpracuje. Ponadto wskazane w zarządzeniu nr 12/2010/POIN akty prawne stanowiące podstawę uregulowania zasad przetwarzania danych w NFZ dotyczyły ochrony danych osobowych (ustawa o ochronie danych osobowych, rozporządzenia wykonawcze do ustawy). Nie wskazywały natomiast ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[24] i rozporządzenia KRI.

(dowód: akta kontroli Tom I str. 79-123, Tom III str. 19-30,31-57)

W powyższej dokumentacji nie dokonano klasyfikacji informacji przetwarzanych w NFZ, w tym nie zidentyfikowano danych (nie sporządzono ewidencji informacji i danych), których ochrona nie jest prawnie wymagana, a mogłyby one zostać wykorzystane przeciwko NFZ poprzez ujawnienie, zablokowanie lub zmanipulowanie.

(dowód: akta kontroli Tom I str. 79-123, Tom III str. 3-12, 19-58)

P.o. Zastępcy Dyrektora DI podał m.in., że *„w czerwcu 2014 r. NFZ w wyniku przeprowadzonego postępowania o zamówienie publiczne zawarł umowę z zewnętrznym podmiotem o doradztwo eksperckie w procesie opracowania i wdrożenia w NFZ Zintegrowanego Systemu Zarządzania (ZSZ). (...) w ramach projektu ZSZ – Etap IV „Przeprowadzenie pilotażowego wdrożenia Systemu Zarządzania Bezpieczeństwa Informacji oraz Systemu Zarządzania Ciągłością Działania" trwają prace nad przeprowadzeniem klasyfikacji aktywów informacyjnych Funduszu. Zgodnie z przyjętymi w projekcie założeniami, klasyfikacja przeprowadzana jest w Centrali NFZ i oddziałach wojewódzkich NFZ i zawierać będzie: Zidentyfikowane grupy informacji; Wagę Informacji w zakresie utraty poufności, integralności i dostępności; Obszary przetwarzania informacji; Listę systemów informatycznych w których są przetwarzane informacje."*

(dowód: akta kontroli Tom III str. 1, 3-5)

Jak wynika z informacji udzielonych przez p.o. Zastępcy Dyrektora DI w ramach ZSZ opracowywana jest obecnie dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji obejmująca swoim zakresem wszystkie aktywa informacyjne NFZ, a w szczególności takie obszary jak: obsługa incydentów bezpieczeństwa informacji; klasyfikacja i oznaczanie informacji; nadzór nad

[24] Dz. U. z 2014 r., poz. 1114.

dokumentami i zapisami SZBI; ocena skuteczności zabezpieczeń; działania zapobiegawcze; działania korygujące; audyt wewnętrzny; badania efektywności SZBI; nadawanie, przegląd i odbieranie uprawnień; wykonywanie i testowanie kopii zapasowych.

(dowód: akta kontroli Tom III str. 15-18, Tom IV str. 96-214, 281-296)

W związku z niesporządzeniem ewidencji aktywów informacjom przetwarzanym w NFZ formalnie nie przypisano właścicieli.

(dowód: akta kontroli Tom III str. 1-2, 58)

P.o. Zastępcy DI wyjaśnił: *„Ewidencja informacji i danych zostanie stworzona w ramach projektu Zintegrowanego Systemu Zarządzania – Etap IV „Przeprowadzenie pilotażowego wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji oraz Systemu Zarządzania Ciągłością Działania". W ramach realizowanego procesu klasyfikacji aktywów informacyjnych zostaną określeni właściciele informacji*".

(dowód: akta kontroli Tom III str. 12)

W odniesieniu do sposobu, w jaki dotychczas (od 2014 r.) chroniono informacje wrażliwe[25] rozumiane jako informacje nie podlegające obligatoryjnemu obowiązkowi ochrony, ale które są chronione ze względu na dobrze pojęty interes NFZ, pracowników NFZ lub podmiotów i instytucji, z którymi NFZ współpracuje (i podstawy tego działania) p.o. Zastępcy Dyrektora DI wyjaśnił: *„W tym okresie nie było żadnego formalnego dokumentu, który określałby zasady ochrony takich informacji. Z mojej wiedzy wynika, że cześć informacji istotnych z punktu widzenia organizacji NFZ była w praktyce chroniona np. struktura sieci informatycznej LAN/WAN, architektura systemów bezpieczeństwa, informacje dotyczące struktury baz danych, dane statystyczne związane z działalnością NFZ. Przykładowo w odniesieniu do ochrony informacji dotyczących struktury baz danych, są one chronione poprzez zdeponowanie ich w postaci papierowej w skrytce bankowej, do której dostęp ma ograniczony krąg osób. Dane te są również zdeponowane w postaci elektronicznej na serwerach znajdujących się w sieci wewnętrznej (bez dostępu do sieci zewnętrznej). Dostęp do tego zasobu jest również reglamentowany poprzez udostępnienie loginu i hasła dla Naczelników Wydziałów Informatyki w Oddziałach NFZ. Kolejnym przykładem może być stosowanie wielopoziomowego dostępu do infrastruktury informatycznej. Mimo braku wprowadzenia formalnych zasad regulujących ten dostęp, w praktyce jest stosowany. Wprowadzony został np. podział haseł wg. użytkowników niższego poziomu oraz użytkowników głównych*".

(dowód: akta kontroli Tom III str. 58-60)

W badanym okresie w NFZ formalnie nie określono zasad identyfikacji i oznaczania danych i informacji, w tym danych wrażliwych czy chronionych.

(dowód: akta kontroli Tom III str. 10, 58)

P.o. Zastępcy Dyrektora DI wyjaśnił: *„W chwili obecnej prowadzone są intensywne prace nad określeniem zasad oznaczania danych i informacji, w tym danych wrażliwych"* oraz poinformował, że *„w tym okresie nie było żadnego formalnego dokumentu, który określałby zasady oznaczania danych i informacji, w tym wrażliwych w rozumieniu informacji istotnych dla NFZ, a nie chronionych przepisami prawa. W praktyce informacje te nie były oznaczane, lecz podlegały pewnej ochronie np. poprzez zobowiązanie pracowników firm trzecich do zachowania*

[25] Poza informacjami, do ochrony których NFZ jest prawnie zobowiązane, np. dane osobowe, informacje niejawne.

w tajemnicy wszelkich informacji uzyskanych podczas realizacji umów z NFZ. Taki wymóg jest obligatoryjny do każdej umowy".

(dowód: akta kontroli Tom III str. 12, 8-60)

NIK ocenia jako nierzetelne nieprzypisanie informacjom odpowiedniego poziomu ochrony, zgodnego z ich wagą dla Centrali NFZ. Na konieczność dokonania klasyfikacji informacji z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację, a także opracowanie zbioru procedur oznaczania informacji wskazuje pkt. 8.2 normy PN-ISO/IEC 27005. Zgodnie z normą zaleca się również, aby to właściciele zasobów informatycznych byli odpowiedzialni za ich klasyfikację.

2. W Centrali NFZ nie określono typu i siły algorytmów kryptograficznych dla poszczególnych poziomów ochrony danych i informacji.

(dowód: akta kontroli Tom III str. 11-12, 58-60)

P.o. Zastępcy Dyrektora DI wyjaśnił: „*Nie wiem jakie były przyczyny tego stanu rzeczy [...]. Działania w tym zakresie będą podjęte w ramach opracowywania ZSZ oraz w ramach zaleceń otrzymanych od Ministerstwa Zdrowia.*"

(dowód: akta kontroli Tom III str. 58-60)

W badanym okresie w Centrali NFZ nie dokonywano formalnych analiz konsekwencji dla systemu zabezpieczeń przed złośliwym oprogramowaniem, pobierania i wysyłania danych w postaci zaszyfrowanej.

(dowód: akta kontroli Tom III str. 14)

P.o. Zastępcy Dyrektora DI wyjaśnił: „*W pełni skuteczna analiza konsekwencji możliwa jest do zrealizowania na bazie przeprowadzonej wcześniej klasyfikacji aktywów informacyjnych NFZ*". Jak wynika z udzielonych wyjaśnień, klasyfikacja ta zostanie dokonana w ramach projektowanego ZSZ.

(dowód: akta kontroli Tom III str. 14)

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

Ocena cząstkowa

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

IV. Uwagi i wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny i uwagi wynikające z ustaleń kontroli, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[26], wnosi o:

1. Kontynuowanie działań związanych z wdrożeniem w NFZ Zintegrowanego Systemu Zarządzania, w szczególności w zakresie przyjęcia kompletnej i spójnej polityki bezpieczeństwa systemów informatycznych.
2. Przekazywanie informacji o absencjach przekraczających 30 dni zgodnie z przyjętymi uregulowaniami wewnętrznymi.
3. Zapewnienie pełnej rozliczalności systemów teleinformatycznych poprzez wyeliminowanie przypadków stosowania typowych lub domyślnych loginów administratora np. „root".

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 dyrektora Departamentu Porządku i Bezpieczeństwa Wewnętrznego Najwyższej Izby Kontroli.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK proszę o poinformowanie Najwyższej Izby Kontroli, w terminie 14 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag i wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Warszawa, dnia 17 grudnia 2015 r.

Prezes
Najwyższej Izby Kontroli
Krzysztof Kwiatkowski

Podpis

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