Zał. nr 1.

MINISTERSTWO SPRAWIEDLIWOŚCI
2015-12-29
Kancelaria Główna

PREZES
NAJWYŻSZEJ IZBY KONTROLI
Krzysztof Kwiatkowski

Wpłynęło do sekr. W.P.P.
Biura Ministra
29. 12. 2015

BUA IV

KPB.410.004.05.2015
P/15/042

Zapoznać się
Prosi o wyjaśnienie zaleceń pokontrolnych i wypracowanie odpowiedzi

5.01.2016
prosi o informację — sprawy

SEKRETARIAT
PODSEKRETARZA STANU
wpłynęło dnia 2015-12-29

02.01.2016
PODSEKRETARZ STANU
w Ministerstwie Sprawiedliwości
Bogdan Święczkowski

WYSTĄPIENIE POKONTROLNE

DYREKTOR BIURA MINISTRA
UNP 151229-00499

Pan/~~Pani~~ Grzegorz Tomala

- ☐ w ślad za wcześniejszą korespondencją
- ☐ z prośbą o uwagi (wnioski, opinię)
- ☐ proszę o rozmowę
- ☐ do wiadomości
- ☐ zgodnie z rozmową
- ☐ do realizacji
- ☒ wg kompetencji
- ☐ uwagi

Marek Łukaszewicz

Warszawa, 29.12. 2015 r.

Do wiadomości: Pan Min. B. Święczkowski

151229-00499

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. Andrzej Jakubowski, doradca prawny, upoważnienie do kontroli nr 97714 z dnia 28.09.2015 r.

(dowód: akta kontroli str. 7-8)

2. Tomasz Szczęsny, doradca ekonomiczny, upoważnienie do kontroli nr 95759 z dnia 11.08.2015 r.

(dowód: akta kontroli str. 3-4)

3. Dariusz Talarek, doradca ekonomiczny, upoważnienie do kontroli nr 93502 z dnia 02.06.2015 r.

(dowód: akta kontroli str. 5-6)

4. Bogdan Wróblewski, gł. specjalista kp., upoważnienie do kontroli nr 93501 z dnia 02.06.2015 r.

(dowód: akta kontroli str. 1-2)

Jednostka kontrolowana

Ministerstwo Sprawiedliwości, Al. Ujazdowskie 11; 00-950 Warszawa

Kierownik jednostki kontrolowanej

Marek Biernacki, Minister Sprawiedliwości od dnia 6 maja 2013 r. do dnia 22 września 2014 r.

Cezary Grabarczyk, Minister Sprawiedliwości od dnia 22 września 2014 r. do dnia 30 kwietnia 2015 r.

Ewa Kopacz, Prezes Rady Ministrów, pełniąca obowiązki Ministra Sprawiedliwości od dnia 30 kwietnia 2015 r. do dnia 4 maja 2015 r.[1]

Borys Budka, Minister Sprawiedliwości od dnia 4 maja 2015 r. do dnia 16 listopada 2015 r.

Zbigniew Ziobro, Minister Sprawiedliwości od dnia 16 listopada 2015 r.

(dowód: akta kontroli str. 1169;1809-1812)

Wykaz stosowanych skrótów

ABI – Administrator Bezpieczeństwa Informacji
ABGZ – Administrator Bezpieczeństwa Grupy Zasobów
AD – Active Directory (usługa katalogowa, przechowuje dane o użytkownikach)
AI – Administrator Informacji
AS – Administrator Systemu
BO – Biuro Ochrony – Centrum Zarządzania Kryzysowego
BDG – Biuro Dyrektora Generalnego
BKA – Biuro Kontroli i Audytu Wewnętrznego

[1] Zgodnie z art. 36 ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz. U. z 2012 r., poz. 392 ze zm.).

CBDKW – Centralna Baza Danych Ksiąg Wieczystych
CI – podsystem systemu ksiąg wieczystych
DIRS – Departament Informatyzacji i Rejestrów Sądowych
EKW – system informatyczny Elektroniczna Księga Wieczysta
EOD – system informatyczny Elektroniczny Obieg Dokumentów
FK – system informatyczny Finansowo-Księgowy
GABI – Główny Administrator Bezpieczeństwa Informacji
GABS – Główny Administrator Bezpieczeństwa Systemów
HPSM – system informatyczny (służy m.in. do zarządzania usługami)
KRK – Krajowy Rejestr Karny
KRS – Krajowy Rejestr Sądowy
MS – Ministerstwo Sprawiedliwości
NKW – Nowa Księga Wieczysta
PBI MS – Polityka Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości
PBI MS i SP - Polityka Bezpieczeństwa Informacji MS i Sądów Powszechnych
PBDO – Polityka Bezpieczeństwa Danych Osobowych
PBST – Polityka Bezpieczeństwa Systemów Teleinformatycznych
PD CBDKW – podsystem dostępowy do CBDKW
POPD – Podstawowy Ośrodek Przetwarzania Danych
RUST – Regulamin Użytkownika Systemów Informatycznych
RZ – system informatyczny Rejestr Zastawów
SI – system informatyczny
SOWKW – system obsługi wydziału ksiąg wieczystych
SZBI – System Zarządzania Bezpieczeństwem Informacji
SZJ – System Zarządzania Jakością
WAN – Wide Area Network, rozległa sieć komputerowa obejmująca cały kraj
WRP – Wydział Realizacji Projektów DIRS
WRS – Wydział Rozwoju Systemów DIRS
WUA – Wydział Utrzymania Aplikacji DIRS
WUI – Wydział Utrzymania Infrastruktury DIRS
ZOPD – Zapasowy Ośrodek Przetwarzania Danych

II. Ocena kontrolowanej działalności

Ocena ogólna

W oparciu o stosowany w metodologii Cobit 4.1[2] Model dojrzałości Najwyższa Izba Kontroli oceniła poziom zarządzania procesem zapewniania bezpieczeństwa IT oraz wspierania bezpieczeństwa w odniesieniu do systemu teleinformatycznego ksiąg wieczystych[3] jako *Powtarzalny lecz intuicyjny*.

Uzasadnienie oceny ogólnej

Powyższą ocenę uzasadniają w szczególności:

– przyjęcie jako obowiązujących dokumentów polityki bezpieczeństwa w Ministerstwie Sprawiedliwości wytworzonych w 2010 r. przez podmiot zewnętrzny i niedostosowanych do specyfiki Ministerstwa Sprawiedliwości oraz nieaktualizowanych do 2015 r., a w konsekwencji brak realnego wdrożenia systemu zarządzania bezpieczeństwem informacji;

[2] Aby oddać rzeczywisty obraz funkcjonowania kontrolowanej jednostki w zakresie objętym kontrolą NIK odszedł od kryteriów oceny określonych ustawą o Najwyższej Izby Kontroli (Dz. U. z 2015 r., poz. 1096) i zastosował ocenę opisową, w skali od 0 do 5, opartą na metodologii Cobit.4.1 (Control Objectives for Information and related Technology) - uznanego międzynarodowego standardu i zbioru dobrych praktyk w obszarze technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego.

[3] W okresie od 1 stycznia 2014 r. do zakończenia czynności kontrolnych, tj. dnia 6 listopada 2015 r.

- w okresie do lipca 2015 r. brak zasad dokumentowania incydentów związanych z bezpieczeństwem, co niosło ryzyko dla bezpieczeństwa posiadanych aktywów informacyjnych;
- postrzeganie, przed podjęciem działań zmierzających do zmiany systemu zarządzania bezpieczeństwem informacji w 2015 r., bezpieczeństwa jako domeny głównie działu IT wspartego przez zamawiane na zewnątrz ministerstwa usługi (np. audyty) i narzędzia (np. do monitorowania bezpieczeństwa);
- wzrost świadomości potrzeby zapewnienia bezpieczeństwa informacji w Kierownictwie resortu oraz podjęcie działań zmierzających do zmiany systemu zarządzania bezpieczeństwem informacji na poziomie organizacyjnym oraz dokumentacji polityk bezpieczeństwa w 2015 r., zwłaszcza w odniesieniu do ochrony przetwarzanych danych osobowych, przy braku zapewnienia wystarczających zasobów dla realizacji tych zadań;
- brak w okresie objętym kontrolą istotnych błędów i awarii systemu teleinformatycznego ksiąg wieczystych skutkujących naruszeniem poufności, integralność i dostępność zgromadzonych w nim danych przy jednoczesnym realizowaniu procesów związanych z funkcjonowaniem systemu zgodnie z przyjętymi praktykami, często bez formalnych procedur lub na podstawie procedur nie zatwierdzonych.

III. Opis ustalonego stanu faktycznego

1. Wspieranie bezpieczeństwa IT na poziomie całej organizacji

1.1 Plan zapewnienia bezpieczeństwa IT

Opis stanu faktycznego

Polityka (plan) bezpieczeństwa informacji w Ministerstwie Sprawiedliwości powstała w wyniku realizacji zamówienia publicznego w ramach projektu *Modernizacja świadczenia usług przez wymiar sprawiedliwości* współfinasowanego ze środków Europejskiego Funduszu Społecznego w wykonaniu umowy z dnia 7 czerwca 2010 r. zawartej z [redacted][4]
Zarządzenie Ministra Sprawiedliwości w sprawie wprowadzenia *Polityki Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości i sądów powszechnych* wydane zostało w dniu 27 czerwca 2012 r.[5] (dalej: zarządzenie z czerwca 2012 r.). PBI MS i SP ustanawiała strukturę dokumentacji polityki bezpieczeństwa na pięciu poziomach: ministerstwa i sądów powszechnych; jednostki organizacyjnej, w tym MS; systemu teleinformatycznego; poszczególnych systemów informatycznych oraz procedur, instrukcji i regulaminów[6]. W dniu 25 października 2012 r. PBI MS, PBST, RUST zatwierdził Główny Administrator Bezpieczeństwa Informacji – zgodnie

[4] Przedmiotem umowy było: 1/ opracowanie metodyki i analizy ryzyka; 2/ opracowanie dokumentacji polityki bezpieczeństwa; 3/ przeprowadzenie analizy ryzyka dla systemów informatycznych wymienionych w wymaganiach szczegółowych; 4/ szkolenie oraz wsparcie przy wdrożeniu polityki bezpieczeństwa. Wartość przedmiotu zamówienia wynosiła 461,16 tys. zł brutto, w tym opracowanie dokumentacji polityki bezpieczeństwa 234,24 tys. zł.

[5] Dz. Urz. MS z 2012 r., poz. 93.

[6] Dokumentacja polityki zawierała: Politykę Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości (dalej: PBI MS); szablon PBI dla jednostki organizacyjnej; Politykę Bezpieczeństwa Systemów Teleinformatycznych MS; szablon PBST dla jednostki organizacyjnej; Politykę Bezpieczeństwa Danych Osobowych MS; szablon PBDO dla jednostki organizacyjnej; Regulamin Użytkownika Systemów Teleinformatycznych MS; szablon RUST dla jednostki organizacyjnej; szablon polityki bezpieczeństwa dla systemu informatycznego oraz polityki bezpieczeństwa 7 systemów informatycznych: Rejestru Zastawów, systemu finansowo-księgowego, Active Directory Centrali MS, systemu poczty elektronicznej Exchange, elektronicznego obiegu dokumentów, Krajowego Rejestru Sądowego, Nowej Księgi Wieczystej oraz słownik pojęć używanych w dokumentach bezpieczeństwa informacji resortu sprawiedliwości.

z przewidzianym w PBI MS podziałem ról w obszarze ochrony informacji[7]. W dniu 27 grudnia 2012 r. Minister Sprawiedliwości zatwierdził PBDO oraz polityki dla systemów informatycznych w tym PBI SI NKW, tj. systemu informatycznego będącego przedmiotem szczegółowej kontroli NIK. Minister Sprawiedliwości przedstawił ww. dokumenty, jako aktualnie obowiązujące elementy Systemu Zarządzania Bezpieczeństwem Informacji.
PBI MS, PBDO, PBST, RUST oraz szablon polityki bezpieczeństwa SI (ale nie polityki opracowane dla poszczególnych systemów) udostępnione zostały pracownikom ministerstwa w wewnętrznej sieci komputerowej - intranecie (zakładka *Polityka Bezpieczeństwa Informacji*).

Dokumentacja polityki bezpieczeństwa informacji[8] (dalej: polityki) zawiera podstawowe elementy zalecane normą PN-ISO/IEC 27001[9], w szczególności podział ról w sferze zarządzania bezpieczeństwem na pion administracyjny i pion bezpieczeństwa.

(dowód: akta kontroli str. 13-82;405-411;454-494;528-591;1086)

W dniu 28 kwietnia 2015 r. zarządzeniem Ministra Sprawiedliwości powołany został Zespół ds. bezpieczeństwa informacji w MS[10] kierowany przez ABI[11], którego zadaniem było w szczególności wypracowanie rozwiązań usprawniających funkcjonowanie SZBI oraz wprowadzenie na ich podstawie odpowiednich zmian do dokumentacji polityki. Zespół pracował wg ustalonego harmonogramu (zmienianego w trybie roboczym). Kierunkowo zmiany miały zapewnić:

- zgodność dokumentacji z przepisami prawa oraz normami ISO dot. zarządzania bezpieczeństwem informacji;
- aktualizację dokumentacji polityki uwzględniającą specyfikę resortu sprawiedliwości;
- optymalny podział ról w zakresie bezpieczeństwa informacji;
- sprawne rozwiązywanie incydentów w zakresie bezpieczeństwa informacji;
- podejmowanie działań zapobiegawczych na podstawie analizy ryzyka;
- okresowe audytowanie/kontrolowanie SZBI;
- w odniesieniu do dokumentacji poszczególnych systemów informatycznych odpowiedzialność za administrowanie i bezpieczeństwo systemu, zarządzanie dostępem, zasady awaryjnego odtwarzania, tworzenie kopii zapasowych, monitorowanie, przeglądy, metody i środki uwierzytelniania, zabezpieczenie przed złośliwym oprogramowaniem, nadzór nad połączeniem z siecią publiczną.

Zespół podjął prace nad aktualizacją polityk bezpieczeństwa dla poszczególnych systemów informatycznych. W dniu 4 września 2015 r. w trakcie kontroli NIK na spotkaniu z udziałem Dyrektor Generalnej zdecydowano o zmianie priorytetów - ustalono, że w pierwszej kolejności należy zaktualizować PBI MS. Nowa, zaktualizowana dokumentacja w zakresie zarządzania bezpieczeństwem informacji uwzględnić miała przyszłą aktualizację regulaminu organizacyjnego ministerstwa oraz wnioski wynikające z *Audytu bezpieczeństwa teleinformatycznego*

---

[7] Pkt 6.3 *Odpowiedzialność za bezpieczeństwo informacji* w PBI MS. Główny Administrator Informacji – GAI, czyli Minister Sprawiedliwości – zatwierdza i wprowadza PBI MS i SP, PBDO oraz polityki bezpieczeństwa dla poszczególnych systemów informatycznych przetwarzających dane osobowe; Główny Administrator Bezpieczeństwa Informacji – GABI, czyli dyrektor Biura Ochrony – Centrum Zarządzania Kryzysowego zatwierdza i wprowadza PBI MS, PBST, RUST oraz polityki bezpieczeństwa dla poszczególnych systemów nie przetwarzających danych osobowych.

[8] Do dokumentacji polityki NIK zaliczyła: PBI MS i dokumenty związane, tj. PBST MS, RUST, PBDO oraz szablon polityki bezpieczeństwa systemu informatycznego; nie zaliczono dokumentacji z poziomu procedur, instrukcji i regulaminów.

[9] Norma PN – ISO/IEC 27001 – Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.

[10] Zarządzenie Nr 178/15/BKA Ministra Sprawiedliwości z dnia 28 kwietnia 2015 r. w sprawie powołania Zespołu do spraw bezpieczeństwa informacji w Ministerstwie Sprawiedliwości.

[11] Powołanego zgodnie z art. 36a ustawy o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 ze zm.).

przeprowadzonego przez [redacted] który został odebrany w dniu 15 lipca 2015 r.[12] (dalej: audyt z lipca 2015 r.).

(dowód: akta kontroli str. 303-321;405-411;449-453;718-721;731-732;828-838;964-967;1073-1076;1350-1353)

Kierownictwo ministerstwa zadeklarowało w obowiązującej polityce (zatwierdzonej w 2012 r.), iż cele wdrożenia SZBI, w tym m.in. zagwarantowanie właściwej ochrony informacji oraz ciągłości procesu ich przetwarzania, zostaną zapewnione m.in. przez przegląd i aktualizację polityk oraz procedur dokonywane przez odpowiedzialne osoby w celu jak najlepszej reakcji na zagrożenia i incydenty. Zgodnie z pkt. 6.1.2 PBI MS SZBI miał być monitorowany poprzez wykonywanie audytów wewnętrznych, wykonywanie audytów zewnętrznych oraz przeglądów dokonywanych przez Kierownictwo. W 2013 r. przeprowadzony został wewnętrzny *Audyt bezpieczeństwa informacji*[13] (dalej: audyt z 2013 r.), ale audytorzy odstąpili od wydania opinii w zakresie funkcjonowania kontroli zarządczej w tym obszarze[14]. W 2014 r. wykonany został audyt *Zarządzanie bezpieczeństwem informacji w wybranych grupach zabezpieczeń* (dalej: audyt z 2014 r.). Stan kontroli zarządczej oceniony został na poziomie 2.*Powtarzalny*[15]. Ponadto w 2014 r. przeprowadzony został przez audytora zewnętrznego *Audyt wydajności infrastruktury w Ministerstwie Sprawiedliwości*[16].

Ujęty w planie na 2015 r. ponowny *Audyt zarządzania bezpieczeństwem informacji w wybranych grupach zabezpieczeń* nie odbył się do zakończenia czynności kontrolnych NIK, jednak z uwagi na przeprowadzenie audytu zleconego [redacted] zachowane zostały wymogi § 20 ust. 2 pkt 14 rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności[17] (dalej: rozporządzenie KRI), w zakresie zapewnienia nie rzadziej niż raz na rok audytu bezpieczeństwa informacji.

Dokumentację polityki oraz SZBI krytycznie oceniono we wszystkich ww. audytach.

MS nie podejmowało działań w celu uzyskania certyfikatu ISO dla SZBI. *Ministerstwo Sprawiedliwości planuje w pierwszej kolejności wdrożyć zalecenia poaudytowe, a następnie w 2016 r., ponownie przeprowadzić audyt zewnętrzny m.in. w obszarze PN-ISO/IEC 27001:2014-12, celem sprawdzenia prawidłowości wdrożonych mechanizmów. Dopiero po stwierdzeniu, iż ministerstwo spełnia wszystkie założone wymogi, może zostać rozpoczęta procedura certyfikacji SZBI* – wyjaśniła Dyrektor Generalna.

(dowód: akta kontroli str. 13-41;172-302;405-411;841-858;1339-1341;1354-1369)

---

[12] Umowa Nr BDG-0452-3/15/2 z dnia 15 kwietnia 2015 r. Przedmiotem umowy było m.in. wykonanie: audytu zgodności systemów informatycznych z wymaganiami w zakresie ochrony danych osobowych w Ministerstwie Sprawiedliwości, w tym przygotowanie Polityki Bezpieczeństwa Danych Osobowych Ministerstwa Sprawiedliwości oraz Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych; Audyt zgodności zarządzania bezpieczeństwem informacji w Ministerstwie Sprawiedliwości z wymaganiami normy PN-ISO/IEC 27001, przeprowadzenie testów bezpieczeństwa (penetracyjnych).

[13] Audyt bezpieczeństwa informacji został zainicjowany przez audyt zlecony przez Ministerstwo Finansów we wrześniu 2013 r. - Zarządzanie bezpieczeństwem systemów teleinformatycznych w wybranych urzędach administracji rządowej. Przeprowadzone czynności doradcze stanowiły wstępny przegląd do opracowania programu i przeprowadzenia pogłębionych czynności audytu prowadzonych przez audytorów wewnętrznych od 17 września do 20 grudnia 2013 r.

[14] Sprawozdanie końcowe z wewnętrznego *Audytu Bezpieczeństwa Informacji* z dnia 30 grudnia 2013 r.

[15] Wg przyjętego sposobu klasyfikacji wyników (cztery poziomy dojrzałości), tj. system zarządzania obejmuje określony sposób postępowania ukierunkowany na wypełnianie minimalnych wymogów prawnych w zakresie zapewnienia bezpieczeństwa informacji w ramach zasad ogólnych, posiadający znaczące luki, niezgodności i słabości - Sprawozdanie końcowe z audytu wewnętrznego *Zarządzanie bezpieczeństwem informacji w wybranych grupach zabezpieczeń* z dnia 31 grudnia 2014 r.

[16] Celem audytu było zbadanie czy infrastruktura sieciowa MS działa poprawnie i spełnia kryteria wydajności, dostępności i niezawodności do poprawnego działania aplikacji intranetowych używanych w MS, tj. EOD i FK. Wyniki audytu omówione zostały w pkt. 1.7 wystąpienia pokontrolnego.

[17] Rozporządzenie 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 (Dz.U. z 2012 r., poz. 526 ze zm.).

Pkt. 6.3.1 PBI MS określał ogólnie, iż Kierownictwo Ministerstwa Sprawiedliwości odpowiedzialne jest za zapewnienie zasobów niezbędnych dla opracowania, wdrożenia, funkcjonowania, utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji oraz poszczególnych zabezpieczeń. Deklaracja Kierownictwa nie odnosiła się do przeznaczenia środków finansowych na bezpieczeństwo informacji. Wg zestawień sporządzonych na podstawie budżetu zadaniowego w 2014 r. na bezpieczeństwo informacji wydatkowano 2 609 tys. zł (z czego blisko 60% stanowiły wynagrodzenia osobowe i pochodne), a w 2015 r. (do 4 września) – 1 837 tys. zł.

(dowód: akta kontroli str. 13-41;768-776;1109-1121)

Obowiązek przestrzegania procedur i przepisów wewnętrznych wynikających z polityki zawierały umowy z wykonawcami systemów informatycznych, w szczególności umowa nr 38 z dnia 25 listopada 2013 r. z [redacted] *na zaprojektowanie, wykonanie i wdrożenie systemu informatycznego Elektroniczne Księgi Wieczyste*[19]. Powyższa umowa zawierała zapisy o prawie dostępu i prawie do audytu[20].

W okresie objętym kontrolą istotnie zmodernizowane zostały - w rozumieniu § 23 rozporządzenia KRI - systemy informatyczne NKW[21] oraz KRS. W ramach projektu *Wprowadzenie e-usług w zakresie ksiąg wieczystych* system NKW został w okresie od 1 lipca 2014 r. do czerwca 2015 r. zmodernizowany w zakresie architektury techniczno-systemowej oraz aplikacyjnej[22] i zmienił nazwę na Elektroniczne Księgi Wieczyste[23] (zamiennie używana jest też nazwa Elektroniczne Usługi Ksiąg Wieczystych – EUKW). Z uwagi na powyższą modernizację w skład dokumentacji bezpieczeństwa informacji dla NKW/EKW wchodziła zarówno PB SI NKW zatwierdzona 27 grudnia 2012 r., dokumenty opracowane i zatwierdzone przed 1 stycznia 2014 r.[24] oraz dokumentacja wytworzona w ramach projektu. Część dokumentacji projektowej nie została formalnie zatwierdzona, ale była stosowana – jak wyjaśnił Dyr. DIRS - *z uwagi na konieczność eksploatacji wdrożonych funkcjonalności systemu EKW.*

(dowód: akta kontroli str. 594-610;626-628;768-776;999-1004;1053-1055;1333-1336;1377-1379;1426-1547;1873-1880)

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

---

[18] Po przekształceniach [redacted] z dniem 1 października 2015 r. zmieniła nazwę na [redacted]. W wystąpieniu używana była nazwa [redacted]

[19] § 9 ust. 5 pkt 5 ww. umowy.

[20] Odpowiednio § 9 ust. 5 pkt 2 i § 3 ust. 11 umowy.

[21] W związku z wejściem w życie ustawy z dnia 24 maja 2013 r. o zmianie ustawy o księgach wieczystych i hipotece (Dz. U. poz. 941 i 1641), których skutkiem była zmiana w ustawie z dnia 6 lipca 1982 r. o księgach wieczystych i hipotece (Dz. U. z 2013 r., poz. 707 ze zm.) umożliwiająca od 1 lipca 2014 r. przeglądanie ksiąg wieczystych oraz składania wniosku o wydanie dokumentu za pośrednictwem systemu teleinformatycznego

[22] Do zakończenia czynności kontrolnych proces modernizacji systemu nie został zakończony. Zgodnie z aneksem nr 8 do umowy nr 38 z dnia 25 listopada 2013 r. z [redacted] termin kompletnej modernizacji systemu wyznaczony został na 28 listopada 2015 r. Zgodnie z umową [redacted] będzie jednak nadal realizował nadzór nad eksploatacją, świadczenie serwisu i wsparcia technicznego dla systemu.

[23] Zamiennie używana jest także nazwa Elektroniczne Usługi Ksiąg Wieczystych – EUKW, w dalszej części wystąpienia posługujemy się na oznaczenie powyższego systemu skrótem NKW/EKW, w cytatach i nazwach dokumentów zachowując użyte w nich nazwy.

[24] W ramach prac nad przygotowaniem wewnętrznych przepisów zastępujących obowiązujące procedury SZJ decyzją Dyr. DIRS z 24 czerwca 2015 r. pracownicy departamentu zobligowani zostali do zapoznania się i bezwzględnego stosowania w wykonywanych czynnościach w ramach powierzonych obowiązków dokumentów wewnętrznych systemu kontroli zarządczej departamentu (wg zaktualizowanej listy instrukcji i procedur np. procedury Nadawanie użytkownikom uprawnień do SI (B.4.2.1_v4.0), czy instrukcji - Zasady i organizacja pracy oraz nadzór nad infrastrukturą POPD_ZOPD (B..4.1.1_v7.0)).

z zapewnieniem warunków bezpieczeństwa systemów informatycznych w działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1. Zatwierdzona w 2012 r. i obowiązująca dokumentacja polityki była niedostosowana do specyfiki MS oraz niestarannie opracowana, co skutkowało niespójnością, nieczytelnością i w konsekwencji brakiem skutecznej ochrony zasobów informacyjnych ministerstwa. Nie spełniła zatem wymogów określonych w § 20 ust. 1 rozporządzenia KRI zobowiązującego podmiot realizujący zadania publiczne do opracowania i ustanowienia, utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji zapewniającego jej poufność, dostępność i integralność.

Przyjęta zarządzeniem z czerwca 2012 r. systematyka (hierarchia) dokumentacji polityki bezpieczeństwa oraz podział odpowiedzialności za zarządzanie bezpieczeństwem informacji określony w pkt 6.3 PBI MS były skomplikowane i nieprzejrzyste dla jej odbiorców. W szczególności wymienić należy:

- multiplikowanie treści dot. zasad ochrony informacji w odniesieniu do systemów informatycznych na trzech poziomach: PBI MS; PBST oraz politykach dla poszczególnych systemów;
- powielenie zadań GABI (Dyrektora BO) w zakresie nadzoru nad realizacją zapisów polityki bezpieczeństwa z zadaniami GABS (Dyrektora DIRS), tj. sprawowaniem nadzoru nad bezpieczeństwem systemów teleinformatycznych;
- nakładanie się zadań GABS, jako osoby nadzorującej bezpieczeństwo systemów teleinformatycznych z zadaniami ABGZ[25], do którego należało m.in: przygotowywanie procedur awaryjnych związanych z incydentami bezpieczeństwa, przygotowywanie dokumentów wymagań bezpieczeństwa dla systemów teleinformatycznych, nadzorowanie bezpieczeństwa systemów teleinformatycznych i analizowanie ich podatności.

Słownik przyjęty w PBI MS zawierał nieprecyzyjne i niezrozumiałe dla użytkowników pojęcia np. „informacja" zdefiniowana została jako *taki czynnik, któremu można przypisać określone znaczenie, aby móc go wykorzystać do różnych celów.*

(dowód: akta kontroli str. 13-41;214-234;768-776;841-846;932-951975-976;999-1004)

Pkt 2 PBST (*Organizacja bezpieczeństwa systemów teleinformatycznych)* stanowił, iż przetwarzanie informacji w MS musi być wykonywane na urządzeniach zgodnych z minimalnymi wymaganiami w zakresie bezpieczeństwa. Minimalne wymagania definiują standardy bezpieczeństwa (miały stanowić załącznik do PBI MS). PBI MS nie zawierała załącznika definiującego standardy bezpieczeństwa. Ponadto nie określono w polityce mierników skuteczności stosowanych zabezpieczeń.

PBI MS wielokrotnie odsyłała do procedur określonych w systemie zarządzania jakością[26], czy wewnętrznych regulacji ministerstwa, bliżej nie wskazując o jakie zapisy chodzi, co także nie sprzyjało czytelności powyższego dokumentu. Ponadto nie zawierała wykazu aktów normatywnych, zgodnie z którymi należy rozstrzygać

---

[25] Decyzją Nr BO-0452-1/12/2 Głównego Administratora Bezpieczeństwa Informacji (Dyr. BO) z dnia 25 października 2012 r. do pełnienia funkcji ABGZ wyznaczono pięć osób z Wydziału Ochrony Informacji Niejawnych BO, decyzja ta straciła moc w dniu 19 marca 2015 r. (Decyzja Dyr. BO Nr BO-I-0452-10/15/1).

[26] SZJ został wdrożony w MS w 2003 r., a po raz ostatni certyfikowany był w dniu 13 lutego 2013 r. Decyzją Dyrektora Generalnego MS z 23 lipca 2013 r. komórki organizacyjne urzędu zostały zobowiązane do podjęcia, w ramach własnych kompetencji, działań zmierzających do uporządkowania dokumentacji SZJ poprzez analizę dotychczasowych procedur. *Wraz z wdrożeniem wszystkich koniecznych regulacji, SZJ w dotychczasowej formie zostanie wycofany* – wyjaśnił Zastępca Dyr. Biura Dyrektora Generalnego. W okresie objętym kontrolą obowiązywał § 12 regulaminu organizacyjnego MS, na podstawie którego w urzędzie funkcjonuje SZJ, bez względu na aktualność dokumentów certyfikujących.

kwestie w niej nie ujęte, za wyjątkiem wskazania, iż informacje niejawne posiadają własny, niezależny od definiowanego przez niniejszą politykę system ochrony zgodny z wymaganiami ustawy o ochronie informacji niejawnych. Nie zawierała także zasad podejmowania stosownych działań (także spoza zakresu kompetencji) oraz odstępowania od działania (także należącego do obowiązków), z inicjatywy własnej lub na wezwanie (także w przypadku braku podległości służbowej) w przypadku stwierdzenia zagrożenia interesów instytucji. Dyr. BO wyjaśnił, iż przedmiotowe zasady nie zostały ujęte w polityce, gdyż stanowią część instrukcji bezpieczeństwa pożarowego dla poszczególnych budynków MS. A w odniesieniu do załącznika definiującego standardy bezpieczeństwa, że *zamieszczenie informacji o załączniku do PBI MS należy uznać za niedopatrzenie.*

Ustalenia NIK potwierdza *Ocena dokumentów Polityki Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości* przygotowana w grudniu 2013 r. w wyniku realizacji umowy zawartej przez Dyr. Biura Ochrony - Centrum Zarządzania Kryzysowego z Panem [redacted]. Ekspert wskazał m.in., że:

- Brak było jasnego określenia poziomów poszczególnych dokumentów i ich przeznaczenia.
- Poszczególne dokumenty są niespójne, tj. niejednolita terminologia, różne opisy tych samych terminów, zamienne stosowanie zupełnie odmiennych pojęć, niejasne i wzajemnie dublujące się uprawnienia i obowiązki.
- Dokumenty są sporządzone niechlujnie. Układ zawartości i formatowanie powodują, że czytelnik może mieć spore problemy w poruszaniu się po dokumentach i właściwym zrozumieniu ich treści.

(dowód: akta kontroli str. 13-51;768-776;1088-1106)

2. Brak zapisów odnośnie zapoznawania się pracowników z dokumentacją polityki oraz chaos organizacyjny dot. przechowywania stosownych oświadczeń w 2014 r. wskazuje na niespełnienie wymogów § 20 ust. 2 pkt 4 rozporządzenia KRI w zakresie zapewnienia warunków umożliwiających podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji uczestniczą w nim w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji.

PBI MS nakładała na pracowników ministerstwa oraz firm zewnętrznych realizujących prace na rzecz MS obowiązek ochrony informacji i przestrzegania zasad w niej zawartych[28]. Sposób zapoznawania się pracowników z polityką nie został jednak wskazany. RUST zawierał wzór załącznika – oświadczenia o zapoznaniu się z regulaminem, ale bez wskazania, gdzie te oświadczenia winny być przechowywane. Za zapoznanie z RUST odpowiadał przełożony użytkownika[29].

Ustalenia NIK potwierdza sprawozdanie z audytu z 2013 r.: *wskazać należy, że dokumentacja dotycząca zapoznania się pracowników z regulaminem jest niekompletna i rozproszona, tj. częściowo znajduje się w BO, a częściowo w sekretariatach komórek organizacyjnych*[30]. Ponadto *Notatka z monitoringu realizacji zaleceń Audytu bezpieczeństwa informacji* wskazuje, iż na dzień 31 grudnia 2014 r. nie dokonano zmian w RUST poprzez wskazanie miejsca przechowywania oświadczeń, natomiast ustalono i wprowadzono zasadę, że komórką organizacyjną MS właściwą do prowadzenia przedmiotowej dokumentacji jest BO, co zostało następnie zmienione w ramach reformy SZBI w 2015 r.

---

[27] Umowa Nr BO-III-260-78/13/1 z dnia 22 listopada 2013 r.

[28] Pkt 4 PBI MS.

[29] Pkt 1. 4 RUST.

[30] Sprawozdanie końcowe z wewnętrznego *Audytu Bezpieczeństwa Informacji* z dnia 30 grudnia 2013 r.

Dyr. DIRS wyjaśnił: *Każdy nowy pracownik MS od 1 czerwca 2015 r. zobowiązany jest do podpisania oświadczenia o zapoznaniu się z dokumentami, tj. PBI MS i RUST. Dodatkowo każdy pracownik musi złożyć wniosek o nadanie, modyfikację, usunięcie uprawnień użytkownika systemu EOD MS.* Wniosek zawiera oświadczenie o zapoznaniu się użytkownika z PBI MS i SP (ale nie PBI MS) oraz RUST. Powyższa zasada została wprowadzona komunikatem Biura Dyrektora Generalnego oraz DIRS opublikowanym w intranecie. Oświadczenia przechowywane były w Biurze Dyrektora Generalnego.

(dowód: akta kontroli str. 13-41;214-234;282-284;422-428;617-628)

3. W art. 7 pkt 4 ustawy o ochronie danych osobowych zawarto legalną definicję administratora danych, którym zgodnie z wolą ustawodawcy stał się każdy organ, jednostka organizacyjną, podmiot lub osoba, o których mowa w art. 3, decydująca o celach i środkach przetwarzania danych osobowych. Wypełniając treścią przedmiotową definicję, w pkt. 6.3.1 lit. d PBI MS wskazano, iż administratorem danych w ministerstwie jest Minister Sprawiedliwości. Tymczasem w zakresie spraw określonych w art. 25 ust. 4 pkt 2 ustawy z dnia 21 listopada 2008 r. o służbie cywilnej[31] (dalej: ustawa o służbie cywilnej) Administratorem Danych jest również Dyrektor Generalny MS, czego postanowienia PBDO ani PBI MS nie uwzględniały.
Wyjaśniając powyższe Minister Sprawiedliwości wskazał: *W § 4 rozporządzenia Ministra Sprawa 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*[32] (dalej: rozporządzenie w sprawie dokumentacji przetwarzania danych osobowych) *nie wskazano, że Polityka Bezpieczeństwa Danych Osobowych powinna wskazywać administratorów danych. Zaznaczyć należy, że w przekazanym kontrolerom rejestrze/wykazie zbiorów danych osobowych określono administratorów danych (Ministra Sprawiedliwości bądź Dyrektora Generalnego Ministerstwa Sprawiedliwości) dla każdego ze zbiorów danych przetwarzanych w Ministerstwie Sprawiedliwości.*
Przedstawione wyjaśnienia nie przystają do treści § 4 rozporządzenia, w którym ustawodawca wskazując elementy polityki bezpieczeństwa posłużył się sformułowaniem „zawiera w szczególności" co oznacza, iż poza elementami obligatoryjnymi wymienionymi w przedmiotowej normie, pozostawił swobodę w kształtowaniu treści polityki bezpieczeństwa dostosowanej do potrzeb jednostki. Skoro w wykazie zbiorów danych osobowych określono administratorów danych dla każdego ze zbiorów danych, a zbiory zgodnie z postanowieniami § 4 rozporządzenia winny być wskazane w PBDO, to mając na względzie fakt, iż polityka jest aktem wewnętrznym regulującym w sposób kompleksowy tematykę ochrony danych osobowych w jednostce celowym byłoby wskazanie komu przysługuje przymiot administratora danych.
Ponadto NIK zauważa, iż zatwierdzona w dniu 27 grudnia 2012 r. PBDO:

- Nie zawierała, wbrew obowiązkowi określonemu w § 4 ww. rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych, wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych osobowych, opisu struktury danych wskazujących zawartość poszczególnych pól informacyjnych i powiązań między nimi, sposobu przepływu danych pomiędzy poszczególnymi systemami. Wyjaśniając powyższe Minister Sprawiedliwości wskazał: *z uwagi na ilość zbiorów danych osobowych wykaz zbiorów danych osobowych wraz ze wskazaniem programów*

[31] Dz. U. z 2014, poz. 1111 ze zm.

[32] Dz. U. z 2004 r. Nr 100, poz. 1024.

zastosowanych do przetwarzania tych danych prowadzony jest elektronicznie. Wykaz zawiera wszystkie elementy wymagane przepisami rozporządzenia.

Zdaniem NIK nie można zaakceptować praktyki, w której element obligatoryjny polityki bezpieczeństwa wskazany enumeratywnie w § 4 rozporządzenia w żaden sposób nie został powiązany chociażby w formie załącznika z polityką. Ustawodawca w § 4 rozporządzenia wskazał elementy konieczne każdej polityki bezpieczeństwa danych osobowych (do których zaliczył wykaz zbiorów danych) bez względu na ich wielkość i ilość.

- Zezwalała w pkt 3 na przetwarzanie danych osobowych w arkuszach Excel, co jest niezgodne z § 7 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych, bowiem przy przetwarzaniu danych osobowych w arkuszach kalkulacyjnych nie są automatycznie odnotowywane dane dotyczące daty pierwszego wprowadzenia danych osobowych oraz dane dotyczące identyfikatora użytkownika wprowadzającego te dane. W wyjaśnieniach Minister Sprawiedliwości wskazał, iż: *na nieprawidłowe postanowienia w Polityce Bezpieczeństwa Danych Osobowych zwrócono uwagę po przeprowadzeniu audytu przez zewnętrzną firmę [redacted] (...) W chwili obecnej w Ministerstwie Sprawiedliwości trwają prace mające na celu utworzenie uniwersalnej aplikacji w oparciu o oprogramowanie PostGres. Aplikacja będzie posiadała funkcjonalności przewidziane w § 7 rozporządzenia Ministra Spraw Wewnętrznych i Administracji.*

(dowód: akta kontroli str. 13-41;69-82;116-118;159-171;964-967;1767-1806;)

4. Klasyfikowanie aktywów oraz określenie ich wartości dla instytucji, przydzielenie aktywom właścicieli oraz stworzenie struktury zarządzania i odpowiedzialności za aktywa są podstawowymi elementami świadomego budowania systemu zarządzania bezpieczeństwem informacji, które powinny poprzedzać stworzenie dokumentacji SZBI. Przedstawiona w PBI MS klasyfikacja aktywów jest niepełna np. nie definiuje (nie wymienia) kluczowych aktywów informacyjnych ministerstwa niezbędnych do realizacji kluczowych procesów instytucji, wraz ze wskazaniem poziomów ich ochrony i oszacowaniem kosztów naruszenia bezpieczeństwa tych informacji, co zalecały normy PN-ISO/IEC 27002 oraz PN-ISO/IEC 24762[33].

Przyjęte w PBI MS zasady klasyfikacji informacji[34] określały ogólnie, iż w ministerstwie występują aktywa publiczne; ważne aktywa (aktywa obejmujące dane osobowe oraz inne tajemnice ustawowo chronione, za wyjątkiem informacji niejawnych) oraz pozostałe aktywa informacyjne (wg wyjaśnień Dyr. BO są to informacje niejawne). Z zasad ochrony informacji klasyfikowanych[35] wynikało, że aktywa publiczne chronione być miały ze względu na ich integralność i dostępność, a aktywa ważne i pozostałe ze względu na poufność, integralność i dostępność.

Ustalenia NIK potwierdza audyt z 2014 r. Audytorzy wskazali m.in., iż:

- w MS nie przeprowadzono pełnej klasyfikacji informacji (zidentyfikowane i sklasyfikowane zostały zbiory danych osobowych) z uwzględnieniem ich wartości, wymagań prawnych, wrażliwości i krytyczności dla organizacji;
- w MS nie wprowadzono kompleksowych zasad oznaczania informacji i postępowania z nimi, zgodnych z klasyfikacją informacji przyjętą w jednostce.

---

[33] PN-ISO/IEC 27002 – Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji; PN-ISO/IEC 24762 – Technika informatyczna – Techniki bezpieczeństwa –Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie.

[34] Pkt 8.3 PBI MS.

[35] Pkt 8.4 PBI MS.

Brakuje procedur obejmujących przetwarzanie, przechowywanie, przesyłanie, zmianę klasyfikacji oraz niszczenie;
- w MS zidentyfikowane i sklasyfikowane zostały zbiory danych osobowych. Wykaz (prowadzony przez BO) zawierał tylko informacje wymagane ustawą o ochronie danych osobowych;
- dokumentacja, którą można uznać za rejestr ważnych aktywów nie zawierała wszystkich aktywów informacyjnych, o których mowa w PBI MS;
- nie wszystkie informacje, usługi, oprogramowanie/aplikacje miały przypisanych właścicieli, brakowało świadomości wśród pracowników, kto jest odpowiedzialny za poszczególne aktywa.

Audytorzy zalecili aktualizację/wdrożenie rejestru ważnych aktywów, z uwzględnieniem wymogów obowiązującej PBI MS, w tym ustalenie właścicieli takich aktywów. Dopiero w trakcie kontroli NIK w dniu 27 października 2015 r. ABI rozpoczął (od kierowników komórek organizacyjnych MS i ich zastępców) szkolenie w zakresie identyfikacji, klasyfikacji i oznaczania aktywów w MS oparte na zaleceniach norm serii PN-ISO/IEC 27000[36].

(dowód: akta kontroli str. 13-41;87-89;116-118;159-171;267-281;768-776;1983-2011)

Ponadto w dokumentacji polityki brak było odniesienia do utrzymywanych w ministerstwie systemów informatycznych. W PBI MS przyjęto definicję systemu informatycznego za ustawą o ochronie danych osobowych[37]. Jednak w dokumentach polityki posługiwano się głównie pojęciem systemy teleinformatyczne, znaczeniowo odmiennym. Ponadto w wewnętrznych dokumentach MS, a także wykazach systemów przedstawionych NIK w toku kontroli jako systemy informatyczne identyfikowano także podsystemy złożonych systemów teleinformatycznych, aplikacje, czy strony internetowe.

(dowód: akta kontroli str. 116-118;159-171;214-234;405-411;527;718-721;768-776;828-838;1053-1058;1215-1248;1342-1347)

Powyższe ustalenia wskazały na ryzyko nie zrealizowania celu polityki, tj. zapewnienia właściwej ochrony zasobów Ministerstwa Sprawiedliwości pomimo formalnego ustanowienia SZBI, a więc nie zapewnienie zrealizowania wymogów określonych w § 20 ust. 1 rozporządzenia KRI zobowiązującego podmiot realizujący zadania publiczne do wdrożenia, monitorowania, utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji zapewniającego jej poufność, dostępność i integralność.

5. Brak realnego wdrożenia SZBI w MS nie spełniało wymogów § 20 ust. 1 rozporządzenia KRI, zobowiązującego podmiot realizujący zadania publiczne do wdrożenia, utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji zapewniającego jej poufność, dostępność i integralność.

Formalne ustanowienie SZBI w 2012 r. nie oznaczało realnego wdrożenia polityki bezpieczeństwa informacji w MS. Zwracały na to uwagę także audyty wewnętrzne przeprowadzone w latach 2013-2014. I tak audyt z 2013 r. wskazał m.in., że:
- W przypadku siedmiu systemów teleinformatycznych nie wprowadzono polityk bezpieczeństwa, a w niektórych komórkach organizacyjnych objętych audytem,

[36] Norma PN-ISO/IEC 27001 w załączniku A.8.1 zaleca jak identyfikować aktywa i definiować odpowiedzialność za ich ochronę, a w załączniku A.8.2 omawia klasyfikowanie i oznaczanie informacji, w tym przypisywanie im odpowiednich poziomów ochrony. Do klasyfikacji informacji odnosi się też w pkt 8.2.1 norma PN-ISO/IEC 27002, a do identyfikowania aktywów punkt 8.2.2. normy PN-ISO-IEC 27005 (Technika informatyczna - Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji).

[37] Zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych - art. 7 pkt 2a ustawy o ochronie danych osobowych.

w tym w DIRS, nie sporządzono polityk dla wszystkich nadzorowanych systemów, bądź były one nieaktualne.

- GABI (Dyrektor BO) nie realizował zadania dotyczącego analizy ryzyka dla bezpieczeństwa informacji i utrzymywania rejestru ważnych aktywów.
- ABGZ nie realizowali prawidłowo szeregu zadań, w tym: przygotowania procedur awaryjnych w związku z incydentami bezpieczeństwa; nadzorowania przypadków naruszania bezpieczeństwa; analizy podatności systemów teleinformatycznych.
- GABS (Dyrektor DIRS) nie realizował prawidłowo m.in. delegowania pracowników do pełnienia funkcji AS; prowadzenia analizy ryzyka technologicznego; prowadzenia analizy podatności systemów teleinformatycznych.
- Rejestr incydentów nie zawierał żadnych zapisów (zadanie to przypisane było ABGZ).
- Procedury dot. zarządzania ryzykiem związanym z bezpieczeństwem informacji nie zostały zatwierdzone i wdrożone, nie przeprowadzono także udokumentowanej analizy ryzyka.
- Role przypisane administratorom systemów oraz osobom odpowiedzialnym za bezpieczeństwo systemów często wykonywane były przez te same osoby, co dotyczyło m.in. SI NKW.

W szczególności Izba zwróciła uwagę na tę ostatnią kwestię, tj. faktyczny brak rozdzielenia roli administratorów systemów od roli osób odpowiedzialnych za ich bezpieczeństwo, co było niezgodne z pkt. 6.3 PBI MS, która zgodnie z zaleceniami normy PN ISO/IEC 27001 rozdzieliła i zdefiniowała role w dwóch pionach: administracyjnym i bezpieczeństwa. Decyzją Nr 2/12/BINiSO Ministra Sprawiedliwości z dnia 3 października 2012 r. na podstawie ustawy o ochronie danych osobowych oraz zarządzenia Ministra Sprawiedliwości w sprawie wprowadzenia PBI MS i SP wyznaczeni zostali Administrator Bezpieczeństwa Informacji w Ministerstwie Sprawiedliwości (Dyr. BO – GABI) oraz podlegający mu czterej ABI – osobno w DIRS, w BI KRK oraz w innych komórkach organizacyjnych MS. Do dnia 18 marca 2015 r. rolę ABI w DIRS, pełnił pracownik, który był administratorem czterech systemów informatycznych. *Te dwie role były oczywiście sprzeczne ze sobą, bo jako ABI, w zakresie jego odpowiedzialności, musiałem kontrolować sam siebie* – wyjaśnił były ABI w DIRS.

Dla realizacji zaleceń audytu z 2013 r. zapadła decyzja o powołaniu Zespołu do opracowania rozwiązań usprawniających funkcjonowanie SZBI (w tym aktualizacji dokumentacji polityki). Zespół, któremu przewodniczył GABI (Dyrektor BO), został powołany zarządzeniem MS z czerwca 2014 r.[38] i odbył tylko jedno spotkanie, a aktualizacja dokumentacji polityki nie została wykonana. W trakcie kolejnego, przeprowadzonego w 2014 r., audytu w obszarze bezpieczeństwa informacji dokonano sprawdzenia realizacji zaleceń audytu z 2013 r. Z 14 zaleceń osiem nie zostało zrealizowanych, a pięć zrealizowano częściowo[39]. Ponadto audyt z 2014 r. wskazał m.in. na:

- brak aktualnych procedur określających zarządzanie kopiami zapasowymi;

[38] Zarządzenie Nr 121/14/BO Ministra Sprawiedliwości z dnia 13 czerwca 2014 r. w sprawie powołania Zespołu do opracowania rozwiązań usprawniających funkcjonowanie Systemu Zarządzania Bezpieczeństwem Informacji w Ministerstwie Sprawiedliwości oraz wprowadzenia zmian do obowiązującej dokumentacji Polityki Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości.

[39] Notatka z dnia 9 marca 2015 r. na posiedzenie Kierownictwa dotycząca zadań realizowanych przez Samodzielne Stanowisko do spraw Audytu Wewnętrznego w zakresie bezpieczeństwa informacji w Ministerstwie Sprawiedliwości.

– brak właściwego zarządzania dostępem użytkowników do systemu AD, w tym brak sprawowania kontroli nad procesem przyznawania praw dostępu przez ABGZ[40].

W końcu Zastępca Dyr. DIRS przyznał, iż w odniesieniu do systemu NKW/EKW nie zostały wdrożone zalecenia normy PN - ISO/IEC 27001.

(dowód: akta kontroli str. 13-41;214-234;267-284;405-411;422-428;434-444;841-846;932-951;1170-1180;1873-1878)

Zgodnie z pkt 6.3.4 lit. b PBI MS nadzór nad realizacją zapisów polityki bezpieczeństwa sprawował GABI (Dyr. BO). *Zadania związane z Polityką Bezpieczeństwa Informacji Biuro przejęło z DIRS bez wzmocnienia etatowego. Bez przydzielenia co najmniej dwóch etatów specjalistów w dziedzinie sieciowych systemów teleinformatycznych i wdrażanych w nich zabezpieczeń nie jest możliwe realizowanie zadań z powyższego zakresu* – alarmował Dyr. BO w latach 2013 – 2014 w pismach kierowanych do Ministra Sprawiedliwości, Dyrektora Generalnego i dyrektora ówczesnego Biura Organizacji, Finansów i Kontrolingu.

Uzasadniając brak wzmocnienia kadrowego Biura Ochrony – Centrum Zarządzania Kryzysowego Dyrektora Generalna wskazała m.in. na uwarunkowania rynku pracy - niekonkurencyjne wynagrodzenia dla informatyków w sektorze publicznym; zamrożenie wynagrodzeń w administracji od 2008 r.; utrzymujący się od 2013 r. najniższy poziom wynagrodzeń w MS na tle pozostałych ministerstw.

NIK dostrzega, że brak realnego wdrożenia polityki wynikał m.in. z jej schematycznych, nie dostosowanych do specyfiki ministerstwa zapisów oraz braku zasobów odpowiednich do przypisanych BO zadań. W szczególności dotyczy to określonych w pkt 9.1 PBI MS wymagań dla ABGZ, tj. rocznego doświadczenia w zarządzaniu sieciami teleinformatycznymi, serwerami, w audycie systemów informatycznych, co było niemożliwe do spełnienia - przy usytuowaniu tego stanowiska w Wydziale Ochrony Informacji Niejawnych Biura Ochrony – Centrum Zarządzania Kryzysowego.

(dowód: akta kontroli str. 13-41;422-428;445-448;514-527;733-736;1809-1812)

6. Dokumentacja polityki (PBI MS, PBST, PBDO, RUST) od zatwierdzenia w 2012 r. nie były aktualizowane, a podejmowane działania w zakresie przeglądów i aktualizacji polityk dla systemów informatycznych miały charakter doraźny, interwencyjny, co także wskazuje na niespełnienie wymogów § 20 ust. 2 pkt 1 rozporządzenia KRI zobowiązującego w ramach zarządzania bezpieczeństwem do zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.

Zarządzanie bezpieczeństwem informacji jest procesem, dlatego monitorowanie i aktualizacja polityk to klucz dla zapewnienia właściwego poziomu jego ochrony w danej instytucji. Pkt 17 PBI MS – *Zasady rozpowszechniania dokumentu PBI oraz trybu wprowadzania zmian*, stanowił kto wnosi, kto opiniuje, kto zatwierdza zmiany w dokumentacji polityki. W ramach podziału ról za aktualizację polityk bezpieczeństwa informacji na szczeblu ministerstwa, bezpieczeństwa systemów teleinformatycznych oraz regulaminu użytkowników odpowiadali ABGZ, za aktualizację polityk dla poszczególnych systemów – AI (dyrektorzy biur i departamentów), przy czym o zmiany w dokumentacji PBDO oraz polityk systemów przetwarzających dane osobowe wnosić mogli ABI.

Już w sprawozdaniu z audytu z 2013 r. stwierdzono m.in., że *dokumentacja jest niekompletna, nieaktualna i niedostosowana do specyfiki jednostki (...) dyrektorzy poszczególnych biur i departamentów (Administratorzy Informacji) nie prowadzili prawidłowego nadzoru nad przygotowaniem i aktualizacją polityk bezpieczeństwa*

[40] Ustalenia audytu odnoszące się do klasyfikacji aktywów informacyjnych MS przedstawiono w uwadze nr 4.

dla poszczególnych systemów teleinformatycznych, nad którymi sprawowali nadzór. Zalecenie audytorów dot. kompleksowego przeglądu, aktualizacji i uzupełnienia dokumentacji w 2014 r. zostało wykonane tylko w części[41], m.in. w listopadzie 2014 r. DIRS przekazał BO do zaopiniowania zaktualizowane (w oparciu o szablon polityki bezpieczeństwa dla systemu przygotowany przez [redacted] polityki dla kilkunastu systemów. Do zmiany struktury organizacyjnej w zakresie zarządzania bezpieczeństwem informacji w 2015 r. nie zostały one zaopiniowane.
Jak wyjaśnił Dyr. Biura Ochrony (GABI), żaden z pracowników Wydziału Ochrony Informacji Niejawnych, którym powierzono role ABGZ (mieli oni wnioskować o zmiany w politykach dla SI), nie posiadał wykształcenia informatycznego oraz wiedzy z zakresu funkcjonowania złożonych systemów i zapewnienia im bezpieczeństwa. Dlatego w dniu 27 sierpniu 2014 r. Dyr. BO zawarł umowę zlecenia z [redacted] dot. jego udziału w Zespole do opracowania rozwiązań usprawniających funkcjonowanie SZBI oraz opiniowania polityk dla poszczególnych systemów teleinformatycznych, w tym Systemu Dozoru Elektronicznego[42]. W okresie objętym umową nie odbyło się żadne posiedzenie ww. zespołu, a ekspert zaopiniował sześć ze 153 przekazanych do BO dokumentów.
Ponadto na dzień 29 października 2015 r. nadal trzy systemy utrzymywane przez DIRS nie posiadały polityki bezpieczeństwa.

(dowód: akta kontroli str. 13-41;214-234;282-284;1809-1812;1881;1973-1985)

7. W dniu 18 marca 2015 r. Minister Sprawiedliwości nadał klauzulę „zastrzeżone" informacjom utrwalonym w PB SI KRS, PB SI NKW, PB SI RZ, PB SI PESEL-SAD, PB SI SIS-SAD z uzasadnieniem, iż polityki dla tych systemów *to wprawdzie materiał o dużym stopniu ogólności, ale jednak będący źródłem wiedzy o sposobie zarządzania kluczowymi elementami systemu informatycznego Ministerstwa Sprawiedliwości, bazie danych, systemach operacyjnych oraz wskazuje dokumenty zawierające szczegóły dotyczące składników zainstalowanego oprogramowania; polityka bezpieczeństwa zawiera też wskazanie, w jakim dokumencie określono zasady tworzenia haseł w systemie, użycia haseł administracyjnych systemu, a także informacje o zabezpieczeniu systemu informatycznego przed szkodliwym oprogramowaniem, awarią systemu oraz sposobie odtworzenia systemu po awarii.* Zdaniem NIK odbyło się to z naruszeniem art. 5 ust. 4 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[43] (dalej: ustawa o ochronie informacji niejawnych), bowiem klauzula tajności została nadana po 26 miesiącach jawnego funkcjonowania powyższych dokumentów i sprowokowana została wnioskiem o udostępnienie powyższych polityk w trybie dostępu do informacji publicznej, co oznacza, iż przez ten okres dokumenty o statusie „zastrzeżone" pozbawione były ochrony należnej informacjom, o których stanowi art. 5 ust. 4 ww. ustawy - pozostając przez ten czas powszechnie dostępnymi. Zauważyć należy, że – co wskazał również we wniosku o nadanie klauzuli tajności Podsekretarz Stanu – jest ona dokumentem o dużym stopniu ogólności, a procedury i instrukcje są dokumentami jawnymi, zaś ujawnienie, który z wydziałów DIRS jest w ich posiadaniu, nie stanowi przesłanki uzasadniającej nadanie klauzuli „zastrzeżone". Niezrozumiałym w świetle przywołanej wyżej argumentacji jest zatem działanie Ministra Sprawiedliwości polegające na tym, że zatwierdzona (po aktualizacji) w dniu 10 sierpnia 2015 r. polityka bezpieczeństwa dla systemu informatycznego PESEL-SAD pozostała dokumentem jawnym.

---

[41] Notatka z monitoringu realizacji zaleceń zawartych w sprawozdaniu z zadania *Audyt bezpieczeństwa informacji* z dnia 20 grudnia 2013 r. skierowana przez audytora wewnętrznego do Ministra Sprawiedliwości w dniu 31 grudnia 2014 r.

[42] Umowa zlecenia Nr BO-I-0452-18/14/3 zawarta na okres od 1 września 2014 r. do 31 grudnia 2014 r.

[43] Dz. U. Nr 182, poz. 1228 ze zm.

Ponadto, skoro w świetle obowiązujących norm niedozwolone jest zawyżanie klauzuli tajności, to tym bardziej niedopuszczalne jest jej utrzymywanie (czyli de facto zawyżanie) w sytuacji, kiedy dane informacje takowej ochrony w ogóle nie wymagają – co zdaniem NIK miało miejsce w tym przypadku.
NIK zauważyła również, iż brak jest dokumentów potwierdzających fakt poinformowania pracowników i kontrahentów zewnętrznych o zastrzeżeniu ww. polityk. Wyjaśniając tę sytuację Dyr. DIRS wskazał: *dziennik ewidencyjny pism niejawnych o klauzuli „zastrzeżone" nie przewiduje odnotowywania informacji dotyczących zapoznania się pracowników DIRS z dokumentami polityk bezpieczeństwa systemów teleinformatycznych, które posiadają klauzulę „zastrzeżone". W tym zakresie nie istnieje obowiązek wynikający z przepisów prawa.*
W świetle § 3 ust. 1 instrukcji nr BO-I-021-5/14/2 z dnia 10 listopada 2014 r.[44] stanowiącego, iż informacje zastrzeżone mogą być udostępnione wyłącznie osobie uprawnionej i tylko w zakresie niezbędnym do wykonywania przez nią pracy oraz § 24 instrukcji w brzmieniu - *po zniesieniu lub zmianie klauzuli tajności, podejmuje się czynności polegające na naniesieniu odpowiednich zmian w oznaczeniu dokumentu i poinformowaniu o nich odbiorców* - nie sposób zaakceptować powyższego stanowiska Dyr. DIRS. Skoro bowiem istnieje obowiązek informowania odbiorców informacji zastrzeżonej o zniesieniu klauzuli tajności, to tym bardziej – niezależnie od struktur dziennika ewidencyjnego – powinien istnieć obowiązek poinformowania odbiorcy polityki bezpieczeństwa NKW o nadaniu klauzuli, bowiem z tą chwilą ciąży na nich obowiązek ochrony informacji niejawnych pod rygorem odpowiedzialności karnej.

(dowód: akta kontroli str. 83-84;90-96;1255-1309)

Ponadto w dniu 15 lipca 2015 r. na część dokumentacji przekazanej w związku z realizacją umowy na wykonanie *Audytu bezpieczeństwa teleinformatycznego* zawartej z [redacted], tj. *Ocenę zgodności zarządzania bezpieczeństwem informacji w Ministerstwie Sprawiedliwości z wymaganiami normy PN-ISO/IEC 27001* oraz *Raport z poziomu bezpieczeństwa teleinformatycznego dla Ministerstwa Sprawiedliwości* także nałożona została klauzula „zastrzeżone". W uzasadnieniu powyższej decyzji (zastępcy Dyrektora Biura Dyrektora Generalnego) podkreślono, iż powyższe dokumenty *zawierają informacje wrażliwe, których upublicznienie i wykorzystanie przez osoby trzecie wiąże się z dużym ryzykiem wycieku danych osobowych Ministerstwa Sprawiedliwości czy skutecznym przeprowadzeniem ataków na infrastrukturę teleinformatyczną Ministerstwa*[45].

NIK zauważa, iż treść przedmiotowych dokumentów nie wskazuje, aby ich ujawnienie mogło mieć szkodliwy wpływ na wykonywanie przez Ministerstwo Sprawiedliwości zadań określonych w art. 5 ust. 4 ustawy o ochronie informacji niejawnych. Zdaniem NIK fakt wytworzenia i przekazania przez podmiot profesjonalny raportów w formie jawnej świadczy o tym, iż przedmiotowe dokumenty nie zawierały informacji uprawniających do nadania im przymiotu „zastrzeżone", zaś nadanie im dopiero w dniu 15 lipca br. (protokolarne przekazanie końcowych raportów po uwagach Ministerstwa Sprawiedliwości) klauzuli tajności z punktu widzenia ochrony informacji niejawnych należy ocenić jako działanie bezprzedmiotowe, podobnie, jak jej dalsze utrzymywanie.

Ponadto, zgodnie z art. 6 ust. 1 ustawy o ochronie informacji niejawnych, klauzulę tajności nadaje osoba uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału. W tym przypadku podmiotem tym była firma [redacted]

---

[44] Instrukcja w sprawie sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone" w Ministerstwie Sprawiedliwości oraz zakresu i warunków stosowania środków bezpieczeństwa w celu ich ochrony.

[45] Notatka z wykonania usługi audytu bezpieczeństwa teleinformatycznego oraz opracowania dokumentacji poaudytowej z dnia 13 lipca 2015 r.

(będąca wytwórcą ww. raportów), a nie Zastępca Dyrektora Biura Dyrektora Generalnego w MS.
W toku czynności kontrolnych NIK wystąpiła do Ministra Sprawiedliwości z wnioskiem o zniesienie klauzuli „zastrzeżone" z dokumentu PB SI NKW oraz do Dyrektora Generalnego Ministerstwa Sprawiedliwości o zniesienie klauzuli z ww. raportów, przy czym w odniesieniu do *Raportu z poziomu bezpieczeństwa teleinformatycznego dla Ministerstwa Sprawiedliwości* w części, w jakiej nie odwołuje się do testów bezpieczeństwa (testów penetracyjnych). Wobec odmowy przychylenia się do ww. wniosków na podstawie art. 9 ust. 2 ustawy o ochronie informacji niejawnych Prezes NIK wystąpił do Szefa Agencji Bezpieczeństwa Wewnętrznego o rozstrzygnięcie sporu.

(dowód: akta kontroli str. 841-846;975-981;1249-1254)

1.2 Zarządzanie bezpieczeństwem IT

Opis stanu faktycznego

W 2015 r. decyzją Kierownictwa resortu rozpoczęto proces zmiany w obszarze zarządzania bezpieczeństwem informacji w MS. Wejście w życie nowego regulaminu organizacyjnego Ministerstwa Sprawiedliwości[46] (od 1 lutego 2015 r.) w konsekwencji oznaczało uproszczenie schematu zarządzania bezpieczeństwem informacji. W marcu 2015 r. na spotkaniu Kierownictwa MS poświęconemu m.in. bezpieczeństwu systemów teleinformatycznych, audytor wskazała, iż obszar bezpieczeństwa informacji nie był w pełni zarządzany, czego przyczyną był brak kompetencji w komórkach organizacyjnych realizujących działania związane z bezpieczeństwem informacji, a także brak koordynacji działań[47]. Ta ocena spowodowała podjęcie decyzji o zamówieniu w firmie zewnętrznej audytu bezpieczeństwa teleinformatycznego (ww. audytu z lipca 2015 r. realizowanego przez [redacted]. Także w marcu 2015 r. powołany został ABI zgodnie z art. 36a ustawy o ochronie danych osobowych, którego zadaniem było m.in. koordynowanie działań związanych z zapewnieniem bezpieczeństwa informacji przetwarzanych w MS. W kwietniu 2015 r. Minister Sprawiedliwości powołał ww. Zespół ds. bezpieczeństwa informacji w MS[48].
W skład powyższego Zespołu weszli kluczowi pracownicy DIRS, KRK, Biura Dyrektora Generalnego, BO[49]. Zespół miał być wsparciem dla ABI w prawnych, organizacyjnych i technicznych pracach mających na celu wypracowanie rozwiązań usprawniających funkcjonowanie SZBI i wprowadzenie na ich podstawie zmian do dokumentacji polityki. *Zasoby, z których korzysta Zespół, przypisane są do komórki Administratora Bezpieczeństwa Informacji i na 2015 r. wynosiły 250 tys. zł na audyty (wydatkowano 86 097,54 zł na audyt zewnętrzny) oraz 30 tys. zł na aktualizację dokumentacji* – wyjaśnił ABI. W ramach prac zespołu zrealizowano m.in.[50]:

---

[46] Zarządzenie Ministra Sprawiedliwości z dnia 30 stycznia 2015 r. w sprawie ustalenia regulaminu organizacyjnego Ministerstwa Sprawiedliwości (Dz. Urz. MS z 2015 r., poz. 54 ze zm.). Regulamin w strukturze Biura Kontroli i Audytu Wewnętrznego przewidywał stanowisko Administratora Bezpieczeństwa Informacji, który wykonuje zadania przewidziane w ustawie o ochronie danych osobowych, stanowisko to wyodrębnione zostało wewnętrznym regulaminem organizacyjnym BKA zatwierdzonym przez Dyrektora Generalnego MS w dniu 16 lutego 2015 r.

[47] Notatka ze spotkania Kierownictwa MS w dniu 11 marca 2015 r.

[48] Na to, że problematyka bezpieczeństwa informacji stała się ważnym zagadnieniem dla Kierownictwa resortu wskazuje także oświadczenie o stanie kontroli zarządczej Ministra Sprawiedliwości za rok 2014, w którym Dyrektor Generalna wskazała, iż główne nieprawidłowości stwierdzono m.in. w obszarze zarządzania bezpieczeństwem informacji w związku z czym zaplanowano do realizacji na rok 2015 m.in. uaktualnienie polityk bezpieczeństwa, ujednolicenie ścieżki komunikowania o występujących incydentach i podjętych działaniach zapobiegawczych i korygujących, przeprowadzenie oceny zgodności przetwarzania danych osobowych.

[49] § 3 zarządzenia w sprawie powołania Zespołu ds. bezpieczeństwa informacji.

[50] Stan na 15 lipca 2015 r.

- opracowano aktualizację polityk dla poszczególnych systemów (SIS-SAD, PESEL-SAD, KRK, EOD, system nagrywania rozmów telefonicznych), trzy pierwsze zostały zatwierdzone;
- opracowano projekt procedury nadawania, modyfikowania oraz odbierania uprawnień użytkownikom systemów (AD, poczty, dyski sieciowe, EOD, FK);
- wdrożono oświadczenie pracowników MS o zasadach przetwarzania danych osobowych oraz zasadach korzystania z zasobów teleinformatycznych;
- sporządzono analizę ryzyka dla systemów EOD i FK, strona internetowa i BIP[51];
- opracowano skrypt *Materiał szkoleniowy w zakresie ochrony danych osobowych* do wykorzystania w szkoleniu nowozatrudnionych pracowników.

Po 15 lipca 2015 r. harmonogram prac Zespołu uległ modyfikacji w związku z koniecznością podjęcia działań wynikających z zaleceń audytu przeprowadzonego przez [redacted] Za opracowanie projektów dokumentacji dla poszczególnych systemów odpowiadał właściciel systemu, nadzór nad opracowaniem dokumentacji należał do ABI, zatwierdzał ją administrator danych.

(dowód: akta kontroli str. 385-391;405-411;449-453;718-721;731-732;828-838;841-862;964-967;999-1004)

NIK ustaliła, że wyniki audytu z lipca 2015 r. wskazujące na duże ryzyko wycieku danych osobowych MS, czy skutecznego przeprowadzenia ataku na infrastrukturę teleinformatyczną ministerstwa, spowodowały natychmiastową reakcję Kierownictwa resortu. Od dnia 27 lipca 2015 r. do dnia 27 sierpnia 2015 r. na spotkaniach o charakterze roboczym z udziałem m.in. Dyrektor Generalnej, dyrektorów BO, BKA, DIRS oraz ABI oceniano zalecenia przedstawione przez audytorów oraz podejmowano decyzje o wdrożeniu organizacyjnych i technicznych rozwiązań kluczowych dla zarządzania bezpieczeństwem informacji. Realizacja zaleceń przypisana została do poszczególnych departamentów i biur. W pierwszej kolejności podjęte zostały działania interwencyjne dotyczące m.in:

- stworzenia „białej listy" urządzeń (komputery, laptopy, drukarki), które będą posiadały uprawnienia do korzystania z zasobów i usług;
- ustalenia krytyczności danych przetwarzanych przez pracowników korzystających z dysków sieciowych, a następnie uruchomienie ich szyfrowania;
- eliminacji krytycznych podatności, tj. domyślnych haseł drukarek sieciowych; nieszyfrowanych e-maili wysyłanych z aplikacji dziedzinowych; nieszyfrowanych zasobów sieciowych;
- automatyzacji zarządzania konfiguracją urządzeń bezpieczeństwa;
- ustalenia listy aplikacji „bez właściciela" i migracji wszystkich aplikacji do wspólnej platformy programowej;
- blokowania witryn internetowych (facebook, youtube);
- zatwierdzenia i wprowadzenia w życie PBDO oraz instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych Ministerstwa Sprawiedliwości[52].

Na 201 zaleceń audytorów do dnia 7 września 2015 r. 24 zostały całkowicie lub częściowo zrealizowane, m.in.:

- wprowadzono do wzoru umowy z dostawcami/wykonawcami zapis dot. zwrotu lub niszczenia danych w przypadku zakończenia współpracy z MS;

[51] W sierpniu 2015 r. sporządzona została analiza ryzyka dla systemu NKW/EKW.

[52] Ustalono na podstawie rejestru zaleceń oraz notatek ze spotkań w sprawie wdrożenia zaleceń poaudytowych w obszarze bezpieczeństwa teleinformatycznego z 27 lipca 2015 r., 4 sierpnia 2015 r., 12 sierpnia 2015 r., 24 sierpnia 2015 r.

- każdy pracownik DIRS (w szczególności administrator) został zobowiązany do stosowania określonych procesów m.in. zarządzania incydentem w systemie HPSM;
- rozpoczęła się dystrybucja służbowych nośników przenośnych z ochroną kryptograficzną;
- zatwierdzona została procedura nadawania użytkownikom uprawnień do systemów informatycznych;
- wykonana została analiza ryzyka dla systemów EOD, Famoc, FK;
- sporządzono wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych i opisem struktury zbiorów.

Podjęto także działania dotyczące klasyfikacji aktywów informacyjnych MS. Przeprowadzona została inwentaryzacja zasobów informacyjnych obejmujących dane osobowe, a do końca 2015 r. planowana była inwentaryzacja aktywów obejmujących informacje ustawowo chronione, a następnie informacji obejmujących aktywa publiczne. *W zakresie określenia kosztów utrzymania i odtworzenia poszczególnych systemów teleinformatycznych planowane było udzielenie w 2015 r. zamówienia publicznego na usługę opracowania i wdrożenia procedur, zgodnie z wymaganiami normy PN-EN ISO 22301:2014-11, która obejmie kwestie związane z kosztami ciągłości działania* – wyjaśnił Zastępca Dyr. BKA.
W dniu 20 października 2015 r. zarządzeniem Dyrektora Generalnego powołany został Zespół ds. realizacji zaleceń po audycie bezpieczeństwa teleinformatycznego MS, pod przewodnictwem zastępcy dyrektora BDG. Zakres zadań Zespołu ds. bezpieczeństwa informacji oraz Zespołu ds. realizacji zaleceń audytu będą komplementarne – zapewniła Dyrektor Generalna.

(dowód: akta kontroli str. 116-118;405-411;718-721;982-997;1073-1076;1122-1141;1350-1353;1813-1816)

Po lipcu 2015 r. dokumentacja dotycząca polityk bezpieczeństwa dla poszczególnych systemów przygotowywana była własnymi siłami (głównie we współpracy DIRS i BDG). Decyzja ta podyktowana była m.in:
- ustaleniami z audytów wewnętrznych wskazującymi, iż niektóre zapisy dokumentacji SZBI opracowanej przez [redacted] nie odpowiadają w pełni specyfice Ministerstwa Sprawiedliwości;
- koniecznością uwzględnienia ocen audytu z lipca 2015 r.;
- potrzebą uwzględnienia zapisów Regulaminu organizacyjnego Ministerstwa Sprawiedliwości oraz regulaminów wewnętrznych komórek organizacyjnych.

Przeprowadzenie aktualizacji dokumentacji SZBI wymaga przede wszystkim bardzo dobrej znajomości zasad funkcjonowania i specyfiki Ministerstwa Sprawiedliwości oraz resortu sprawiedliwości – wyjaśniła dodatkowo Dyrektor Generalna.
Ponadto stwierdzone w trakcie audytu z lipca 2015 r. braki w zakresie procedur bądź instrukcji opisujących poszczególne procesy (np. sporządzanie kopii zapasowych, zarządzanie dostępem użytkowników, metody i środki uwierzytelnienia, monitorowanie i konserwacja systemu, postępowanie z nośnikami, sposób rozpoczęcia i zakończenia pracy z systemem, aktualizacja bądź modyfikacja oprogramowania itd.) były uzupełniane w trakcie opracowywania dokumentacji dla poszczególnych systemów.
W ramach umowy z [redacted] *na zaprojektowanie, wykonanie i wdrożenie systemu informatycznego EKW* w październiku 2014 r. opracowane zostały projekty

Polityki Bezpieczeństwa Informacji Systemu Elektroniczne Księgi Wieczyste oraz dokumentów powiązanych, tj. *Architektura Bezpieczeństwa Systemu EKW, Zarządzanie ciągłością działania w Systemie EKW, Zasady bezpieczeństwa Systemu EKW, Procesy i procedury organizacji bezpieczeństwa*[53]. ABI dodał, że dokumentacja NKW/EKW będzie zatwierdzona po zakończeniu projektu, *co nie wyklucza prowadzenia prac mających na celu aktualizację części procedur i instrukcji.*

(dowód: akta kontroli str. 594-610;982-997;1073-1076;1122-1141;1350-1353;1809-1812)

Opis ról i zadań związanych z zarządzaniem bezpieczeństwem systemów teleinformatycznych przedstawione zostały w pkt 6.3 PBI MS. Nadzór nad bezpieczeństwem systemów teleinformatycznych sprawował GABS – Dyrektor DIRS (w tym delegował pracowników do pełnienia funkcji AS) utrzymywanych przez DIRS oraz ABGZ[54]. AS odpowiadali za techniczne zapewnienie bezpieczeństwa funkcjonowania systemów informatycznych. Przy czym zgodnie z wewnętrznymi regulaminami organizacyjnymi DIRS od czerwca 2013 r. strukturę departamentu tworzyły głównie wydziały odpowiedzialne za rozwój (rozwoju systemów, realizacji projektów) oraz utrzymanie (wydziały utrzymania infrastruktury i utrzymania aplikacji). W ramach WUI wyodrębnione zostały zespoły: Komputera centralnego, Serwerów, Sieci i Zasobów IT. Pracownicy poszczególnych zespołów oraz WUA wykonywali zadania techniczne, w tym zapewnienie bezpieczeństwa (np. komputerów klasy Mainframe i ich infrastruktury, serwerów, urządzeń sieciowych – WUI; czy obsługi incydentów, zarządzanie uprawnieniami dostępu – WUA).

Administratorzy systemów w DIRS wykonywali zadania na potrzeby kilku systemów jednocześnie. W przypadku systemów, których właścicielami było np. BDG administratorami byli pracownicy Biura. *Osoby wyznaczone do ról administratorów systemów wykonują zadania właściwe dla administratorów aplikacji. DIRS dostarcza i konfiguruje zgodnie z ich wytycznymi połączenia pomiędzy serwerami oraz instaluje gotowe oprogramowanie na dostarczonej infrastrukturze* – wyjaśnił rolę tych ostatnich Naczelnik WUA.

(dowód: akta kontroli str. 13-41;889-923;1191-1211;1221-1248;1342-1347;1659-1661)

Na dzień 24 września 2015 r. w posiadaniu MS było 11 egzemplarzy norm PN ISO/IEC określających wytyczne związane z zarządzaniem bezpieczeństwem informacji (w tym techniką bezpieczeństwa, ryzykiem, ciągłością działania). O zakup żadnego ze wskazanych egzemplarzy nie wystąpił DIRS, jednak Dyrektor Generalna wyjaśniła, że z poszanowaniem praw autorskich do publikacji, z zakupionych norm korzystać mogą pracownicy, dla których jest to uzasadnione zakresem wykonywanych zadań.

(dowód: akta kontroli str. 1350-1353)

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

---

[53] Powyższe dokumenty nie zostały jednak zatwierdzone do dnia zakończenia czynności kontrolnych.

[54] W uwagach w pkt 1.1 wystąpienia pokontrolnego omówiono, których zadań, wg audytu z 2013 r., GABS oraz ABGZ nie realizowali prawidłowo.

1. Realizowany w 2014 r. model przywództwa i zaangażowania w zarządzanie bezpieczeństwem informacji w MS nie spełniał wymogów określonych w § 20 ust. 1 rozporządzenia KRI zobowiązującego podmiot realizujący zadania publiczne do wdrożenia oraz doskonalenia systemu zarządzania bezpieczeństwem informacji zapewniającego jej poufność, dostępność i integralność.
Co najmniej do zmian funkcjonowania modelu zarządzania bezpieczeństwem informacji podjętych w 2015 r. „myślenie o bezpieczeństwie informacji" i rekomendowanie sposobów zapewnienia bezpieczeństwa ograniczało się do działań DIRS (utrzymującego kluczowe systemy informatyczne w MS, takie jak np. KRS, NKW/EKW, przy czym właścicielem danych w tych systemach były sądy powszechne). W szczególności zwraca uwagę brak aktywności Kierownictwa resortu[55] o czym świadczyły:

- treść notatek ze spotkań Kierownictwa Ministerstwa Sprawiedliwości odbytych w 2014 r., gdzie problematyka bezpieczeństwa informacji (w szczególności bezpieczeństwa systemów informatycznych) nie była przedmiotem uzgodnień;
- brak decyzji dot. wzmocnienia kadrowego (specjalistami w zakresie informatyki) Biura Ochrony – Centrum Zarządzania Kryzysowego, którego dyrektor odpowiadał za nadzór nad funkcjonowaniem SZBI, a pracownicy BO za nadzór nad bezpieczeństwem systemów teleinformatycznych;
- brak reakcji na brak raportu dot. stanu bezpieczeństwa informacji w 2014 r. (przedstawianie okresowych raportów o stanie bezpieczeństwa informacji zakładała PBI MS);
- treść wyjaśnień Dyr. DIRS – *Departament Informatyzacji i Rejestrów Sądowych informuje, iż nie otrzymał i nie posiada wypracowanych przez Kierownictwo Ministerstwa Sprawiedliwości rekomendacji w zakresie sposobów zapewnienia bezpieczeństwa informacji.*

Przy czym stwierdzić należy, iż Kierownictwo resortu zdawało sobie sprawę z istniejących zagrożeń o czym świadczyły np.:

- odebranie sprawozdań z *Audytu Bezpieczeństwa Teleinformatycznego* w grudniu 2013 r. oraz audytu *Zarządzanie bezpieczeństwem informacji na podstawie wybranych grup zabezpieczeń* w grudniu 2014 r.;
- informacja o stanie bezpieczeństwa teleinformatycznego w resorcie przedstawiona w sierpniu 2014 r. Ministrowi Administracji i Cyfryzacji, w której wskazano m.in. na ograniczenia etatowo-finansowe odbijające się na jakości nadzoru i wymuszające redukcję zabezpieczeń sprzętowo-programowych, w tym wykorzystywanie niewspieranego przez Microsoft od 8 kwietnia 2014 r. systemu operacyjnego Windows XP;
- przedstawione Ministrowi Administracji i Cyfryzacji w styczniu 2015 r. wyniki szacowania ryzyka bezpieczeństwa w cyberprzestrzeni w MS;
- otrzymywane przez Kierownictwo alerty z Rządowego Zespołu Reagowania na Incydenty Komputerowe (CERT.GOV.PL) dotyczące zagrożeń np. złośliwym oprogramowaniem w ministerstwie i jednostkach organizacyjnych resortu.

Ponadto NIK zauważyła brak aktywności w rekomendowaniu sposobów zapewnienia bezpieczeństwa przez powołanych do tego Głównego Administratora Bezpieczeństwa Informacji, Administratorów Bezpieczeństwa Grupy Zasobów oraz

[55] Wyjątkiem było wydanie, w reakcji na ustalenia audytu z 2013 r., zarządzenia o powołaniu Zespołu do opracowania rozwiązań usprawniających funkcjonowanie Systemu Zarządzania Bezpieczeństwem Informacji w Ministerstwie Sprawiedliwości. Nie było jednak żadnych efektów pracy Zespołu, gdyż odbył on zaledwie jedno spotkanie.

Administratorów Informacji (merytorycznych właścicieli systemów)[56]. W odniesieniu do rekomendacji merytorycznych właścicieli systemów informatycznych ABI wskazał, iż zawarte są one w dokumentacji poszczególnych systemów (zabezpieczenia organizacyjne i techniczne). Należy powtórzyć, że ustalenia audytu z 2013 r. wskazały na brak przypisania właścicieli do niektórych systemów (a także brak polityk bezpieczeństwa dla części z nich). Ponadto Naczelnik WUA poinformował, iż użytkownicy końcowi nie wskazywali na potrzebę wprowadzania zabezpieczeń.

(dowód: akta kontroli str. 214-234; 282-284;322-402;405-416;594-610;718-721;733-738;794-818; 1005-1048;1053-1058;1073-1076;1342-1347)

2. Brak obsadzenia Stanowiska do spraw Bezpieczeństwa Informacji Przetwarzanych w Systemach Teleinformatycznych (dalej: stanowisko ds. bezpieczeństwa teleinformatycznego) i wykonywanie przypisanych do niego zadań przez administratorów systemów nie odpowiadało ustanowionej w pkt. 6.3 PBI MS zasadzie rozdzielenia funkcji zarządzających i kontrolnych od funkcji administracyjno-technicznych, zalecanej przez normę PN - ISO/IEC 27001. Nie zostały zatem spełnione wymogi określone w § 20 ust. 2 pkt 4 rozporządzenia KRI w zakresie zapewnienia przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie podejmowania działań zapewniających, polegających na tym, że osoby zaangażowane w proces przetwarzania informacji uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji. W lutym 2015 r. w strukturze DIRS wewnętrznym regulaminem organizacyjnym utworzono stanowisko ds. bezpieczeństwa teleinformatycznego. Przypisano do niego wykonywanie zadań związanych m.in. z: *całością eksploatowanych systemów w zakresie bezpieczeństwa i ciągłości działania Ministerstwa i sądów; identyfikowaniem ewentualnych zagrożeń na podstawie informacji pochodzącej z całej infrastruktury teleinformatycznej oraz aplikacji; zarządzanie wykrywaniem, priorytetyzowaniem i rozwiązywaniem incydentów w zakresie bezpieczeństwa systemów teleinformatycznych.* Zdaniem NIK wymienione zadania przekraczały możliwości rzetelnego ich wykonania na jednoosobowym stanowisku przy liczbie i wielkości systemów utrzymywanych przez DIRS. Do zakończenia czynności kontrolnych powyższe stanowisko nie zostało obsadzone. Powyższego braku nie wypełniło zatrudnienie w sierpniu 2015 r. specjalisty w WUA, do którego obowiązków należało m.in. tworzenie i aktualizowanie polityk bezpieczeństwa systemów informatycznych utrzymywanych lub nadzorowanych przez DIRS; przygotowywanie listy wymagań dotyczących bezpieczeństwa informacji dla nowo tworzonych systemów i opiniowanie przygotowanej dokumentacji; zadania związane z analizą ryzyka dla poszczególnych systemów oraz raportowanie zagrożeń[57]. Zastępca Dyr. DIRS wyjaśnił ponadto, iż obowiązki przypisane do stanowiska ds. bezpieczeństwa teleinformatycznego wykonywali administratorzy systemów oraz pracownicy I i II linii wsparcia[58].

Według mnie nie ma dziś osoby, do której przypisana jest odpowiedzialność za bezpieczeństwo. Doraźnie zajmuje się tym jeden z administratorów systemów, ja i osoby z Service Desku (np. nadawanie uprawnień), każdy w swoim zakresie –

---

[56] Co omówione zostało w pkt 1.1 wystąpienia pokontrolnego w odniesieniu do realnego wdrożenia polityki bezpieczeństwa, jej przeglądów i aktualizacji.

[57] Powyższą problematyką zajmował się nadal były ABI, nowo zatrudniona osoba nie weszła też w skład Zespołu ds. bezpieczeństwa informacji.

[58] Przez I i II linię wsparcia należy rozumieć zespół osób zapewniających wsparcie techniczne w procesie zarządzania incydentami, w odniesieniu do poszczególnych systemów. I i II linia wsparcia ulokowane były w 8 sądach apelacyjnych na podstawie zarządzenia Ministra Sprawiedliwości z dnia 17 września 2014 r. w sprawie powierzenia wykonywania czynności związanych z projektowaniem, wdrożeniem i utrzymywaniem systemów informatycznych obsługujących sądy powszechne.

wyjaśnił Naczelnik WUA. Dodał też, że nikt nie analizuje raportów związanych z bezpieczeństwem (kompetencja GABS), a analizę ryzyka technologicznego (kompetencja GABS) dla dwóch systemów utrzymywanych przez DIRS wykonali administratorzy systemów.

(dowód: akta kontroli str. 405-411;594-605;903-923;930-931;1142-1145;1313-1318;1323-1324;1342-1347;1909-1913;1921-1922)

3. Zdaniem NIK na zapewnienie bezpieczeństwa systemów teleinformatycznych negatywny wpływ miały braki kadrowe oraz rotacja kadr w DIRS. W okresie objętym kontrolą – 22 miesięcy – kierowało DIRS dwóch dyrektorów i sześciu zastępców dyrektora. We wrześniu 2015 r. staż kierownictwa departamentu wynosił nie więcej niż siedem miesięcy, a na stanowisku drugiego z zastępców dyrektora DIRS od dnia 1 września 2015 r. był wakat. Nieobsadzone były też stanowiska dwóch naczelników wydziałów[59]. Na istotne dla zapewnienia bieżącego bezpieczeństwa systemów stanowisko naczelnika WUI nie wpłynęła żadna oferta spełniająca wymagania. Niepowodzeniem zakończyła się także próba obsadzenia stanowiska ds. bezpieczeństwa teleinformatycznego w wewnętrznym naborze.

Na dzień 23 września 2015 r. w DIRS zatrudnionych było 120 pracowników (118,6 etatów), a do obsadzenia pozostało 11 etatów (wakaty stanowiły 9%), dodatkowo pracę w DIRS wykonywało pięć osób delegowanych z innych komórek organizacyjnych. W okresie od dnia 1 stycznia 2014 r. do dnia 1 czerwca 2015 r. zakończyło pracę w DIRS 34 pracowników; zatrudniono 19 osób. W trakcie czynności kontrolnych NIK, tj. od 2 czerwca 2015 r. do 6 listopada 2015 r. kolejnych 10 osób zwolniło się z DIRS (a następne cztery były w okresie wypowiedzenia), dziewięć zostało zatrudnionych.

Wg. analizy kierownictwa DIRS braki kadrowe w departamencie na dzień 11 września 2015 r. wynosiły 29 etatów (czyli ok. 25 % liczby zatrudnionych, brakowało m.in. istotnych dla zapewnienia bezpieczeństwa systemów: administratora RACF[60] (dwie osoby, w nawiasach podano liczbę osób brakujących na danym stanowisku), administratora systemu z/OS[61] (2), administratora DB2[62] (2), administratora storage[63] (2), administratora monitoringu Systemu Przetwarzania Danych MS (1), administratora centralnego systemu wykonywania kopii bezpieczeństwa (1), architekta bezpieczeństwa (1), administratorów usług w WUA (5), nieobsadzone były także przewidziane regulaminem organizacyjnym z lutego 2015 r. stanowisko ds. koordynacji testów (2) oraz stanowisko ds. bezpieczeństwa teleinformatycznego (2). Na brak większości ww. administratorów zwrócili uwagę audytorzy w przedstawionej w lipcu 2015 r. *Ocenie zgodności zarządzania bezpieczeństwem informacji w MS z wymaganiami normy PN-ISO/IEC 27001.*

Szczególną uwagę zwracały braki kadrowe w WUA. *Wydział utrzymuje ponad 20 systemów teleinformatycznych, które w większości składają się z dodatkowych aplikacji - w sumie 40 podsystemów. W WUA pracuje 8 administratorów aplikacji, z których każdy ma minimum 2, a w niektórych wypadkach 5 systemów. Praca ich polega na nadzorowaniu czy systemy prawidłowo działają oraz w razie zauważenia nieprawidłowości jak najszybsze reagowanie na zauważone błędy* – wyliczał Dyr. DIRS[64]. Dyrektor Generalna uznała, że nie ma podstaw do kwestionowania powyższych danych, ale wyjaśniła: (...) *taki wzrost zatrudnienia przy aktualnym*

---

[59] Ogłoszony w lipcu nabór na stanowisko naczelnika Wydziału Architektury Korporacyjnej IT zakończył się zatrudnieniem wyłonionego kandydata od października 2015 r.

[60] Systemu bezpieczeństwa [redacted].

[61] System operacyjny komputera centralnego.

[62] Bazy danych [redacted].

[63] Sieci pamięci masowej.

[64] Pismo do Dyrektora Generalnego MS z dnia 11 września 2015 r. sygn. DIRS-VI-1010-1/15/6.

stanie funduszu wynagrodzeń nie jest możliwy do zrealizowania w całości. Ogłoszone zostały nabory na wakujące stanowiska i podjęte zostały działania polegające na oddelegowaniu do MS pracowników sądów.

(dowód: akta kontroli str. 594-605;629-637;1169;1350-1353;1576-1594;1817-1820)

Od dnia 5 sierpnia 2015 r. system NKW/EKW nie miał dedykowanego administratora[65], jeden z pracowników WUA wykonywał stosowne czynności w zastępstwie. *Brak administratora systemu powoduje wolniejszą reakcję na incydenty związane z utrzymaniem systemu lub – jak w przypadku NKW/EKW – przerzucenie odpowiedzialności za pełne utrzymanie systemu na firmę zewnętrzną, co ma z definicji negatywny wpływ na aspekt bezpieczeństwa, gdyż wiedza o administracji systemem informatycznym, jego infrastrukturze technicznej oraz relacjach pomiędzy nimi musi być przechowywania w organizacji, która system utrzymuje. (...) Przy rejestrach państwowych powinno być minimum dwóch dedykowanych administratorów do każdego systemu* – podkreślał Naczelnik WUA. Do połowy 2013 r. w osobnym wydziale, który zajmował się wyłącznie utrzymaniem i rozwojem NKW pracowało 12 osób. *Co oznaczało, że wsparcie dla wykonawcy i użytkowników sytemu było na dużo wyższym poziomie niż obecnie, a od tej chwili system został znacznie rozbudowany o nowe funkcjonalności* – ocenił tzw. administrator funkcjonalny (osoba rozliczająca umowę utrzymaniową z [redacted].

(dowód: akta kontroli str. 1342-1347;1560-1565;1575;1904-1907)

Jakkolwiek aktualne pozostają uwagi Dyrektor Generalnej odnoszące się do uwarunkowań rynku pracy, jednakże konsekwencje braków kadrowych w DIRS skutkowały ryzykiem niewypełnienia wymogów określonych w § 20 ust. 2 pkt 12 rozporządzenia KRI zobowiązującego podmiot realizujący zadania publiczne do zarządzania bezpieczeństwem informacji m.in. poprzez stworzenie warunków umożliwiających zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych.

4. W okresie objętym kontrolą nie przedstawiono Kierownictwu resortu okresowych raportów o stanie bezpieczeństwa informacji, co wskazywało na ryzyko niespełnienia wymogów określonych w § 20 ust. 1 rozporządzenia KRI zobowiązującego podmiot realizujący zadania publiczne do monitorowania, przeglądania oraz doskonalenia systemu zarządzania bezpieczeństwem informacji dla zapewnienia jej poufności, dostępności i integralności.

Zgodnie z pkt 6.3.4 PBI MS za przedstawianie okresowych raportów o stanie bezpieczeństwa informacji odpowiedzialny był GABI (Dyr. BO), ale nie były one wykonywane ze względu na brak w BO wyspecjalizowanych w tym zakresie pracowników. O ważnych zdarzeniach związanych z bezpieczeństwem przetwarzania informacji w systemach teleinformatycznych Kierownictwo MS, administratorzy informacji i administratorzy systemów powiadamiani byli przez CERT.GOV.PL lub przez BO za pośrednictwem pism lub pocztą internetową[66] – wyjaśnił Dyr. BO (GABI). ABI dodał, że istotne kwestie związane z bezpieczeństwem informacji omawiał na spotkaniach z Dyrektorem Generalnym

---

[65] Administrator systemu NKW/EKW w okresie od 1 stycznia 2014 r. do 3 lipca 2015 r. wykonywał powierzone zadanie bez formalnego powołania. A po powołaniu rozwiązał stosunek pracy po okresie zaledwie miesiąca (z datą rozwiązania umowy 30 września 2015 r.).

[66] Dyr. BO przedstawił przykładowo korespondencję wewnętrzną (z październik 2014 r.) dot. domniemanego ujawnienia na stronach internetowych MS danych dotyczących sprzętu i oprogramowania należącego do MS (zostały opublikowane na potrzeby zamówienia publicznego) oraz (z marca 2015 r.) dot. niezapewnienia właściwej ochrony stronie internetowej MS (Biuro Ministra poinformowało GABI o planowanym rozszerzeniu umowy z firma zewnętrzną dot. wsparcia technicznego, w tym zabezpieczenia witryn przed atakami na aplikację jak również usuwanie stwierdzonych podatności).

MS[67], a po wdrożeniu procedury zarządzania incydentami w systemie HPMS będzie do niego należało cykliczne informowanie Kierownictwa o zgłoszonych i rozwiązanych incydentach.

(dowód: akta kontroli str. 13-41;405-416;718-721;733-736)

5. Brak systemu zarządzania ryzykiem dla bezpieczeństwa informacji, w szczególności okresowych analiz ryzyka i planów postępowania z ryzykiem stanowiło niewypełnienie zapisów pkt 6.1.1 PBI MS oraz wymogów określonych w § 20 ust. 2 pkt 3 rozporządzenia KRI, który stanowi, iż kierownictwo podmiotu publicznego realizuje zarządzanie bezpieczeństwem informacji poprzez zapewnienie warunków umożliwiających przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowanie działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.
Zgodnie z pkt 6.3.4 lit. h PBI MS za prowadzenie analizy ryzyka bezpieczeństwa informacji odpowiadał Dyr. BO (GABI), a za analizę podatności systemów teleinformatycznych ABGZ (pracownicy BO) oraz GABS (Dyr. DIRS). W zakresie obowiązków GABS była także analiza ryzyka technologicznego w odniesieniu do systemów teleinformatycznych (pkt 6.3.7 lit. c PBI MS). Zgodnie z procedurą – zarządzanie ryzykiem[68] identyfikacja i szacowanie ryzyka winna być przeprowadzana okresowo, w terminach wyznaczonych przez GABI przez AI lub osoby przez administratorów wyznaczone.
Minister Sprawiedliwości nie przedstawił NIK rejestrów ryzyk w odniesieniu do bezpieczeństwa IT. Naczelnik Wydziału Kontroli Zarządczej i Analiz wyjaśnił: *MS nie posiada odrębnego systemu identyfikacji ryzyk dedykowanego wyłącznie do identyfikacji zagrożeń związanych z ryzykiem informatycznym.* Przedstawione zostały opracowane do planu pracy MS: analizy ryzyka dla komórek organizacyjnych MS, w których incydentalnie wymienione zostały ryzyka związane z bezpieczeństwem informacji.
Przy czym zdaniem NIK w odniesieniu do Biura Ochrony w 2014 r. analiza ryzyka przeprowadzona w ramach kontroli zarządczej nie odnosiła się do zadań związanych z pełnioną przez Dyr. BO rolą GABI, kluczową w obszarze zarządzania bezpieczeństwem informacji. Nie uwzględniała także zadań przypisanym pracownikom Biura w rolach ABGZ takich jak np. nadzór nad bezpieczeństwem systemów teleinformatycznych. Analizą objęta została tylko kwestia zapewnienia ochrony przetwarzanych danych osobowych, przy czym Dyr. BO wskazał, że działania zapobiegawcze, polegające na weryfikacji prawidłowości zapisów w polityce, nie mogły być zrealizowane z powodu nie przydzielenia do biura etatu (etatów) specjalisty ds. sieciowych systemów teleinformatycznych.
Analiza ryzyka dla DIRS za 2014 r. w zakresie utrzymania i eksploatacji centralnych systemów sądowych wskazywała m.in. na następujące zagrożenia:

- brak realizacji zadań lub opóźnienia w wykonywaniu zadań z powodu zbyt niskiego stopnia zatrudnienia;
- brak zapewnienia zasobów dla prawidłowego utrzymania systemów, brak możliwości przyjmowania nowych systemów do utrzymania;
- brak kadry z odpowiednimi umiejętnościami do efektywnego wykonywania zadań (szkolenia);

---

[67] Przykładowo ABI przedstawił notatki służbowe dot. zakończenia kontroli systemu SIS2 SAD przez GIODO (kwiecień 2015 r.) oraz spotkania przedstawicieli BKA z reprezentantami MSW na temat udostępniania sądom powszechnym danych ze zbioru PESEL za pomocą urządzeń teletransmisji (maj 2015 r.).

[68] Przygotowaną przez [redacted], ale nie zatwierdzoną.

– brak procedur technologicznych i organizacyjnych utrzymania systemów informatycznych.

Takie zagrożenia wskazane zostały także w odniesieniu do zapewnienia sprawnego funkcjonowania systemu teleinformatycznego i infrastruktury technicznej NKW.

(dowód: akta kontroli str. 13-41;97-115;119-158;454-483)

Już w sprawozdaniu z audytu z 2013 r. wskazano m.in., że w MS nie zostały zatwierdzone i wdrożone procedury zarządzania ryzykiem dla bezpieczeństwa informacji. Audytorzy pokreślili, że w MS nie był realizowany obowiązek przeprowadzenia analizy ryzyka. Kupiony przez MS program *Analizator Ryzyka* (*Risk Analyzer*) nie był wykorzystywany, a plan postępowania z ryzykiem nie został przedłożony do akceptacji Kierownictwa MS. *Notatka z monitoringu realizacji zaleceń Audytu bezpieczeństwa informacji* wskazuje, iż na dzień 31 grudnia 2014 r. zalecenie dot. wdrożenia systemu zarządzania ryzykiem nie zostało zrealizowane.
Dyrektor Generalna wyjaśniła, iż wdrożenie systemu zarządzania ryzykiem w zakresie bezpieczeństwa informacji nastąpiło w 2015 r., po zmianach organizacyjnych mających na celu usprawnienie działania SZBI. Sporządzone zostały analizy ryzyka dla systemów EOD, FK, strona internetowa MS, strona BIP, Famoc, KRK i NKW[69].
Planuje się, że raport z analizy ryzyka sporządzony zostanie najpóźniej do końca listopada 2015 r. Do momentu wprowadzenia powyższych zmian organizacyjnych obowiązek wykonywania kompleksowej analizy ryzyka nie był realizowany, a tym samym nie był używany program Risk Analyzer, ponieważ Biuro Ochrony – Centrum Zarządzania Kryzysowego nie dysponowało odpowiednio wykwalifikowaną kadrą – przyznała Dyrektor Generalna. Założono, że w ww. raporcie (sporządzonym dla kluczowych systemów i zasobów ministerstwa) znajdzie się plan postępowania z ryzykiem zawierający m.in. opis postępowania z ryzykiem, osoby odpowiedzialne, koszty realizacji.

(dowód: akta kontroli str. 214-234;282-284;445-448;794-796;999-1004;1142-1145)

6. Sposób przeprowadzenia i wykorzystania analizy ryzyka dla systemu NKW/EKW
NIK uznaje za nie wystarczający dla spełnienia wymogów określonych w § 20 ust. 2 pkt 3 rozporządzenia KRI, w zakresie w jakim powyższa analiza pozwolić miała na zminimalizowanie utraty integralności, dostępności lub poufności informacji w powyższym SI.
Analizę ryzyka dla systemu NKW/EKW w oparciu o opracowaną w 2010 r. metodykę, z wykorzystaniem programu *Analizator Ryzyka* przeprowadził w sierpniu 2015 r. były ABI w DIRS (w ramach prac Zespołu ds. bezpieczeństwa informacji). Analiza objęła całą infrastrukturę techniczną systemu ksiąg wieczystych (w sądach oraz w ministerstwie) oraz zasoby ludzkie.
Powyższa analiza zakończona została jednak na identyfikacji i szacowaniu ryzyka dla SI, tj. pierwszym (z ośmiu) etapów procesu wskazanego w stosowanej w MS procedurze – *Zarządzanie ryzykiem*, co ponadto nie wypełniało zaleceń określonych w pkt 10 (*Akceptowanie ryzyka*) oraz 11 (*Informowanie o ryzyku i konsultowanie ryzyka*) normy PN-ISO/IEC 27005. Z raportem z analizy zapoznać powinno się Kierownictwo, a następnie należało wdrożyć zasady (plan) postępowania z ryzykiem. Naczelnik WUA wprawdzie się z powyższa analizą zapoznał, ale – jak wyjaśnił - uznał ją za nieprzydatną. *Taka analiza ryzyka powinna być prowadzona „z zewnątrz", to znaczy na pewno nie przez administratorów systemów. A także dla wszystkich systemów, żeby mieć pogląd jak się to ryzyko rozkłada na wszystkie systemy utrzymywane w DIRS. Analiza ryzyka dla jednego systemu informatycznego jest bowiem bezużyteczna z powodu liczby systemów w DIRS.*

[69] Stan na dzień 27 sierpnia 2015 r. (ponadto rozpoczęła się analiza dla systemów KRS, RS, PESEL-SAD i SIS-SAD).

Szczególnie, że część ryzyk z racji swej natury jest wspólna np. powódź (ze względu na położenie POPD[70]) – wyjaśnił Naczelnik WUA. Wyniki analizy ryzyka nie wpłynęły na zmianę zabezpieczeń w systemie NKW/EKW.

(dowód: akta kontroli str. 718-721;1142-1145;1723-1756;1860-1863)

7. Podsumowując, NIK uznaje, że co najmniej do podjęcia zmian w zarządzaniu systemem bezpieczeństwa informacji w Ministerstwie Sprawiedliwości w 2015 r. nie odpowiadał on zaleceniom norm PN-ISO/IEC serii 27000 w zakresie budowania SZBI począwszy od identyfikacji aktywów, przez przeprowadzenie analizy ryzyka, po opracowanie dokumentacji dotyczącej zasad ochrony informacji, co wynikało w szczególności z braku wydzielonego zespołu - grupy ludzi o różnych kompetencjach i zakresie wiedzy z obszaru bezpieczeństwa odpowiedzialnego za stworzenie i nadzorowanie takiego systemu[71]. Nie spełnione zostały zatem wymagania określone w § 20 ust. 1 rozporządzenia KRI zobowiązującego podmiot realizujący zadania publiczne do wdrożenia, monitorowania, utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji zapewniającego jej poufność, dostępność i integralność.

Powyższe potwierdził Dyr. DIRS: *Po pierwszej analizie jaką przeprowadziłem po objęciu stanowiska stwierdziłem niski poziom świadomości i realizacji wszelkich aspektów związanych z bezpieczeństwem systemów informatycznych. Zwróciłem także uwagę na fakt, że w każdej organizacji powinna istnieć poza strukturami IT komórka, która wytycza standardy, określa regulacje dotyczące bezpieczeństwa i rozlicza z ich stosowania. W zasobach DIRS brak jest osób, które realizowałyby nawet te zadania, które zostały zapisane w obowiązującym regulaminie. To wynika z ogólnego niedoszacowania – w stosunku do zadań – zasobów departamentu.*
Poinformował także, że we wrześniu 2015 r., w trakcie kontroli NIK, zlecił firmie [redacted] opracowanie audytu i oceny obecnego stanu IT (w tym w zakresie bezpieczeństwa) w MS oraz zaproponowanie zalecanego scenariusza rozwoju IT w MS na najbliższe pięć lat[72].

(dowód: akta kontroli str. 1142-1145;2068-2080)

1.3 Testowanie, nadzorowanie i monitorowanie bezpieczeństwa

Opis stanu faktycznego

Monitorowanie jest podstawą wykrywania nieautoryzowanych zdarzeń dot. bezpieczeństwa informacji. Testy bezpieczeństwa są najskuteczniejszym sposobem identyfikowania potencjalnych zagrożeń. Problematykę tę omówiono w odniesieniu do systemu NKW/EKW, choć przyjęte w MS rozwiązania techniczne z zakresu monitorowania odnoszą się także do innych systemów informatycznych.

System EKW odziedziczył po systemie NKW część rozwiązań związanych z bezpieczeństwem, m.in. wydzielenie środowiska pracy sądów i Centralnej Informacji o Zastawach Rejestrowych, Krajowego Rejestru Sądowego oraz Ksiąg Wieczystych w ramach odseparowanej od Internetu infrastruktury WAN oraz dedykowane środowisko Active Directory. W ramach budowy usług systemu EKW wprowadzone zostały następujące rozwiązania wpływające na zwiększenie bezpieczeństwa:

---

[70] Podstawowy Ośrodek Przetwarzania Danych.

[71] Na problem ten zwrócili uwagę Dyr. DIRS oraz były ABI w DIRS.

[72] Umowa Nr 46 z dnia 14 września 2015 r.

- zastosowanie sieciowych stref backoffice i frontoffice dla całości infrastruktury realizującej różne role w systemie i odseparowanie ich za pomocą urządzeń sieciowych;
- udostępnianie dla uprawnionych instytucji usług EKW (webservice) w wydzielonych sieciach rządowych takich np. jak MEWA (sieć wydzielona Policji);
- separacja usług – dla każdej z usług dedykowano osobna pulę serwerów;
- stosowanie protokołu SSL do zabezpieczenia transmisji pomiędzy użytkownikiem a systemem;
- zastosowanie mechanizmów recaptcha[73] zabezpieczających przed aktywnością robotów internetowych.

Ponadto od połowy czerwca 2015 r. operatorzy odpowiedzialni za zapewnienie dostępu do sieci Internet zobowiązani byli do eliminacji i wykrywania ataków DDos na usługi uruchomione przez MS w sieci publicznej na podstawie umów z[redacted] oraz z[redacted].
Zgodnie z dokumentem *EKW - Architektura bezpieczeństwa*[75] w systemie NKW/EKW określono trzy obszary bezpieczeństwa: e-Usługi, System Centralny NKW i Systemy Lokalne. Opracowane zostały dedykowane dla nich wymagania i mechanizmy zabezpieczeń.

Prawidłowość działania systemu NKW/EKW była monitorowana w następujący sposób:

- w zakresie dostępnych w sieci Internet usług (aplikacja ogólnodostępna) wykorzystywana była usługa zewnętrznego monitoringu świadczonego przez portal WatchScript (odczytywanie czy strona jest dostępna) oraz skrypty monitorujące;
- w zakresie aplikacji centralnych funkcjonujących w sieci MS oraz sieci WAN (aplikacja CI, Centralny Rejestr Zawiadomień z/do ZSIN, obsługa kolejki) monitorowana była automatycznie infrastruktura sprzętowa oraz dostępność poszczególnych usług;
- w zakresie infrastruktury techniczno–systemowej i sieciowej monitoring realizowany był w oparciu o narzędzia SCOM firmy Microsoft, netCrunch (infrastruktura sieciowa) oraz mechanizmy automatycznego monitorowania vCentrer, tj. zużycie zasobów systemowych (pamięć, procesor, przestrzeń dyskowa);
- prawidłowość działania była także monitorowania przez operatorów POPD w systemie pracy ciągłej z wykorzystaniem procedur utrzymaniowych oraz na podstawie zgłoszeń użytkowników w Service Desk.

(dowód: akta kontroli str. 594-610;1556-1565)
W kontrolowanym okresie przeprowadzono testy bezpieczeństwa systemu NKW/EKW w zakresie aplikacji internetowych EKW (aplikacja ogólnodostępna, aplikacja branżowa) - przez wykonawcę [redacted] na etapie uruchomiania usług (przed

---

[73] Narzędzie służące do zabezpieczania stron internetowych przed publikowaniem danych wysyłanych przez automatyczne roboty, za pomocą określonych zadań lub pytań sprawdza, czy tekst (formularz) został napisany/wypełniony przez maszynę, czy przez człowieka.

[74] Umowy nr 26 z dnia 13 maja 2015 r. z[redacted] oraz nr 28 z dnia 15 maja 2015 r. z[redacted] na zapewnienie Ministerstwu Sprawiedliwości dostępu do sieci Internet w oparciu o zestawione i utrzymywane przez wykonawców łącza dostępowe wraz z niezbędnymi urządzeniami teletransmisyjnymi w dwóch lokalizacjach Al. Ujazdowskie 11 oraz ul. Czerniakowska 100 zawarte zostały na okres 1 roku w wyniku rozstrzygnięcia postępowań o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego. Powyższą ochroną objęte były także inne systemy z dostępem do sieci publicznej np. KRS, KRK.

[75] Przygotowanym w ramach projektu *Wprowadzenie e-usług w zakresie ksiąg wieczystych*, realizowanego przez [redacted] do zakończenia czynności kontrolnych dokument nie był zatwierdzony, ale przedstawiał aktualną strukturę systemu.

1 lipca 2014 r.) oraz testy penetracyjne wykonane przez [redacted][76] (w okresie październik 2014 r. – luty 2015 r.). W drugim przypadku wskazano 13 podatności, przy czym w żadnym wypadku ryzyko naruszenia bezpieczeństwa informacji nie osiągnęło poziomu krytycznego, w trzech przypadkach określono je jako wysokie, a w pięciu jako średnie. Do każdej z podatności [redacted] przedstawiła rekomendacje[77]. Uzgodniono z wykonawcą ich usunięcie w etapie 11 projektu - podczas wdrożenia usług pełnych EKW, tj. do dnia 28 listopada 2015 r. *W okresie od zidentyfikowania podatności do dnia 30 września br. nie stwierdzono wykorzystania którejkolwiek z podatności przez jakiegokolwiek napastnika* – poinformował Dyr. DIRS.

(dowód: akta kontroli str. 594-610;1313-1318;1556-1559)

Ustalone nieprawidłowości

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

1.4 Incydenty związane z bezpieczeństwem

Opis stanu faktycznego

Obowiązująca PBI MS przyjęła definicję incydentu na podstawie normy PN-ISO/IEC 17799:2007 – *pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań Ministerstwa i zagrażają bezpieczeństwu informacji.* Powyższa definicja wskazuje, że ewidencjonowane i obsługiwane powinny być także zdarzenia, które nie wywołały skutku, ale stwarzały prawdopodobieństwo jego wystąpienia. W §§ 39 i 40 RUST określono m.in., iż obowiązkiem każdego użytkownika jest reagowanie na niepoprawne działania sprzętu i oprogramowania; wszystkie zaistniałe incydenty oraz podatności należy bezzwłocznie zgłaszać do działu informatyki. W przypadku zgłoszenia incydentów i podatności dotyczących danych osobowych, należy powiadomić ABI. W PBST nie zamieszczono regulacji odnośnie zarządzania incydentami.

W *Instrukcji użytkownika service desk* – dostępnej dla pracowników MS z poziomu strony intranetowej wśród czterech typów zgłoszeń wyróżniony został incydent, zdefiniowany w następujący sposób: *jeśli potrzebujesz pomocy w usunięciu awarii lub innej niesprawności sprzętu albo oprogramowania – wybierz incydent.*[78] Powyższa definicja nie odnosiła się zatem do incydentów związanych z bezpieczeństwem informacji i nie wyczerpywała możliwych zdarzeń związanych z naruszaniem bezpieczeństwa informacji.

(dowód: akta kontroli str. 13-41;1377-1379)

Zespół ds. bezpieczeństwa informacji w MS podjął w 2015 r. działania w zakresie prac nad wdrożeniem rejestru incydentów związanych z bezpieczeństwem teleinformatycznym, poprzez zmodyfikowanie systemu HPSM. W ramach prac Zespołu opracowany i wdrożony został projekt *Procedury obsługi incydentów w zakresie bezpieczeństwa w Ministerstwie Sprawiedliwości*[79]. Projekt odnosił się do zgłoszeń pracowników oraz CERT.GOV.PL, nie obejmował kontrahentów zewnętrznych i dostawców usług. W systemie HPSM zdefiniowana została usługa

[76] Na podstawie umowy nr 65 z dnia 29 sierpnia 2014 r.

[77] Raport końcowy z testów bezpieczeństwa aplikacji Elektroniczne Księgi Wieczyste ekw.ms.gov.pl dla Ministerstwa Sprawiedliwości, luty 2015 r.

[78] Zgłoszenia użytkowników odbierane były przez I linię wsparcia, czyli Service Desk, powyższa funkcjonalność w systemie HPSM udostępniona została z dniem 24 września 2013 r.

[79] Na dzień 28 września 2015 r. powyższy projekt nie był zatwierdzony.

(USL-099) odnoszącą się do bezpieczeństwa teleinformatycznego[80]. Określono sposób zgłaszania incydentów, reakcji i obsługi incydentu, prowadzenia rejestru oraz monitorowania, odnotowywano m.in. kto zgłosił incydent, kto go obsłużył, w jaki sposób i w jakim czasie. Powyższa procedura nie zawierała wskazań odnośnie analizy po zdarzeniowej.

Decyzją Dyr. DIRS z 24 czerwca 2015 r. pracownicy departamentu zobowiązani zostali do realizacji procesów dot. zarządzania incydentami zgodnie z ich implementacją w HPSM. NIK ustaliła, że po wdrożeniu USL-099 do dnia 8 października 2015 r. użytkownicy zgłosili sześć incydentów związanych z bezpieczeństwem[81] z czego cztery zakwalifikowane zostały jako naruszenie polityki bezpieczeństwa informacji. Zarejestrowano także zalecenie z CERT.GOV.PL (w sprawie ujawnienia adresów IP i domeny) oraz alert CERT.GOV.PL, w związku z ujawnieniem, iż z jednego z adresów IP miało miejsce połączenie z siecią botnet, co mogło świadczyć o jego zainfekowaniu.

Współpraca pomiędzy MS i CERT.GOV.PL odbywała się zgodnie z *Polityką Ochrony Cyberprzestrzeni RP*, na podstawie której Rządowy Zespół Reagowania na Incydenty Komputerowe pełni rolę głównego zespołu CERT dla administracji rządowej. Współpraca była sformalizowana i polegała na przekazywaniu informacji o incydentach wykrywanych w infrastrukturze teleinformatycznej MS oraz sądów bezpośrednio do wyznaczonych osób, w tym pracowników DIRS. Ponadto zawarte zostało porozumienie pomiędzy Agencją Bezpieczeństwa Wewnętrznego a DIRS odnośnie udziału w projekcie ARAKIS 2.0 dot. wczesnego ostrzegania o zagrożeniach występujących w sieci Internet. Przedstawiciele DIRS nie byli członkami organizacji/platform wspierających wymianę informacji o zagrożeniach w dziedzinie bezpieczeństwa.

(dowód: akta kontroli str. 405-411;611-613;653-666;718-721;748-759;794-796;819-825;1313-1318;1333-1336;1560-1565;1570-1574;1605-1658;1834-1859)

W MS nie powołano zespołu reagowania na incydenty. Z wewnętrznego regulaminu organizacyjnego DIRS[82] wynika, iż zadania w zakresie obsługi zdarzeń dotyczących bezpieczeństwa informacji, w tym incydentów należały do pracowników wydziałów WUI oraz WUA DIRS, tj. II linii wsparcia. Pracownicy, do kompetencji których należała odpowiedzialność za zapewnienie technicznego bezpieczeństwa systemów informacje o zdarzeniach zagrażających bezpieczeństwu otrzymywali z BKA (audyty, ABI), kierownictwa DIRS, z I linii wsparcia, BO (np. o przerwach w dostawie prądu). W WUI w pracach na potrzeby wszystkich systemów utrzymywanych w DIRS, w tym NKW/EKW, uczestniczyły osoby z zespołów Sieci, Komputera Centralnego oraz Serwerów, przy czym żaden z pracowników nie był przypisany do konkretnego systemu. W WUA za obsługę zdarzeń dot. bezpieczeństwa odpowiadali administratorzy systemów[83].

(dowód: akta kontroli str. 594-605;903-923;1377-1379)

Ww. dokument *Architektura bezpieczeństwa systemu EKW* w pkt 7 *(Identyfikacja zagrożeń)* wylicza 30 zidentyfikowanych dla EKW kategorii zagrożeń[84]. Dla okresu objętego kontrolą Dyr. DIRS wskazał odpowiadające im incydenty w trzech

---

[80] Z karty usługi wynikało, że uwzględniono cztery podkategorie incydentu – naruszenie PBI, alert o cyberataku, zalecenie oraz ostrzeżenie (np. z CERT.GOV.PL). Usługa była realizowana przez WUI DIRS. Powyższa funkcjonalność w HPSM została udostępniona użytkownikom z dniem 28 lipca 2015 r., pierwsze zgłoszenie zarejestrowano 31 lipca 2015 r.

[81] Zgłoszenia od użytkowników kategoryzowała I linia wsparcia, zgłoszenia od CERT.GOV.PL rejestrowane były automatycznie.

[82] W okresie kontroli obowiązywały Regulamin organizacyjny DIRS z dnia 28 czerwca 2013 r. oraz Wewnętrzny regulamin organizacyjny DIRS z dnia 23 lutego 2015 r.

[83] Jak wskazano w pkt 1.2 wystąpienia od dnia 5 sierpnia 2015 r. system NKW/EKW nie miał dedykowanego administratora.

[84] Począwszy od awarii infrastruktury, poprzez ataki na sieć, serwery, włamanie i zniszczenie danych, nielegalne przetwarzanie danych, użycie nieautoryzowanego oprogramowania, po błędy pracowników i kradzież informacji.

kategoriach: 26 przypadków błędów w oprogramowaniu systemu, 26 przypadków ataków znanego malware oraz osiem przypadków awarii/niedostępności bloków architektonicznych i aplikacji udostępnianych przez CPD i mających wpływ na funkcjonowanie systemu[85]. *Dokument przygotowany przez Wykonawcę, pomimo dobrej jakości nie odpowiada zasobom kadrowym Ministerstwa Sprawiedliwości, w szczególności służb informatycznych. Skuteczna realizacja monitorowania i ewidencjonowania zagrożeń będzie rozłożona w czasie* – podkreślił Dyr. DIRS.

Incydenty związane z niedostępnością usług w obszarze ksiąg wieczystych, w tym awarie, na podstawie umowy nr 38 diagnozowała i rozwiązywała [redacted] świadcząca – poza rozbudową systemu - usługi utrzymaniowe[86]. [redacted] zobowiązana była w każdym miesiącu sporządzić protokół dot. prowadzenia usługi utrzymaniowej, nadzór nad jej wykonaniem sprawował tzw. administrator funkcjonalny w WUA. Błędy w oprogramowaniu systemu usuwane były przez wykonawcę w trybie reklamacji. W kontrolowanym okresie nie było błędów skutkujących utratą lub uszkodzeniem danych.

W odniesieniu do analizy nieskutecznych incydentów naruszenia bezpieczeństwa NKW/EKW Dyr. DIRS wyjaśnił, iż: *odnotowywane są setki incydentów polegających na próbach skanowania portów usług MS. Są one odfiltrowywane do właściwego ruchu biznesowego za pomocą urządzeń sieciowych (firewalle aplikacyjne). Jednocześnie MS nie prowadzi typowego rejestru incydentów naruszenia bezpieczeństwa innego niż logi urządzeń sieciowych i serwerów aplikacyjnych, gdyż z uwagi na jawny charakter danych ksiąg wieczystych użytkownicy internetowi mogą zadawać zgodnie z prawem zapytania o dowolne księgi wieczyste zgromadzone w Centralnej Bazie Danych Ksiąg Wieczystych, których numery są im znane. Jedynym zabezpieczeniem jest mechanizm racaptcha, którego celem jest jedynie ograniczenie działania automatów działających w sieci Internet pobierających masowo (automatycznie) dane ksiąg wieczystych.*

(dowód: akta kontroli str. 594-610;617-628;1556-1569;1909-1913;2051-2059)

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

1. Ogólne zasady zarządzania incydentami zawarte w pkt 14 PBI MS oraz obowiązujące w MS procedury dotyczące incydentów naruszających bezpieczeństwo informacji odnosiły się wyłącznie do zasad ich dokumentowania, nie zawierały regulacji dot. zbierania związanych z nimi dowodów pod kątem naruszenia przepisów prawa, regulacji wewnętrznych oraz wymagań związanych z zawartymi umowami z dostawcami usług informatycznych, co nie spełniało zaleceń określonych w pkt 16 (*Zarządzanie incydentami związanymi z bezpieczeństwem informacji*) normy PN-ISO/IEC 27002.

---

[85] Np. w dniu 17 września 2015 r. miała miejsce awaria systemu centralnego EUKW (aplikacja ogólnodostępna i branżowa) polegająca na braku możliwości zalogowania się do aplikacji przez użytkowników uwierzytelnionych (komorników, notariuszy), a aplikacja wystawiona w sieci publicznej (dla każdego, bez uwierzytelnienia) miała przerwy w dostępie.

[86] Zdarzały się przypadki, że [redacted] nie była w stanie sama rozwiązać problemu np. w nocy z 13 na 14 lutego 2015 r. spłonął Most Łazienkowski w Warszawie, wskutek czego przerwany został ring światłowodowy łączący m.in. POPD i ZOPD, co mogło skutkować niedostępnością systemu dla sądów, jednakże zdarzenie to miało miejsce w czasie przerwy technicznej i DIRS uruchomił usługę transmisji danych przez inny most.

Ponadto prowadzona w MS ewidencja incydentów w okresie co najmniej do lipca 2015 r. nie zapewniała odpowiednich warunków dla analizowania przypadków naruszania bezpieczeństwa informacji w celu doskonalenia systemu zabezpieczeń. Nie spełnione zostały zatem wymagania określone w § 20 ust. 2 pkt 13 rozporządzenia KRI dot. zapewnienia warunków umożliwiających realizację i egzekwowanie obowiązku bezzwłocznego zgłaszania incydentów naruszania bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

Już audyt z 2013 r. wskazał m.in., że rejestr incydentów (zgodnie z polityką jego prowadzenie należało do ABGZ) nie zawierał żadnych zapisów, mimo iż w badanym przez audytorów okresie incydenty wystąpiły. W wyniku monitoringu realizacji zaleceń powyższego audytu (w grudniu 2014 r.) audytorzy stwierdzili, że rejestr incydentów został zaktualizowany i jest prowadzony przez BO. Przedstawiony NIK dokument nie był jednak rejestrem, lecz dziennikiem incydentów i zawierał jedynie spis komunikatów przekazanych ministerstwu przez CERT.GOV.PL wraz z opisem (treścią) tychże komunikatów. Dziennik zawierał 74 komunikaty z okresu od 22 lipca 2013 r. do 21 września 2015 r[87]. Dziennik nie zawierał incydentów zgłoszonych przez użytkowników, czy pochodzących z własnych systemów monitorowania infrastruktury informatycznej.

Wg informacji ABW w okresie od 3 stycznia 2014 r. do 5 czerwca 2015 r. CERT.GOV.PL w systemie ewidencji i obsługi incydentów RTIR zarejestrował 82, obsługiwane przez Zespół, incydenty dotyczące Ministerstwa Sprawiedliwości, skategoryzowane jako: przestępstwo o charakterze terrorystycznym popełnione w cyberprzestrzeni, włamanie na konto/ataki siłowe, nieuprawnione logowanie, skanowanie, inżyniera społeczna. W dzienniku dla powyższego okresu odnotowano 47 komunikatów CERT.GOV.PL. Dyr. BO nie potrafił wyjaśnić powyższej rozbieżności, a Dyr. DIRS poinformował, że departament nie ewidencjonował informacji otrzymywanych z CERT.GOV.PL, gdyż zadanie to było przypisane Administratorowi Bezpieczeństwa Grupy Zasobów.

(dowód: akta kontroli str. 214-234;282-284;422-428;760-764;1560-1565;1597-1599)

Z bazy danych systemu HPSM istniała możliwość wygenerowania raportu „zestawienie incydentów" w podziale na usługi. NIK zwraca jednak uwagę, że powyższe raporty dotyczyły „incydentów" zdefiniowanych jako pomoc w usunięciu awarii lub innej niesprawności sprzętu albo oprogramowania. Z ewidencji zgłoszeń wynika, że dotyczyły one najczęściej zdarzeń związanych z błędami w funkcjonowaniu aplikacji. Ponadto w HPSM można było odnaleźć incydenty (np. awarie) dla konkretnych elementów konfiguracji tylko wówczas, gdy zgłaszający wskazywał konkretny sprzęt do niego przypisany. Do HPSM automatycznie, przez SCOM[88], generowane były jako incydenty także typowe błędy systemowe i techniczne identyfikowane przez powyższe narzędzie.

DIRS nie posiadał odrębnej procedury reagowania na incydenty związane z bezpieczeństwem SI NKW. W ramach realizacji projektu EUKW został wytworzony dokument *EKW – Procesy i procedury organizacji bezpieczeństwa*[89] opisujący m.in. proces zarządzania incydentami bezpieczeństwa. *Zapisy tego dokumentu będą podstawą do stworzenia procedur i instrukcji reagowania na incydenty związane z bezpieczeństwem w SI NKW* – wyjaśnił Dyr. DIRS.

(dowód: akta kontroli str. 594-613;626-628;653-666;1821-1833)

---

[87] Od poz. 72, tj. 11 czerwca 2015 r. dziennik prowadzony był przez ABI.

[88] System Center Operation Menager – narzędzie Microsoft służące do monitorowania usług i aplikacji.

[89] Opracowany przez [redacted] dokument nie został zatwierdzony i nie został wskazany jako stosowany.

1.5 Zarządzanie kluczami kryptograficznymi

Opis stanu faktycznego

Środki ochrony kryptograficznej danych przesyłanych w sieci publicznej wykorzystywane były dla zapewnienia poufności, integralności i niezaprzeczalności. Uregulowania w zakresie stosowania mechanizmów kryptograficznych w MS określone zostały ogólnie w dokumentach PBI MS, PBST, RUST. Sposób zarządzania kluczami kryptograficznymi w systemie NKW/EKW uszczegółowiony został w:

- *Polityce certyfikacji systemu EKW*, gdzie określony został zbiór zasad opisujących świadczenie niekwalifikowanych usług certyfikacyjnych przez Centrum Certyfikacji. Jej treść odnosiła się nie tylko do składników samej Infrastruktury Klucza Publicznego w Centrum Certyfikacji, lecz także do Subskrybentów (klientów usług certyfikacyjnych) oraz Stron ufających (odbiorców informacji zabezpieczonych elektronicznie z użyciem Certyfikatów wystawionych przez Centrum Certyfikacji).
- Załączniku Nr 3 do *Polityki certyfikacji systemu EKW*, w którym określono prawa i podstawowe zasady oraz wskazówki wynikające z praktycznych doświadczeń oraz norm regulujących sposób zarządzania, ochrony i dystrybucji danych w systemie EKW.
- Dokumentacji technicznej Centrów Certyfikacji w systemie PD CBDKW[90].
- Procedurach generowania certyfikatów[91] dostępowych dla użytkowników systemu PD CBDKW w domenie Active Directory rejestrpd.ms.gov.pl.

Jak wyjaśnił Zastępca Dyr. DIRS, ww. *Polityka certyfikacji* została wdrożona, ale jej zatwierdzenie nastąpi po zrealizowaniu całości projektu *Wprowadzenie e-usług w zakresie ksiąg wieczystych* i wykonaniu audytu zgodności polityki z normą ETSI TS 102 042.

Zgodnie z Załącznikiem Nr 3 do *Polityki certyfikacji systemu EKW* zasady bezpieczeństwa związane z dostępem do usług systemu EKW, należy wprowadzać m.in. w oparciu o analizę ryzyka. Jak wyjaśnił Zastępca Dyr. DIRS na etapie projektowym, w zakresie analizy ryzyka, zidentyfikowano aktywa, zagrożenia oraz zdefiniowano katalog zabezpieczeń i środków kontrolnych mających na celu minimalizację ryzyka wystąpienia tych zagrożeń. W rezultacie przeprowadzenia ww. analizy, wskazano warstwy architektoniczne systemu, a także poszczególne rodzaje zagrożeń, dla których należy zastosować mechanizmy ochrony kryptograficznej.

W celu zapewnienia poufności, autentyczności oraz integralności informacji w systemie NKW/EKW stosowano następujące zabezpieczenia kryptograficzne:

- od 1 lipca 2014 r. wydawane były, zgodnie z art. 36^4 ust. 8 ustawy o księgach wieczystych i hipotece, certyfikaty dla użytkowników „branżowych", tj. dla komorników, notariuszy oraz określonych w innych przepisach prawa (np. dla prokuratury, policji),
- certyfikat SSL wystawiony przez Centrum certyfikacji CENTRUM,
- certyfikaty do komputera centralnego [redacted] które zabezpieczały połączenia terminalowe i FTP pomiędzy stacjami roboczymi a serwerem.

Do generowania i przechowywania certyfikatów użyte zostały dwie sprzętowe karty Crypto zainstalowane w serwerze Mainframe. Certyfikaty wydawane były imiennie,

[90] PD CBDKW to podsystem dostępu do Centralnej Bazy Danych Ksiąg Wieczystych – centralnej części systemu NKW przeznaczony do udostępniania ksiąg wieczystych w sieci Internet.

[91] Certyfikat to elektroniczne zaświadczenie, poświadczające przynależność klucza publicznego do Subskrybenta wskazanego w certyfikacie wygenerowane przez Centrum Certyfikacji.

a każdy certyfikat prywatny zabezpieczony był indywidualnym hasłem. Po wygenerowaniu certyfikatu pliki oraz hasła przesyłane były do wnioskującego (użytkownika) na adres e-mail wraz z instrukcjami wgrania certyfikatów.

W Ministerstwie Sprawiedliwości funkcjonowały cztery centra certyfikacji, w tym jedno dla systemu NKW/EKW. Według stanu na 15 września 2015 r. wydanych zostało łącznie 25 554 certyfikatów, w tym dla systemu NKW/EKW – 5 031.

(dowód: akta kontroli str. 13-56;594-610;617-625;684-696;1313-1320)

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

Zadaniem mechanizmów ochrony przed oprogramowaniem złośliwym jest wykrywanie i ochrona systemów informatycznych przed zagrożeniami takimi jak wirusy komputerowe, oprogramowanie szpiegujące (spyware) itp. Dla systemu NKW/EKW (ale także innych systemów utrzymywanych przez DIRS np. KRS, RZ, AD) jako rozwiązanie umożliwiające zapobieganie szkodliwemu oprogramowaniu i jego wykrywaniu przyjęto Symantec Endpoint Protection (dalej: SEP), oprogramowanie to zainstalowane było w MS oraz na serwerach i stacjach roboczych w Sądach[92]. *Przyczyną dokonania takiego wyboru był fakt, że w okresie wdrażania SI NKW to rozwiązanie funkcjonowało już w MS* - wyjaśnił Dyr. DIRS. Za obsługę centralnych serwerów SEP odpowiadał DIRS, natomiast za obsługę lokalnych instalacji Sądy.
Wskazane powyżej rozwiązanie było aktualizowane w 2009 r. z wersji SEP 10 do wersji 11. W okresie prowadzenia czynności kontrolnych trwało wdrożenia wersji 12 na nowych serwerach EKW. Oprogramowanie SEP było dystrybuowane i zarządzane w sposób scentralizowany. Definicje antywirusowe aktualizowane były codziennie przez operatorów przetwarzania danych MS (w odniesieniu do wersji SEP 11) lub aktualizacja odbywała się automatycznie, co 4 godziny (SEP 12). Proces nadzorowany był przez pracowników WUI, którzy mogli harmonogram aktualizacji zatrzymać/powstrzymać, co skutkowało opóźnieniem dystrybucji nowych definicji.
Używana w ministerstwie wersja SEP nie posiadała funkcjonalności kontroli dostępu do sieci w oparciu o wymagania dla zainstalowanego oprogramowania. Dyr. DIRS poinformował, że taka funkcjonalność (Network Access Control) będzie wdrożona w ramach projektu „Bezpieczny notebook"[93]. Zastosowane zostały natomiast systemy detekcji/zabezpieczeń przed intruzami – aktywny moduł IPS/IDS na urządzeniu Palo Alto Next Generation Firewall, obejmujący wszystkie systemy wystawione do publicznej sieci Internet. Na stacji roboczej każdego użytkownika w MS instalowane było podstawowe oprogramowanie (w tym np. SEP 12.1.5).

(dowód: akta kontroli str. 13-51;684-696;1560-1565;1664-1668;1866-1869)

Urządzenia mobilne - tablety objęte były systemem FAMOC (administrowanym przez BDG), który uniemożliwiał instalację jakiegokolwiek oprogramowania.

---

[92] System Symantec Endpoint Protection składa się z centralnego serwera zarządzająco-monitorującego, na którym działa oprogramowanie Symantec Endpoint Protection Manager, oraz oprogramowania klienckiego, działającego na poszczególnych serwerach.

[93] Więcej w pkt 1.7 wystąpienia pokontrolnego.

W odniesieniu do laptopów/notebooków istniał zakaz – wynikający z RUST – instalowania oprogramowania niedostarczonego wraz ze sprzętem. W systemie NKW/EKW nie wykorzystywano urządzeń mobilnych.

Ponadto w MS funkcjonował system monitorujący zmiany oprogramowania i utrzymania historii zainstalowanego sprzętu i oprogramowania – System Center Configuration Manager (dalej: SCCM). W odniesieniu do systemu NKW/EKW system ten był w trakcie wdrożenia z uwagi na zmianę wersji SCCM.

W odniesieniu do NKW/EKW w okresie od 1 stycznia 2014 r. do 16 lipca 2015 r. wykryto 69 przypadków działania szkodliwego oprogramowania powodowanych przez 22 rodzaje szkodliwego kodu. W przypadku 21 zagrożeń system antywirusowy zablokował szkodliwe oprogramowanie, a raz przeniósł je do kwarantanny, z której wirus został usunięty[94]. Przypadki automatycznego wykrycia lub usunięcia szkodliwego oprogramowania w ramach SI NKW (i innych systemów) były raportowane i analizowane w konsoli centralnej zarządzania oprogramowaniem SEP przez pracowników WUI bądź WUA oraz administratorów lokalnych w sądach.

Przychodzące e-maile były filtrowane z zagrożeń i niechcianych informacji z wykorzystaniem Symantec Mail Security for Microsoft Exchange oraz mechanizmów Anti-spam wbudowanych w Exchange Server.

(dowód: akta kontroli str. 684-696;1560-1565;1664-1669;1866-1869)

Postanowienia, które miały związek z ochroną przed złośliwym oprogramowaniem wprowadził RUST, w szczególności:

- zabrania się użytkownikom uruchamiać i instalować samowolnie na sprzęcie służbowym jakiegokolwiek oprogramowania niedostarczonego wraz ze sprzętem (§ 9 pkt 2);
- ważne pliki należy przechowywać w wyznaczonych folderach na serwerach, które gwarantują bezpieczeństwo danych (§ 11 pkt 1);
- zabrania się przechowywania na sprzęcie służbowym wszelkich plików nie związanych z zadaniami służbowymi np. gier, dokumentów, zdjęć, muzyki, filmów itp. (§ 14).

Powyższe zasady przypominane były pracownikom w komunikatach Service Desk w związku ze zidentyfikowaniem konkretnych zagrożeń.

(dowód: akta kontroli str. 52-56;1077-1083)

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

1. Dokumenty polityki PBI MS oraz PBST nie zawierały regulacji odnoszących się do zapobiegania złośliwemu oprogramowaniu. Także w przedstawionych wyjaśnieniach nie wskazano dokumentacji, która świadczyłaby o ustanowieniu polityki ochrony przed takim oprogramowaniem.

DIRS nie posiadał centralnego wykazu oprogramowania, dzięki któremu zarządza się dopuszczeniem oprogramowania do eksploatacji. Nie prowadził także wykazu licencji oprogramowania z określeniem czasu, miejsca i zakresu ich

[94] Dane z raportów Symantec Endpoint Protection Manager, różnica między liczbą wirusów a liczbą wykryć wynikała z faktu, iż jeden rodzaj oprogramowania identyfikowany był na jednej lub więcej stacji roboczych.

wykorzystywania. System HPSM zawierał jedynie wykaz licencji zmigrowanych z dawnego systemu ewidencji sprzętu.
Obowiązująca instrukcja *Zasady instalacji nowego/nowych wersji oprogramowania w systemie z/OS* dotyczyła wyłącznie oprogramowania dedykowanego, tj. dostarczonego przez dostawców rozwiązań informatycznych dla MS. Powyższa procedura nie obejmowała oprogramowania gotowego lub aktualizacji tego oprogramowania, w tym oprogramowania zapobiegającego złośliwemu oprogramowaniu.
DIRS nie prowadził ewidencji bezpłatnego oprogramowania instalowanego na stacjach użytkowników. Taką informację można było uzyskać z systemu HPSM na podstawie zgłoszeń użytkowników. W wyszukiwarce elementów konfiguracji w systemie HPSM w „szczegółach" wyodrębnione zostało oprogramowanie przypisane dla danej stacji roboczej. Jednak nie zostały wyszczególnione poziomy ochrony przypisane do danego elementu infrastruktury IT.
Dyr. DIRS przyznał, iż *nie są dokonywane regularne przeglądy zainstalowanego oprogramowania. Przeglądy oprogramowania dokonywane są przez administratorów, jednak fakt ten nie jest dokumentowany w żadnym rejestrze. Dokonywanie przeglądu wykonywane jest zgodnie z dobrymi praktykami i praktyką zawodową.*
Ponadto nie wprowadzono zaleceń wynikających z prowadzonych analiz przypadków wykrycia szkodliwego oprogramowania zarejestrowanych w konsoli SEP. Departament nie miał też ustalonych procedur/harmonogramów dla generowania z powyższej konsoli raportów o najczęstszych źródłach ataku czy korelacjach zagrożeń.
(dowód: akta kontroli str. 606-610;653-666;1664-1668;1821-1833;1866-1869;1909-1913)
Powyższe ustalenia wskazują na ryzyko niespełnienia wymagań określonych w § 20 ust. 2 pkt 12 lit. a oraz lit. g rozporządzenia KRI odnośnie zapewnienia warunków umożliwiających zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, w szczególności przez dbałość o aktualizację oprogramowania oraz niezwłocznego podejmowania działań po dostrzeżeniu nieujawnionych podatności.

1.7 Bezpieczeństwo sieciowe

Opis stanu faktycznego

Zgodnie z pkt 12.3 PBI MS (*Kontrola dostępu do sieci*) w celu ochrony usług sieciowych przed nieautoryzowanym dostępem Dyrektor DIRS sprawował kontrolę nad wszystkimi urządzeniami i systemami podłączanymi do sieci. Każde podłączane do sieci urządzenie lub system musiało spełniać minimalne wymagania bezpieczeństwa. Dyr. DIRS wyjaśnił, że nie został opracowany dokument, w którym określone zostałyby minimalne wymagania bezpieczeństwa, wymagania takie określane były zgodnie z najlepszymi praktykami w odniesieniu do ogólnych zasad bezpieczeństwa zawartych w PBI MS, a kontrola sprawowana była za pośrednictwem uprawnionych pracowników WUI, którzy dokonywali podłączania urządzeń.

Zarządzanie sprzętem sieciowym realizowane było w DIRS z wykorzystaniem procesów zarządzania zmianą i konfiguracją. Procesy te były zaimplementowane w systemie HPSM, a obligatoryjność ich stosowania przez pracowników wynikała z decyzji Dyr. DIRS z 24 czerwca 2015 r. Dodatkowo w zakresie zarządzania sprzętem sieciowym wykonywane były m.in. następujące zadania i procedury:

- zarządzanie hasłami dostępowymi do urządzeń sieciowych realizowane było zgodnie z określoną instrukcją;
- deponowanie haseł dostępowych do urządzeń sieciowych odnotowywane było w stosownym rejestrze;
- utworzono dokumentację opisującą sposób wykonywania pomiarów przepustowości sieci wraz z rekomendacją odpowiednich narzędzi;
- dostęp zdalny dla pracowników DIRS i firm zewnętrznych udzielany był na podstawie zaakceptowanych wniosków w systemie HPSM;
- dla urządzeń sieciowych zapewniane były usługi serwisowe gwarantujące naprawę tych urządzeń, a także dodatkowe usługi związane m.in. z aktualizacją oprogramowania systemowego tych urządzeń.

W strukturze DIRS rozdzielona została odpowiedzialność za bieżące zarządzanie zasobami infrastruktury sieciowej od odpowiedzialności za funkcjonowanie systemów korzystających z tej sieci. Do zadań Zespołu Sieci w strukturze WUI należało m.in. bieżące zarządzanie zasobami infrastruktury sieciowej w celu zapewnienia odpowiednich warunków eksploatacji systemów teleinformatycznych i ciągłości świadczenia usług IT, a także wdrażanie poprawek i uaktualnień dla infrastruktury sieciowej oraz przygotowywanie tej infrastruktury do instalacji aplikacji. Natomiast do zadań WUA należało m.in. identyfikowanie i definiowanie zmian funkcjonalnych w systemach teleinformatycznych wynikających z utrzymania systemów, a także prowadzenie prac serwisowych i modernizacyjnych dla aplikacji utrzymywanych przez DIRS.
W okresie od stycznia 2014 r. do 29 października 2015 r. złożonych zostało łącznie 127 wniosków dotyczących nadania uprawnień do pracy zdalnej dla pracowników 10 kontrahentów zewnętrznych. Pracownicy zewnętrzni potwierdzali zapoznanie się z PBI MS podpisując *kartę dostępu do zasobów sieci MS dla firm świadczących usługi na rzecz ministerstwa*. Od 1 czerwca 2015 r. przechowywane były one w Service Desk w WUA, przez okres dwóch lat, liczony od momentu (czasu) włączenia usługi zdalnego dostępu do zasobów sieci.
(dowód: akta kontroli str. 13-41;699-711;1215-1220;1333-1336;1908;1955-1958)

Wytyczne w zakresie zarządzania istotnymi dla bezpieczeństwa elementami sieci zostały określone w decyzji Dyr. DIRS z 24 czerwca 2015 r., którą pracownicy zobowiązani zostali do stosowania m.in. instrukcji *Nadzór nad kopiami bezpieczeństwa w POPD i ZOPD MS oraz deponowanie haseł dostępowych w Departamencie Informatyzacji i Rejestrów Sądowych*. Stosowane były także następujące dokumenty: *Rejestr przekazywania haseł dostępowych, Rejestr zmian konfiguracji firewall'a POPD/ZOPD MS, Dziennik nadzoru nad infrastrukturą POPD/ZOPD MS*[95].

Sporządzony został dokument zawierający listę urządzeń sieciowych wraz z przypisanymi do nich kontaktami serwisowymi. Dla urządzeń sieciowych zapewniane były usługi serwisowe, a także dodatkowe usługi związane m.in. z aktualizacją oprogramowania systemowego tych urządzeń. Ponadto, każdy rekonfigurowany port przełącznika był sprawdzany pod kątem, czy uruchomiona jest funkcjonalność port-security (służąca do kontroli dostępu do portów), a nowo zakupione urządzenia sieciowe były dołączane do narzędzi monitorujących infrastrukturę sieciową.

Polityka haseł administracyjnych dla urządzeń infrastruktury sieciowej określona została w punkcie 6.4 PBST. Do zarządzania kontami administratorów sieci służyło

[95] Powyższe procedury przygotowane zostala w ramach SZJ przed 1 stycznia 2014 r. i obowiązywały w ramach systemu kontroli zarządczej DIRS.

urządzenie Cisco AC, które w przechowywało bazę użytkowników oraz dokonywało sprawdzenia, czy dany użytkownik administrujący urządzeniami Cisco ma uprawnienia do zalogowania się. Zastępca Dyr. DIRS dodał, że urządzenia sieciowe były monitorowane przez narzędzia Cacti i NetCrunch.

Pracownicy MS posiadający przenośne komputery służbowe nie mieli bezpośredniego dostępu do wewnętrznej infrastruktury sieciowej. Jedynie część administratorów zespołów sieci, serwerów oraz komputera centralnego w razie awarii miała możliwość zestawienia szyfrowanego tunelu VPN SSL z firewall brzegowym PaloAlto 5050 z komputerów służbowych z zainstalowanym odpowiednim oprogramowaniem (AV, NAC).
Regulacje dotyczące zdalnych połączeń szyfrowanych określone zostały w dokumentach:

- *Projekt techniczny VPN – Realizacja zdalnego dostępu do zasobów Sieciowych,*
- *Karta dostępu do zasobów Sieci Ministerstwa Sprawiedliwości.*

(dowód: akta kontroli str. 606-610;699-711;1313-1318;1333-1336; 1556-1565)
Zgodnie z pkt 4 PBST w MS stworzyć należało wydzielone obszary bezpieczne, w których mieszczą się systemy teleinformatyczne. Zasady dostępu do poszczególnych obszarów w MS określały zarządzenia Dyrektora Generalnego w sprawie zasad ruchu osobowego, samochodowego i materiałowego na terenie Ministerstwa Sprawiedliwości, a także w sprawie zasad gospodarowania kluczami oraz nadawania kodów do pomieszczeń i wejść w budynkach Ministerstwa Sprawiedliwości[96]. W MS wydzielono dwa obszary bezpieczne, w których zlokalizowano serwerownie oraz punkty dystrybucyjne.

Dyrektor DIRS wyjaśnił, że wydzielenia obszarów dokonano – zgodnie z PN-EN 50133-1, przy zastosowaniu elektronicznego Systemu Kontroli Dostępu w:

- klasie rozpoznania 1 – informacja zapamiętana: rozwiązanie bazuje przede wszystkim na haśle, osobistym numerze identyfikacyjnym,
- klasie dostępu B – przejścia kontrolowane pracujące z wykorzystaniem funkcji siatki czasu oraz rejestracji zdarzeń.

(dowód: akta kontroli str. 1664-1685)

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

1. Stosowane w MS zasady przetwarzania mobilnego oraz pracy na odległość nie zapewniały warunków pełnego bezpieczeństwa wykonywanych czynności, co nie spełniało wymagań określonych w § 20 ust. 2 pkt 8 rozporządzenia KRI.

[96] Zarządzenie Nr 159 Dyrektora Generalnego Ministerstwa Sprawiedliwości z dnia 17 grudnia 2013 r. w sprawie zasad ruchu osobowego, samochodowego i materiałowego na terenie Ministerstwa Sprawiedliwości przy ul. Zwycięzców 34; Zarządzenie Nr 52/15/BO Dyrektora Generalnego Ministerstwa Sprawiedliwości z dnia 30 kwietnia 2015 r. w sprawie zasad ruchu osobowego, samochodowego i materiałowego na terenie Ministerstwa Sprawiedliwości przy Al. Ujazdowskich 11 w Warszawie; Zarządzenie Nr 53/15/BO Dyrektora Generalnego Ministerstwa Sprawiedliwości z dnia 30 kwietnia 2015 r. w sprawie zasad ruchu osobowego, samochodowego i materiałowego na terenie Ministerstwa Sprawiedliwości przy ul. Czerniakowskiej 100 w Warszawie.

W MS nie stosowano zalecanych przez RUST (§ 24) zabezpieczeń kryptograficznych przenośnych komputerów i nośników danych.

Interwencyjne działania dot. stworzenia „białej listy" urządzeń (komputery, laptopy, drukarki), które miały posiadać uprawnienia do korzystania z zasobów i usług podjęto po audycie z lipca 2015 r. podjęto. W planach był zakup oprogramowania do monitoringu obcych urządzeń w sieci wraz z systemem powiadamiania o incydentach bezpieczeństwa. W dniu 31 sierpnia 2015 r. podpisana została z [redacted] umowa na zaprojektowanie, dostawę i wdrożenie systemu bezpiecznego zdalnego dostępu do sieci teleinformatycznej MS. Celem zamówienia było zapewnienie pracownikom MS zdalnego bezpiecznego dostępu do zasobów informatycznych (korzystanie z komputerów przenośnych z aplikacji firmowych poza centralą, jak i wewnątrz sieci MS). Dyski komputerów miały być chronione za pomocą szyfrowania, a dostęp do urządzenia zabezpieczony za pomocą tokenu i/lub czytnika linii papilarnych.

(dowód: akta kontroli str. 454-478;626-628;982-997;1664-1669;1696-1721;1955-1958)

W MS nie opracowano zalecanych przez PBST (pkt 6.5) procedur dotyczących:

- przerywania sesji zdalnego dostępu do systemów krytycznych po określonym czasie bezczynności;
- zdalnego zarządzania sprzętem.

Jak wyjaśnił Dyr. DIRS. w związku z brakiem powyższych procedur czynności w tym zakresie realizaowane były w oparciu o dobre praktyki. W zakresie zdalnego zarządzania sprzętem dostęp realizowany był poprzez przejęcie pulpitu zdalnego stacji roboczej po wcześniejszej akceptacji i pod kontrolą użytkownika. Natomiast dostęp do krytycznych systemów realizowany był w strefie zamkniętej, a administratorzy zobowiązani byli do wylogowania się ze stacji roboczych w przypadku odejścia od stanowiska pracy.

(dowód: akta kontroli str. 594-605;699-708)

2. Na nieprawidłowości w zakresie zapewniania przez MS środków uniemożliwiających nieautoryzowany dostęp na poziomie usług sieciowych co najmniej do początku 2015 r., co stanowiło niespełnienie warunków określonych w § 20 ust. 2 pkt 7 lit c rozporządzenia KRI, wskazały także wyniki audytów zewnętrznych, przeprowadzonych na zlecenie MS, przede wszystkim wyniki *Audytu wydajności infrastruktury* z 2014 r. wykonanego przez Pana [redacted]. Pomimo, że ocena bezpieczeństwa sieci i systemów nie była przedmiotem audytu, to jednak audytor stwierdził istotne słabości lub brak właściwych mechanizmów kontrolnych w obszarze bezpieczeństwa sieci i systemów, które skutkowały naruszeniem PBI MSiSP lub PBST, tj.:

- brak separacji pomiędzy systemami serwerowni, stacjami klienckimi i urządzeniami peryferyjnymi w segmencie sieci obejmującym budynki w Al. Ujazdowskich 11 i 19 oraz ul. Koszykowej 6;
- brak skutecznych mechanizmów kontrolnych nad nieużywanymi lub niepodłączonymi portami na przełącznikach dostępowych, co stanowiło naruszenie PBST;
- brak skutecznych mechanizmów kontrolnych przed nieautoryzowanym podłączeniem obcych urządzeń do sieci, co było możliwe wszędzie tam, gdzie

[97] Umowa nr 33 z dnia 11 czerwca 2014 r. Celem powyższego audytu było zbadanie czy infrastruktura sieciowa MS działała poprawnie i spełniała kryteria wydajności, dostępności i niezawodności do poprawnego działania aplikacji intranetowych używanych w MS, tj. EOD oraz FK.

były zainstalowane urządzenia sieciowe służące do podziału sieci, co stanowiło naruszenie PBST;
- brak skutecznych mechanizmów kontrolnych w zakresie przepływu ruchu sieciowego wewnątrz sieci Ministerstwa Sprawiedliwości.

Zastępca Dyr. DIRS wyjaśnił, że po ww. audycie m.in. dokonano przeglądu nieużywanych i niepodłączonych portów, przedstawiono koncepcję separacji segmentów użytkowników sieci LAN MS od zasobów serwerowych dla całej infrastruktury AD LAN MS. Natomiast wprowadzenie 22 rekomendacji (w całości lub częściowo) zlecono na podstawie umowy zlecenia Panu [redacted][98]. Prowadzone były ponadto prace projektowe w zakresie wymiany okablowania strukturalnego w ramach realizacji remontu budynku przy Al. Ujazdowskich 11.

(dowód: akta kontroli str. 13-51;1354-1369;1372-1376;168-1695)

Ocena cząstkowa

Najwyższa Izba Kontroli zarządzanie procesem zapewniania bezpieczeństwa IT w Ministerstwie Sprawiedliwości w okresie od 1 stycznia 2014 r. do zmian organizacyjnych podjętych w 2015 r. ocenia na poziomie 1. *Początkowe/doraźne*, a po zmianach, tj. w 2015 r. na poziomie 2.*Powtarzalne lecz intuicyjne*.

W odniesieniu do pierwszego z ww. okresów powyższą ocenę uzasadniają w szczególności:
- przyjęcie jako obowiązujących dokumentów polityki bezpieczeństwa w MS nie dostosowanych do specyfiki Ministerstwa Sprawiedliwości, w tym w zakresie ochrony danych osobowych oraz brak aktualizacji tej dokumentacji w warunkach zmieniającego się otoczenia;
- niepełna klasyfikacja aktywów informacyjnych w dokumentacji polityki, w tym brak wskazania na administrowane w ministerstwie systemy informatyczne oraz brak analizy ryzyka dla bezpieczeństwa posiadanych aktywów;
- brak realnego wdrożenia systemu zarządzania bezpieczeństwem informacji;
- brak w okresie do lipca 2015 r. zasad dokumentowania incydentów związanych z bezpieczeństwem i zbierania związanych z nimi dowodów, rejestru takich incydentów oraz analiz pozdarzeniowych, co oznaczało, iż zarządzanie bezpieczeństwem w odniesieniu do tych incydentów nie było realizowane;
- realizowanie procesów zgodnie z przyjętą praktyką, ale bez formalnych procedur lub bez zatwierdzenia procedur.

W odniesieniu do drugiego okresu powyższą ocenę uzasadniają w szczególności:
- świadomość potrzeby zapewnienia bezpieczeństwa informacji na poziomie kierownictwa oraz podjęcie działań zmierzających do zmiany SZBI na poziomie organizacyjnym oraz dokumentacji polityk bezpieczeństwa, zwłaszcza w odniesieniu do ochrony przetwarzanych danych osobowych;
- szczupłość zasobów w sferze odpowiedzialności za bezpieczeństwo IT – oparcie procesu zmian na pojedynczych osobach, których uprawnienia do zarządzania były ograniczone;
- postrzeganie bezpieczeństwa jako odpowiedzialności i domeny głównie działu IT wspartego przez zamawiane na zewnątrz organizacji usługi (np. audyty) i narzędzia (np. do monitorowania bezpieczeństwa);

[98] Na podstawie umowa nr 23/2014 z 12 listopada 2014 r., która wykonana została w 2015 r.

– system sprawozdawczości dotyczącej bezpieczeństwa informacji na etapie budowy.

2. Wspieranie bezpieczeństwa na poziomie wybranego systemu

2.1 Zarządzanie tożsamością

Opis stanu faktycznego

W MS nie została opracowana odrębna procedura naboru na stanowiska realizujące zadania w obszarze bezpieczeństwa informacji. Obowiązywało zarządzenie nr 51/2015 Dyrektora Generalnego z dnia 30 kwietnia 2015 r. dotyczące zasad przeprowadzania naboru zewnętrznego w służbie cywilnej w MS[99], które regulowało szczegółowe zasady przeprowadzania naboru na wyższe stanowiska w służbie cywilnej oraz stanowiska niebędące wyższymi w służbie cywilnej. *Mając na uwadze specyfikę i złożoność zadań wykonywanych na ww. stanowiskach oraz ryzyko wynikające z niewłaściwie prowadzonych działań przez osoby realizujące te zadania, w opisie stanowiska pracy określone zostały szczegółowo wymagania i niezbędne kwalifikacje* – dodatkowo wyjaśniła Dyrektor Generalna.

Po zmianach przeprowadzanych w 2015 r. w organizacji SZBI kluczową rolę w powyższym obszarze odgrywał ABI – radca ministra w Biurze Kontroli i Audytu Wewnętrznego, kierujący pracami Zespołu ds. bezpieczeństwa informacji. W opisie stanowiska ABI znalazły się wymogi związane m.in. z posiadaniem wiedzy w zakresie bezpieczeństwa teleinformatycznego i właściwych norm ISO, które zostały spełnione. Utworzone w lutym 2015 r. w strukturze DIRS wewnętrznym regulaminem organizacyjnym departamentu stanowisko ds. bezpieczeństwa teleinformatycznego do zakończenia czynności kontrolnych nie zostało obsadzone. Działania zmierzające do obsadzenia tego stanowiska w ramach naboru wewnętrznego nie przyniosły rezultatu. Opublikowane w lipcu 2015 r. ogłoszenia o naborach na wakujące w DIRS stanowiska naczelników wydziałów WUI i WAK zawierały wymóg legitymowania się przez kandydatów certyfikatem ITIL odnoszącym się do zarządzania usługami IT, w tym zarządzania ich bezpieczeństwem.

(dowód: akta kontroli str. 405-411;594-605;722-730;841-846;903-923;953-956;1073-1076)

Dla systemu NKW/EKW wykaz pracowników kluczowych dla bezpieczeństwa informacji nie został sporządzony. *W obecnej strukturze organizacyjnej w DIRS, jest podział na Utrzymanie (WUI oraz WUA) oraz Rozwój (WRS i WRP). Wykaz taki byłby zasadny w sytuacji kiedy Departament do roku 2013 miał strukturę silosów to znaczy za utrzymanie i rozwój systemu odpowiadała jedna i niezmienna grupa osób. Zadania i funkcje, które wykonują pracownicy opisane są w zakresach czynności i w opinii Departamentu nie ma potrzeby wykonywać oddzielnego wykazu osób kluczowych* – wyjaśnił Dyr. DIRS. W pracach związanych z utrzymaniem infrastruktury tego systemu uczestniczyli pracownicy zatrudnieni w WUI: Zespole Sieci, Zespole Komputera Centralnego, Zespole Serwerów. *Każda z osób powinna być uznana jako kluczowa. Nikt z pracowników powyższych zespołów nie jest przypisany do konkretnego systemu, z uwagi na fakt że każdy wykonuje zadania na potrzeby wszystkich systemów* – wyjaśnił Dyr. DIRS. W WUA za aspekt techniczny utrzymania systemu NKW/EKW odpowiedzialni byli administrator systemu[100] oraz

[99] Poprzedzało je określające zasady naboru zarządzenie Dyrektora Generalnego nr 127/2013 z dnia 18 września 2013 r.

[100] Na brak administratora NKW/EKW od dnia 5 sierpnia 2015 r. wskazano w rozdziale 1.2 wystąpienia pokontrolnego.

tzw. administrator funkcjonalny, odpowiedzialny za rozliczanie umowy utrzymaniowej[101].

(dowód: akta kontroli str. 594-605;617-625;1548-1552)

Obowiązek ochrony informacji i przestrzegania zasad zawartych w polityce nakładał na pracowników ministerstwa oraz firm zewnętrznych realizujących prace na rzecz MS pkt 4 PBI MS, a RUST (§ 2) zobowiązywał użytkowników do zachowania w tajemnicy informacji pozyskanych za pomocą systemów teleinformatycznych, których ujawnienie mogłoby narazić pracodawcę na szkodę. Ponadto obowiązki zachowania tajemnicy służbowej regulowały przypisy ustawy o służbie cywilnej. Postępowanie niezgodne z polityką i/lub naruszenie RUST wiązało się ze skutkami prawnymi przewidzianymi w Regulaminie pracy, w tym sankcjami dyscyplinarnymi[102].

Od dnia 1 czerwca 2015 r. wprowadzono nowe oświadczenia pracowników o zapoznaniu się i przestrzeganiu obowiązków wynikających z ustawy o ochronie danych osobowych, PBI MS i SP oraz RUST. Oświadczenie zawierało także zobowiązanie do zachowania w tajemnicy danych osobowych oraz ich zabezpieczenia po ustaniu zatrudnienia, czego nie zawierały wcześniej dokumenty polityki oraz oświadczenie stanowiące załącznik do RUST.

Obowiązek przestrzegania procedur i przepisów wewnętrznych wynikających z polityki bezpieczeństwa zawierały umowy z wykonawcami systemów informatycznych, w tym umowa nr 38 z [redacted][103]. Ponadto pracownicy firm zewnętrznych podpisując *karty dostępu do zasobów sieci MS dla firm świadczących usługi na rzecz ministerstwa* zobowiązywali się m.in. do:

- zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić MS na szkodę zarówno w trakcie realizacji zadań wynikających z wykonywanej umowy, jak i po zakończeniu ich realizacji;
- nie uzyskiwania dostępu do innych zasobów niż udostępnionych w celu realizacji umowy;
- nie omijania mechanizmów kontroli i wdrożonych zabezpieczeń w sieci MS;
- nie podłączania i użytkowania sprzętu nie uzgodnionego z zamawiającym;
- nie pozyskiwania, gromadzenia i przechowywania na ww. sprzęcie danych nie związanych z realizacją umowy.

Pracownicy firm zewnętrznych podpisywali ponadto oświadczenie, że ponoszą pełną odpowiedzialność za przeprowadzone działania w sieci teleinformatycznej MS, i że działania będą przeprowadzane zgodnie z przyjętą Polityką Bezpieczeństwa Informacji oraz, że nie udostępnią informacji pozyskanej z sieci MS w wyniku prowadzonych działań. Zobowiązanie wiązało ich w okresie trwania umowy oraz na czas nieograniczony od jej wygaśnięcia.

(dowód: akta kontroli str. 13-41;52-56;606-610;617-628;1809-1812)

Zarządzanie dostępem do informacji i kontrola dostępu mają na celu zapewnienie dostępu tylko użytkownikom autoryzowanym i ochronę zasobów informacyjnych przed dostępem nieuprawnionym. Przejrzyście powinna zostać określona zarówno odpowiedzialność przydzielających prawo dostępu, jak i użytkowników.

---

[101] Tj. umowy z [redacted]

[102] W okresie objętym kontrolą odnotowano dwa przypadki postępowania niezgodnego z polityką bezpieczeństwa (dotyczyły przetwarzania danych w systemie KRK), które skutkowały zawieszeniem pracowników w pełnieniu obowiązków na podstawie art. 69 ustawy o służbie cywilnej do czasu zakończenia postępowania karnego prowadzonego przez prokuraturę.

[103] W § 11 ww. umowy określono zasady bezpieczeństwa przy jej realizacji, m.in. zobowiązano wykonawcę do przedstawienia imiennej listy osób dopuszczonych do wykonywania umowy, zawierającej dane osobowe z określeniem zakresu czynności. Ponadto niektóre umowy np. nr 65 z dnia 29 sierpnia 2014 r. zawarta z [redacted] na wykonanie testów bezpieczeństwa trzech systemów w tym NKW/EKW zawierały klauzule poufności, co omówiono w pkt 2.3 wystąpienia.

W pkt 12.5 PBI MS *(Zasady nadawania uprawnień dla użytkowników)* wskazano, iż udzielanie, zmiana i odbiór uprawnień użytkowników jest wykonywany przez właściciela aktywu lub przez upoważnionego przez niego administratora na wniosek przełożonego. Po ustaniu zatrudnienia przełożony pracownika ma obowiązek zgłosić wniosek o odebranie uprawnień. Po szczegóły polityka odsyła do wewnętrznych procedur określających proces nadawania, modyfikacji i odbierania uprawnień. W pkt 6.2 PBST (*Kontrola dostępu do zasobów informatycznych)* wskazano, iż w szczególności użytkownicy dostają uprawnienia do systemów, danych i usług w zakresie zgodnym z zakresem ich czynności służbowych.
W odniesieniu do systemów RZ, KRS, NKW proces nadawania użytkownikom uprawnień opisano w procedurze *Nadawanie użytkownikom uprawnień do systemów informatycznych*[104]. Od 1 lipca 2015 r. dla pracowników ministerstwa obsługa nadawania uprawnień realizowana była zgodnie z implementacją procesu *Zarządzanie zmianami* w systemie HPSM. Przy czym jeżeli na danym stanowisku pracy w DIRS potrzebny był dostęp do NKW/EKW składany był dodatkowy pisemny wniosek. Wg wyjaśnień Dyr. DIRS w związku z brakiem przypisania właścicielstwa do poszczególnych zasobów informatycznych nadanie uprawnień zatwierdzała, zgodnie z wewnętrznym regulaminem, Dyrekcja DIRS, na wniosek kierowników poszczególnych zespołów WUI lub WUA. Dodatkowo wymagane były karty dostępu do zasobów sieci oraz wnioski o dostęp do zasobów platformy Mainframe (komputera centralnego). Pracownicy wydziału odpowiedzialni za utrzymanie infrastruktury (WUI) nie mieli uprawnień do logowań w aplikacji EKW, posiadali natomiast dostęp do serwerów, na których znajdował się powyższy system (każde ich wejście, nawiązana sesja z danym serwerem, odkładane było w logach na urządzeniu Palo Alto).

(dowód: akta kontroli str. 13-41;606-610;617-628;640-644;768-776;903-923;1873-1878)

Pracownicy MS mający dostęp do systemu NKW/EKW grupowani byli w kontenerach usługi katalogowej w domenie nkw.justice.gov.pl jako CIKW (użytkownicy podsystemu Centralnej Informacji Ksiąg Wieczystych) oraz WNKW – dla użytkowników z wydziałów WRP i WUA. Odnotowywano imię, nazwisko i przyznane uprawnienia. W domenie rejestrpd.ms.gov.pl użytkownicy MS grupowani byli w kontenerach usługi katalogowej ADMI (użytkownicy z WRP, WRS, WUA oraz Centralnej Informacji o Zastawach Rejestrowych, Krajowego Rejestru Sądowego oraz Ksiąg Wieczystych). W tym wypadku odnotowywano imię, nazwisko, PESEL, e-mail i przyznane uprawnienia. System NKW/EKW posiadał bowiem wydzielone/dedykowane środowisko AD.

W zakresie domeny nkw.justice.ms.gov.pl (pracowali w niej m.in. sędziowie z wydziałów ksiąg wieczystych) nie było możliwości dostępu do systemów operacyjnych spoza wydzielonych podsieci ministerstwa (logowania się z domu). W zakresie domeny rejesrtpd.ms.gov.pl (przechowywała tylko informacje na temat uprawnień przypisanych do poszczególnych użytkowników, tj. przynależności do grup i ról w aplikacji oraz systemów informatycznych korzystających z aplikacji branżowej – PD CBDKW[105]) także nie było możliwości dostępu do systemów operacyjnych spoza wydzielonych podsieci ministerstwa (logowania się z domu). Zalogować się mogli użytkownicy posiadający certyfikat i odpowiednie uprawnienia. W domenie tej pracowali m.in. komornicy, notariusze (użytkownicy branżowi) oraz

[104] Powyższa procedura przygotowana została w ramach SZJ przed 1 stycznia 2014 r. i obowiązywała w ramach systemu kontroli zarządczej DIRS.

[105] Procedura tworzenia użytkowników i nadawania uprawnień dla użytkowników w domenie AD w systemie PD CBDKW opisane zostały w dokumentach wytworzonych przez [redacted] nie zatwierdzonych, ale używanych z uwagi na konieczność eksploatacji wdrożonych funkcjonalności EKW po 1 lipca 2014 r.

administratorzy, a także systemy teletransmisyjne (np. ZSIN – Zintegrowany System Informacji o Nieruchomościach).
Wg wyjaśnień Dyr. DIRS mechanizm weryfikacji tożsamości podczas uzyskiwania dostępu do systemu NKW/EKW dotyczył wszystkich typów użytkowników. Nie dotyczył usług udostępnianych za pomocą publicznej sieci Internet w zakresie przeglądania ksiąg wieczystych, składania wniosków o wydanie dokumentu, weryfikacji wydanych dokumentów w zakresie EKW.

Od 1 stycznia 2014 do dnia dzisiejszego[106] *systemy i procesy uzyskujące dostęp na zasadach analogicznych do „żywych" nie miały dostępu do SI NKW za wyjątkiem bezpośredniego dostępu systemu zewnętrznego, administrowanego przez uprawnione podmioty np. (AW, MF, prokuratura, sądy) do wystawianych usług - dedykowanych interfejsów do systemu SI NKW. Nadawanie uprawnień dla użytkowników odbywa się na zasadach obowiązujących u tych podmiotów* – wyjaśnił ponadto Dyr. DIRS.

(dowód: akta kontroli str. 594-605;617-628;640-644;2060-2065)

Rozliczalność[107] w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach). Wg wyjaśnień Dyr. DIRS działania użytkowników NKW/EKW lub obiektów systemowych logowane były za pomocą wbudowanych mechanizmów systemu operacyjnego, jak również w logach serwera aplikacyjnego.
W zakresie komputera centralnego wszystkie działania osób, które posiadały imienne konta lub konta systemowe, logowane były w systemie [redacted], zaś działania użytkowników EUKW (komorników, notariuszy, użytkowników CI) logowane były w centralnej bazie danych ksiąg wieczystych.
Wg wyjaśnień Dyrektora DIRS w systemie NKW/EKW od 1 lipca 2014 r. logi przechowywane były przez 24 miesiące. W zakresie komputera centralnego logi dostępne były od 2010 r. i przechowywane były na macierzach dyskowych. Macierze dyskowe posiadały replikację synchroniczną do zapasowego ośrodka przetwarzania danych. Ponadto po 31 dniach nieużywania pliki z logami były automatycznie przenoszone na taśmy (w dwóch kopiach) i przechowywane w bibliotece taśmowej. Okres retencji wynosił pięć lat. Powyższe działania dotyczące prowadzenia dzienników systemowych były zgodne z § 21 rozporządzenia KRI.

(dowód: akta kontroli str. 617-628)

W trakcie kontroli DIRS przedstawił dzienniki systemowe dla poszczególnych elementów infrastruktury systemu NKW/EKW. Kontrolujący dokonali analizy tych dzienników (wykorzystano pliki logów miesięcznych mainframe typ III) sporządzając wyciągi wskazujące na możliwość zarejestrowania zdarzeń nieprawidłowych lub zagrażających bezpieczeństwu. Dyr. DIRS w odniesieniu do wyciągu wskazującego, iż w dniu 10 stycznia 2014 r. pomiędzy godziną 9:45:05 a godziną 12:12:56 użytkownik [redacted] 145 razy próbował się nieskutecznie zalogować do kilku systemów, w tym NKW, wyjaśnił, iż był to błąd systemu, reakcją było zalogowanie błędu przez system.
W odniesieniu do wyciągu wskazującego, iż użytkownika [redacted] który w okresie od dnia 9 września 2014 r. do dnia 3 lipca 2015 r. próbował zalogować się do systemu NKW ok. 3 tys. razy myląc hasło, Dyr. DIRS wyjaśnił, że był to błąd systemu, reakcją było zalogowanie błędu przez system.

---

[106] Stan na dzień 15 lipca 2015 r.

[107] Rozliczalność polega na zapewnieniu pełnej informacji na temat wszystkich działań, związanych z modyfikacją i przeglądaniem danych, podejmowanych przez każdego z użytkowników systemu.

Odnośnie wyciągu, gdzie ujawniono m.in. pięciu użytkowników [redacted], którzy w okresie od 15 września 2014 r. do 20 lipca 2015 r. zalogowali się mniej niż pięć razy, Dyr. DIRS jako przyczynę powyższego wskazał małą aktywność użytkowników w systemie.

Ponadto z porównania logów z urządzenia Palo Alto 5050[108] (*pa_logslogin_last _year.csv*) z zestawieniem aktywnych użytkowników, którzy mieli dostęp do sieci ministerstwa (różnych zasobów systemowych, nie tylko NKW/EKW) prowadzonym przez WUA (*aktywni_uzytkownicy_palo.xlsx*) wynika, że użytkownik o loginie [redacted] w okresie roku zalogował się ponad 8 tys. razy. *System Palo_Alto wskazał na konto administratora urządzenia Palo Alto. Nie jest to konto używane do dostępu zdalnego, tylko do zalogowania się na konsoli tego urządzenia. To był błąd* – wyjaśnił administrator urządzenia z Zespołu Sieci WUI DIRS. I dodał, że dostęp do konsoli urządzenia ograniczony był do trzech osób, był możliwy tylko w budynku ministerstwa przy ul. Czerniakowskiej 100, w wydzielonej podsieci zarządczej, wydzielonej z sieci LAN MS, a ponadto zabezpieczony był bardzo silnym hasłem. *Liczba zalogowań – ponad 8 tys. razy – wynika stąd, że urządzenie ma wbudowany timer, co powoduje, że administrator loguje się kilkanaście razy dziennie – dla wykonania każdej czynności* – dodał administrator. I oświadczył, iż w toku kontroli NIK w dniu 2 listopada 2015 r. konto [redacted] do konsoli administracyjnej urządzenia Palo Alto zostało usunięte i każdy administrator systemu używa loginu imiennego.

Odnośnie loginów zarejestrowanych z sukcesem w logach pa_logslogin_last _year.csv, których nie wykazano równocześnie w zestawieniu aktywni_uzytkownicy_palo.xlsx, administrator wyjaśnił, iż:

- loginy oznaczone ELP (1 do 20) to były konta założone jednorazowo dla [redacted] na potrzeby szkolenia z system e-płatności i następnie nie były już aktywne;
- konto pod nazwę *workflow* utworzono „na szybko" dla użytkownika DSO[109], ale po ok. dwóch tygodniach zostało zmienione na imienne – pozycja 15 w wykazie;
- część (blisko 30) loginów należy do pracowników firm zewnętrznych realizujących umowy wdrożeniowe/utrzymaniowe;
- 4 loginy to były konta administracyjne do konsoli Palo Alto;
- 2 loginy należały do byłych pracowników;
- a 2 kolejne zostały założone na potrzeby testowe.

(dowód: akta kontroli str. 671-672;1060-1069;1215-1219;2042-2050;2066-2067)

Ustalone nieprawidłowości

Oceniając poziom wspierania bezpieczeństwa w odniesieniu do systemu teleinformatycznego ksiąg wieczystych 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 w działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1. W trakcie przeprowadzonych w 2014 i 2015 r. w DIRS naborów nie sprawdzano zgodności tożsamości kandydatów przez wykorzystanie kilku dokumentów ją potwierdzających, weryfikację treści CV, nie sprawdzano źródeł referencji (jedynie w przypadku kandydata na dyrektora DIRS wskazano na możliwość przedstawienia

[108] Tzw. brzegowego firewalla, który zabezpiecza dostęp do i z wewnętrznej sieci ministerstwa z sieci Internet, filtruje, monitoruje i usuwa niechciany ruch.

[109] Departamentu Sądów, Organizacji i Analiz Wymiaru Sprawiedliwości.

kopii referencji), nie było także wymogu składania przez kandydata jedynie oryginałów dokumentów[110]. Powyższe metody sprawdzenia kandydatów zalecała w pkt 7. 1 .1 (*Postępowanie sprawdzające*) norma PN-ISO/IEC 27002.

Ponadto NIK zauważa, iż w żadnej z umów zawartych z dyrektorami, naczelnikami wydziałów i administratorami systemów informatycznych utrzymywanych przez DIRS (przedstawiono 45 umów) nie określono odpowiedzialności stron w obszarze bezpieczeństwa informacji.

(dowód: akta kontroli str. 629-637;968-970)

Powyższe ustalenia wskazują, iż nie zostały spełnione wymogi określone w § 20 ust. 2 pkt 4 rozporządzenia KRI w zakresie podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zdań oraz obowiązków.

2. W okresie co najmniej do połowy 2015 r. w niewielkim stopniu spełnione zostały wymogi określone w § 20 ust. 2 pkt 6 rozporządzenia KRI w zakresie zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji.

Zgodnie z pkt 9.2.2 PBI MS (*Zarządzanie bezpieczeństwem zasobów ludzkich)* szkolenia dla pracowników w zakresie bezpieczeństwa informacji powinny być przeprowadzane nie rzadziej niż raz na 3 lata oraz każdorazowo po: zmianie przepisów dotyczących bezpieczeństwa informacji, po wprowadzeniu istotnych zmian w polityce oraz na wniosek dyrektora komórki organizacyjnej. Wg. wyjaśnień Dyr. DIRS w okresie od 1 stycznia 2014 r., nie prowadzono szkoleń wstępnych i odświeżających dotyczących bezpieczeństwa informacji dla pracowników mających dostęp do systemu NKW/EKW. Ponadto po przeprowadzeniu audytu w 2013 r. zalecono dokonanie analizy potrzeb szkoleniowych i zorganizowanie cykli szkoleń mających na celu uzupełnienie kompetencji kluczowych pracowników. Notatka z monitoringu wykonania zaleceń ww. audytu (z grudnia 2014 r.) wskazuje, że zalecenie nie zostało zrealizowane. Dyr. BO wyjaśnił, że w związku z zaangażowaniem pracowników Wydziału Ochrony Informacji Niejawnych w szkolenia pełnomocników ds. ochrony informacji niejawnych w sądach i niezapewnieniem dodatkowych etatów, szkolenie dot. bezpieczeństwa informacji planowano przeprowadzić w 2015 r., co nie nastąpiło z powodu zmian organizacyjnych w strukturze MS od lutego 2015 r.

Konieczność podniesienia kompetencji pracowników w zakresie bezpieczeństwa informacji zauważona została także przez realizujących audyt z lipca 2015 r. Kierownictwo MS zdecydowało, iż szkolenia przeprowadzą wyspecjalizowani pracownicy MS. W maju 2015 r. w ramach prac Zespołu ds. bezpieczeństwa informacji opracowano materiały szkoleniowe w zakresie ochrony danych osobowych oraz zasad korzystania z zasobów informatycznych MS, a w październiku 2015 r. rozpoczęto szkolenia w zakresie identyfikacji, klasyfikacji i postępowania aktywami (do zakończenia czynności kontrolnych objęto nim Dyrektora Generalnego oraz dyrektorów i zastępców komórek organizacyjnych MS). Szkolenia pracowników w zakresie ochrony danych osobowych organizowane były przez BDG, a zaplanowane przez ABI miały rozpocząć się w listopadzie[111].

(dowód: akta kontroli str. 13-41;214-234;282-284;405-411;422-428;445-448;617-625;718-721;768-790;982-987;1973-1975;1983-2011)

3. Co najmniej do końca 2014 r. nie przeprowadzono w MS przeglądu aktualności kont użytkowników co było niezgodne z zapisem pkt 6.3 PBST stanowiącym,

---

[110] Analiza dokumentacji dotyczącej przeprowadzonych postępowań na stanowiska pracy w DIRS: 10 procedur w 2015 r. (w tym nabór na Dyrektora i Zastępcę Dyrektora DIRS) oraz 15 procedur w 2014 r.

[111] ABI przeszkolił przedstawicieli firmy zewnętrznej, która podpisała z MS umowę na utylizację dokumentacji.

iż administratorzy systemów zobowiązani byli do analizowania logowań pod kątem kont nie używanych ponad 30 dni. Powyższe zaniechanie stwarzało ryzyko niespełnienia wymogów § 20 ust. 2 pkt 7 rozporządzenia KRI w zakresie zapewnienia ochrony przetwarzanych informacji przed nieuprawnionym dostępem.

Wg ustaleń audytu wewnętrznego z 2014 r. w odniesieniu do kontroli dostępu na przykładzie Active Directory[112] Ministerstwa Sprawiedliwości stwierdzono m.in., że na 1879 kont użytkowników w MS, 350 miało aktywne konta, choć powinny być one wyłączone, wśród aktywnych kont zidentyfikowano loginy osób niepracujących już w MS; stwierdzono aktywne konta użytkowników zewnętrznych, które powinny być zablokowane po zakończeniu zawartych umów[113]. Jako powód powyższej sytuacji audytorzy wskazali m.in. brak nadzoru nad wykonywaniem czynności przez administratorów systemu AD i Service Desk oraz brak regularnych kontroli i przeglądów przeprowadzanych przez ABGZ[114]. Audytorzy zalecili DIRS m.in. dokonanie przeglądu kont użytkowników w systemie AD MS i zablokowanie kont, do których logowanie odbyło się w okresie dłuższym niż 30 dni.

Na przełomie stycznia/lutego 2015 r. zaktualizowane zostały uprawnienia do EOD, FK oraz AD MS, podczas wdrażania nowej struktury organizacyjnej ministerstwa. Zadanie to wykonywało Biuro Dyrektora Generalnego we współpracy z DIRS – poinformował Naczelnik WUA. Wprowadzono też mechanizm, który automatycznie wyszukiwał konta, na które nie logowano się ponad 30 dni[115]. Według informacji Dyr. DIRS, realizacja zaleceń powyższego audytu w zakresie dokonania przeglądu wszystkich systemów teleinformatycznych administrowanych przez MS pod kątem aktualności kont użytkowników nastąpi w ramach projektu „Poprawa zdolności administracyjnych sądów powszechnych w tym systemów informatycznych", działanie nr 4 – „System zarządzania tożsamością". Otwarcie ofert na realizację powyższego zamówienia nastąpiło 1 września 2015 r..

Jednak na dzień 28 października 2015 r. nie zostały opracowane procedury związane z nadawaniem i ewidencjonowaniem uprawnień w systemach teleinformatycznych zgodnie z zaleceniami audytu z lipca 2015 r. (w zakresie zgodności zarządzania bezpieczeństwem informacji z wymaganiami normy PN ISO/IEC 27001). Wg zastępcy Dyr. DIRS analizowane były dopiero możliwości i sposoby wykonania tego zadania.

(dowód: akta kontroli str. 267-281;412-416;617-625;982-997;1313-1318;1380-1425;1873-1878)

2.2 Zarządzanie kontami użytkowników

Opis stanu faktycznego

W pkt 12.6 PBI MS (*Zarządzanie hasłami i innymi danymi uwierzytelniającymi)* podano ogólnie, iż do uwierzytelniania dostępu do systemów informatycznych MS wykorzystywane są certyfikaty klucza publicznego, hasła jednorazowe lub identyfikatory użytkowników i hasła. W pkt 6.3 PBST *(Dostęp użytkowników)* określono zasady przydzielania haseł użytkownikom, w tym że hasło pierwszego logowania powinno być różne dla wszystkich użytkowników, podczas użycia hasła startowego system powinien wymuszać jego zmianę oraz minimalne zasady dla haseł (w tym długość i złożoność hasła). Wg wyjaśnień Dyr. DIRS Active Directory dla NKW/EKW dysponowało funkcjonalnością wymuszającą stosowanie

[112] Wyniki audytu nie dotyczyły użytkowników NKW/EKW, ponieważ system ten posiada dedykowane Active Directory.

[113] Powyższych ustaleń dokonano z wykorzystaniem specjalistycznego programu komputerowego.

[114] Do zadań ABGZ zgodnie z pkt 6.3.5 PBI MS należało m.in. sprawowanie kontroli nad procesem przyznawania praw dostępu oraz nadzorowanie rejestru osób uprawnionych do dostępu do zasobów chronionych.

[115] Powyższe rozwiązanie nie dotyczyło systemu NKW/EKW. DIRS nie miał prawa samodzielnie nadawać/modyfikować/odbierać uprawnień dla użytkowników aplikacji tego systemu (np. pracowników sądów).

obowiązujących reguł dotyczących haseł dostępowych oraz blokowania konta w przypadku użycia błędnego hasła. Departament nie posiada dokumentacji Microsoft potwierdzającej posiadanie dostępność tej funkcjonalności.

Zasady tworzenia haseł dla użytkowników, wskazane w pkt 6.3 PBST, powtórzono w § 5 RUST oraz w punkcie *Metody i środki uwierzytelniania* polityk bezpieczeństwa dla poszczególnych systemów. Ponadto Dyr. DIRS wyjaśnił, że poza loginem i hasłem w ramach uwierzytelniania użytkownicy EKW mieli dostęp do systemu za pomocą certyfikatu. Obowiązywały *Polityka certyfikacji systemu EKW* oraz procedury generowania certyfikatów, tworzenia użytkowników i nadawania uprawnień dla użytkowników w domenie AD w systemie PD CBDKW opisane w dokumentach wytworzonych przez [redacted] Powyższa dokumentacja nie była zatwierdzona, ale była używana z uwagi na konieczność eksploatacji wdrożonych funkcjonalności EKW po 1 lipca 2014 r.[116] Realizował wnioski (tworzył konta, nadawał/odbierał uprawnienia, generował i unieważniał certyfikaty) WUA DIRS.

W pkt 6.4 PBST *(Dostęp administracyjny)* wskazano, iż *hasła kont administracyjnych systemów powinny być deponowane w zaklejonej kopercie. Hasła te przechowuje się w miejscu bezpiecznym. Za kontrolę deponowania haseł odpowiada przełożony Administratora Systemu.* Instrukcja dotycząca haseł systemu NKW znajduje się w dokumencie *Nadzór nad kopiami bezpieczeństwa w POPD i ZOPD MS oraz deponowania haseł dostępowych w DIRS*[117]. W dokumencie tym określono obowiązek deponowania haseł dostępowych (kont administracyjnych i innych niż konta użytkowników wraz z zestawem wszystkich danych tj. nazw kont, haseł itp.), miejsce deponowania i zabezpieczania haseł, ewidencjonowanie haseł (w rejestrze przekazanych haseł w DIRS i w rejestrze dysponowania haseł dostępowych w siedzibie MS). Zgodnie z ww. dokumentem kopie haseł administracyjnych przechowywane były w sejfie w pomieszczeniu o ograniczonym dostępie w gmachu głównym MS (Al. Ujazdowskie 11).

(dowód: akta kontroli str. 13-56;617-628;640-650;699-711)

Ustalone nieprawidłowości

Oceniając poziom wspierania bezpieczeństwa w odniesieniu do systemu teleinformatycznego ksiąg wieczystych 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 w działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1. Dokumentacja polityki nie uregulowała kwestii nadawania uprawnień administracyjnych do systemów, w tym do SI NKW. *Wynika to z faktu, iż w obowiązujących regulacjach określonych w PBI MS i PBST, nie określono takich obowiązków. W związku z powyższym w praktyce, w momencie przyjęcia pracownika do DIRS Naczelnik ustala w zakresie czynności listę zadań oraz listę systemów którymi zajmuje się pracownik. Powierzenie obowiązków nadzoru nad system wskazuje na powierzenie zadań administratora systemu. Zatwierdzenie zakresu obowiązków pracownika stanowi podstawę dla Naczelnika o rejestrowanie wniosku o nadanie uprawnień administracyjnych* - wyjaśnił Dyr. DIRS.

Nadanie uprawnień przeprowadzane było w HPSM w procesie zarządzania zmianą, w schemacie (w uproszczeniu): rejestracja zgłoszenia w Service Desk na wniosek naczelnika WUA – realizacja zgłoszenia przez WUI – akceptacja dyrekcji DIRS –

[116] Szczegóły certyfikacji omówiono w pkt 1.5 wystąpienia.

[117] Powyższa instrukcja przygotowana została w ramach SZJ przed 1 stycznia 2014 r. i obowiązywała w ramach systemu kontroli zarządczej DIRS zgodnie z decyzja Dyrektora DIRS z 24 czerwca 2015 r.

wprowadzenie uprawnień do systemu przez WUI. *Powyższy sposób przyjmowania, realizacji, weryfikacji i akceptacji uprawnień administracyjnych obowiązuje przynajmniej od 1 lipca 2014 r., to znaczy uruchamiania usług związanych z nowymi funkcjonalnościami systemu NKW. Jednakże w okresie od 1 stycznia 2014 do dnia dzisiejszego*[118] *nie było nadawanych uprawnień administracyjnych dla systemu NKW* – wyjaśnił Dyr. DIRS.

NIK zauważa jednak, że w żadnej z procedur nie określono zasad okresowego kontrolowania i odnawiania uprawnień dostępu do systemów i aplikacji, w tym szczególnie uprawnień uprzywilejowanych. Ponadto w okresie objętym kontrolą[119] nie przeprowadzano kontroli w zakresie przestrzegania w systemie NKW/EKW polityki haseł, skuteczności zarządzania tożsamością i kontami użytkowników. Nie podejmowano też działań w zakresie okresowego kontrolowania i odnawiania uprawnień do systemów i aplikacji, w szczególności uprawnień uprzywilejowanych[120] (także do innych niż NKW/EKW systemów utrzymywanych przez DIRS).

(dowód: akta kontroli str. 13-68;594-605;640-644;1575;1909-1913)

Powyższe wskazuje, iż nie zostały spełnione zalecenia normy PN-ISO/IEC 27001 w zakresie stworzenia zarówno formalnego procesu nadawania i odbierania praw dostępu, jak i polityki (procedur) kontroli dostępu. Wskazany brak procedur oraz kontroli zarządzania tożsamością wskazywał na niespełnienie wymogów § 20 ust. 2 pkt 12 lit. h rozporządzenia KRI w odniesieniu do zapewnienia odpowiedniego poziomu bezpieczeństwa systemów teleinformatycznych w zakresie kontroli ich zgodności z odpowiednimi normami i politykami bezpieczeństwa, a także § 20 ust. 2 pkt 7 wymienionego rozporządzenia w zakresie zapewnienia ochrony przetwarzanych informacji przed nieuprawnionym dostępem.

2.3 Ochrona technologii zabezpieczeń

Opis stanu faktycznego

W MS prowadzona była ewidencja aktywów wspierających, odrębnie przez:

- Biuro Administracyjno-Finansowe – ewidencja ilościowo-wartościowa składników majątkowych, w tym m.in. środków trwałych oraz wartości niematerialnych i prawnych,
- DIRS – na potrzeby zapewnienia prawidłowego funkcjonowania i obsługi systemów, urządzeń i rozwiązań informatycznych oraz w celu zapewnienia wsparcia użytkowników MS w zakresie zasobów dotyczących m.in. sprzętu komputerowego występującego przy obsłudze incydentów zgłaszanych za pomocą Service Desk, prowadzono ewidencję elementów konfiguracyjnych w HPSM, przy czym ww. aktywa nie miały przyporządkowanej istotności i poziomu ochrony.

W MS nie było wyodrębnionej ewidencji aktywów wspierających związanych z zapewnieniem bezpieczeństwa systemu NKW/EKW, zawierającej informacje o sprzęcie, oprogramowaniu, sieci, personelu, siedzibie i strukturze organizacyjnej.

W dokumencie *Architektura Bezpieczeństwa Systemu EKW* (do zakończenia czynności kontrolnych dokument nie był zatwierdzony, ale przedstawiał aktualną

[118] Dyr. DIRS przedstawił decyzję nr 2/2015 z 3 lipca 2015 r. w sprawie powołania do pełnienia funkcji Administratora Systemu w systemie Księgi Wieczystej oraz wniosek o odebranie uprawnień z dniem 30 września 2015 r., przed dniem 3 lipca administrator NKW/EKW wykonywał zadania bez formalnego powołania.

[119] Stan na 10 lipca 2015 r.

[120] Taki wymóg nie został zapisany w stosownych procedurach.

strukturę systemu) zidentyfikowano aktywa związane z bezpieczeństwem NKW/EKW, a także ich wrażliwość[121] i krytyczność[122]:

- zasoby infrastruktury środowiskowej ośrodków przetwarzania danych (np. system klimatyzacji i zasilania elektrycznego);
- zasoby infrastruktury IT (sprzęt IT, oprogramowanie);
- aktywa informacyjne (bazy danych, systemy plików, kopie bezpieczeństwa i dane zarchiwizowane, ślady audytowe).

(dowód: akta kontroli str. 606-610;640-644;653-666;699-714)

Zarządzanie elementami systemów informatycznych, w tym NKW/EKW, realizowane było z wykorzystaniem procesów zarządzania zmianą i konfiguracją. Procesy te zostały zaimplementowane w systemie HPSM, a obligatoryjność ich stosowania wynikała z decyzji Dyr. DIRS z 24 czerwca 2015 r.

Dodatkowo, sposób i zasady dystrybucji nowych wersji systemu NKW/EKW do wszystkich lokalizacji (aplikacji, modułów) powstałych w wyniku naprawy błędów lub wykonanej modyfikacji określone zostały w załączniku nr 13 do umowy z [redacted]. Nowe wersje wdrażane były na podstawie polecenia wdrożenia wersji, przygotowywanego w formie papierowej i elektronicznej. Wersje przechowywane były w odrębnym repozytorium, jak również na nośnikach dostarczonych przez wykonawcę w archiwum. Historia zmian konfiguracji wraz z informacjami o dokonanych modyfikacjach rejestrowana była w systemie HPSM.

Zasady realizacji usługi polegającej na nadzorze nad eksploatacją, świadczenia serwisu i wsparcia technicznego dla systemu NKW/EKW opisane zostały w § 8 umowy z [redacted]. Do obowiązków Wykonawcy należało m.in.: usuwanie we wszystkich lokalizacjach, awarii i uszkodzeń systemu oraz skutków awarii systemu, sprzętu i oprogramowania, a także wszelkich negatywnych skutków spowodowanych korzystaniem z błędnie działających wersji systemu.

W zakresie serwisowania zasobów IT, w tym dla NKE/EKW, procedura określona została w instrukcji *Obsługa napraw zasobów IT*. Dodatkowo dla poszczególnych elementów infrastruktury technicznej (urządzenia komputerowe, serwery, macierzy dyskowe, urządzenia sieciowe) zawarte zostały umowy na serwis gwarancyjny tych urządzeń.

Podstawą działań w zakresie utylizacji zasobów IT, w szczególności elementów NKW/EKW, były:

- rozporządzenie Rady Ministrów z dnia 21 maja 2010 r. w sprawie sposobu i trybu gospodarowania składnikami rzeczowymi majątku ruchowego, w który wyposażone są jednostki budżetowe[123],
- Zarządzenie nr 13/2011 Dyrektora Generalnego Ministerstwa Sprawiedliwości z dnia 22 lutego 2011 r. w sprawie powołania oraz zakresu działania Komisji do oceny przydatności, sprzedaży i likwidacji zużytych i zbędnych składników rzeczowych majątku ruchomego Ministerstwa Sprawiedliwości.

Dyr. DIRS wyjaśnił, że MS nie był stroną umowy na świadczenie przez podmioty zewnętrzne na jego rzecz usług niszczenia nośników danych.

(dowód: akta kontroli str. 626-628;653-670;1313-1318;1333-1336)

---

[121] Jako wrażliwość należy rozumieć atrybut informacji wskazujący, że jej ujawnienie przyniesie straty dla resortu sprawiedliwości.

[122] Jako krytyczność należy rozumieć atrybut aktywów wskazujący, że brak dostępu do niego przyniesie straty dla resortu sprawiedliwości.

[123] Dz. U. Nr 114, poz. 761

Dzienniki udanych i nieudanych prób logowania prowadzone były:

- w zakresie serwerów z technologią Microsoft Windows – w dzienniku zdarzeń „Security", który to dziennik powstaje przy instalacji systemu. Zapis w dzienniku zawierał m.in. informacje dotyczące daty zdarzenia, nazwy konta jakiego dotyczyło logowanie oraz adresu sieciowego z jakiego pochodziło logowanie;
- w zakresie serwerów z technologią [redacted] – w logu systemu z/OS na platformie [redacted] który to log powstaje przy instalacji systemu. Zapis w logu zawierał m.in. informacje o dacie zdarzenia, nazwę konta jakiego dotyczyło logowanie, a także zasobu do jakiego osoba chciała uzyskać dostęp;
- w zakresie urządzeń sieciowych – na urządzeniu CISCO ACS rejestrowane były udane i nieudane zdarzenia związane z logowaniem do urządzeń sieciowych.

Dzienniki uruchomionych blokad dotyczących dostępu do istotnych plików i istotnych fizycznych urządzeń (interfejsów do zarządzania nimi) prowadzone były:

- w zakresie serwerów z technologią Microsoft Windows – system plików NTFS zaimplementowany w systemach operacyjnych Windows umożliwiał nadawanie poszczególnych uprawnień od katalogów i plików dla konkretnych kont / grup użytkowników,
- w zakresie serwerów z technologią [redacted] – log powstawał w narzędziach systemu bezpieczeństwa RACF na podstawie logu systemowego,
- w zakresie urządzeń sieciowych – realizowany był przez urządzenie PaloAlto 5050 z systemem Global Protect.

Jak wyjaśnił Dyr. DIRS, za analizę zapisów w dziennikach odpowiedzialni byli administratorzy poszczególnych urządzeń. Analiza zapisów należała do rutynowych czynności administratorskich, jednak częstotliwość tej analizy nie była określona – wynikała z dobrych praktyk administratora.

W MS nie została opracowana procedura zmian domyślnych lub tymczasowych haseł na instalowanym i wykorzystywanym sprzęcie. Dyr. DIRS wyjaśnił, że zmiana domyślnego hasła wynikała z dobrych praktyk administratora instalującego nowe urządzenie. W zakresie sprzętu komputerowego wykorzystującego token użytkownik przy wydaniu urządzenia (tokena) był zobowiązany do zmiany hasła. Procedura dotycząca zmian domyślnych lub tymczasowych haseł w instalowanym lub wykorzystywanym w jednostce sprzęcie była stosowana w przypadku stacji roboczych w zakresie zmiany haseł pierwszego logowania albo zmiany haseł tymczasowych.

(dowód: akta kontroli str. 653-670;1664-1669)

Analiza treści wybranych czterech umów, w tym umów zawartych z [redacted] na zaprojektowanie, wykonanie i wdrożenie systemu EKW oraz umowy z [redacted] na wykonanie audytu bezpieczeństwa teleinformatycznego, wykazała, że wykonawców zobowiązywano do zachowania w poufności wszelkich informacji uzyskanych w związku z zawarciem umów zarówno w trakcie jej obowiązywania, jak i po jej zakończeniu.

(dowód: akta kontroli str. 626-628;1354-1369;1686-1695;1959-1960;1976-1978)

Ustalone nieprawidłowości

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

2.4 Wymiana wrażliwych danych

Opis stanu faktycznego

Zgodnie z art. 2 ustawy 6 lipca 1982 r. o księgach wieczystych i hipotece księgi wieczyste są jawne. Rejestr ksiąg wieczystych, czyli centralna baza danych ksiąg wieczystych jest prowadzony na mocy ustawy. Zakres danych wprowadzanych do rejestru, określony został w art. 25 ustawy. Dane wpisywane do rejestru określone zostały w rozporządzeniu Ministra Sprawiedliwości z dnia 21 listopada 2013 r. w sprawie zakładania i prowadzenia ksiąg wieczystych w systemie informatycznym[124]. Wszelkie zmiany zakresu danych wpisywanych do centralnej bazy danych ksiąg wieczystych są następstwem zmiany ww. rozporządzenia. Zgodnie z ustawą, właścicielem danych gromadzonych w rejestrze są sądy rejonowe prowadzące księgi wieczyste. System NKW/EKW zawiera podsystem SOWKW funkcjonujący w tych sądach. W SOWKW prowadzone były urządzenia ewidencyjne określone w Zarządzeniu Ministra Sprawiedliwości z dnia 12 grudnia 2013 r. w sprawie organizacji i zakresu działania sekretariatów sądowych oraz innych działów administracji sądowej. W zarządzeniu określony został zakres danych gromadzonych w urządzeniach ewidencyjnych sądu. Właścicielem tych danych jest sąd rejonowy. W podsystemie Centralnej Informacji Ksiąg Wieczystych, np. rejestruje się fakt wydania odpisu księgi wieczystej. Właścicielem tych danych jest Minister Sprawiedliwości.

Dyr. DIRS wyjaśnił, że danych przechowywanych w rejestrze ksiąg wieczystych w żaden sposób się nie klasyfikuje, ponieważ wszystkie są ogólnodostępne i każdy może przeglądać księgę wieczystą po podaniu jej numeru. Dane gromadzone w systemie SOWKW są dostępne dla pracowników sądów, zgodnie z przyznanymi im uprawnieniami, o których decyduje przewodniczący wydziału ksiąg wieczystych, składając wniosek o nadanie uprawnień. Natomiast dane CI były dostępne dla pracowników Centralnej Informacji o Zastawach Rejestrowych, Krajowego Rejestru Sądowego oraz Ksiąg Wieczystych, zgodnie z przyznanymi im uprawnieniami, o których decydował jej Naczelnik.

(dowód: akta kontroli str. 675-679)

Zgodnie z pkt 5 instrukcji *Nadzór nad kopiami bezpieczeństwa w POPD i ZOPD MS oraz deponowania haseł dostępowych w DIRS* w pierwszym dniu roboczym kolejnego tygodnia Kierownik Zespołu Komputera Centralnego WUI lub pracownik przez niego wyznaczony przewozić miał najnowsze kopie bezpieczeństwa w postaci taśm z backupem do depozytu, jednocześnie pobierając najstarsze znajdujące się w depozycie kopie bezpieczeństwa. Zasady dotyczące m.in. zamawiania transportu taśm, ich bezpiecznego przewożenia oraz uzupełniania rejestru deponowania określone zostały w procedurze *Transport taśm*. Dyr. DIRS wyjaśnił, że ww. procedura została wdrożona i była stosowana oraz, że wkrótce zostanie zatwierdzona.

W MS nie określono zasad przesyłania wrażliwych danych i informacji przez sieć publiczną, ponieważ w NKW/EKW dane przekazuje się tylko za pomocą teleinformatycznej sieci dedykowanej (nie publicznej) za wyjątkiem usług dostępowych w sieci publicznej. Wg. wyjaśnień Dyr. DIRS sieć WAN MS oparto o usługę Biznes VPN zgodnie z podpisaną umową z [redacted] Usługa ta pozwala na łączenie wszystkich lokalizacji klienta w jedną sieć WAN, pozwalając klientowi na budowę własnej sieci korporacyjnej, transmisję danych, głosu oraz wideo pomiędzy użytkownikami. W sieci WAN została wdrożona separacja sieci z wykorzystaniem list dostępowych. Sieć zamawiającego została

[124] Dz. U. z 2013 r. poz. 1411 ze zm.

podzielona logicznie na cztery podsieci: Sieć MS, Rejestry, KRK, Telefonia IP. Zgodnie z zawartą umową sieć WAN MS była odseparowana od sieci Internet.

Dyr. DIRS wyjaśnił dodatkowo, że dla poszczególnych poziomów ochrony danych i informacji znajdujących się w systemie NKW/EKW nie określono typu oraz siły algorytmów kryptograficznych z uwagi na fakt, iż dane te są jawne.

(dowód: akta kontroli str. 675-681;684-693;699-711;1955-1958;1966-1970)

Ustalone nieprawidłowości

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

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia wspieranie bezpieczeństwa w systemie informatycznym NKW/EKW na poziomie 3.Zdefiniowane, z uwagi na:

- brak w kontrolowanym okresie błędów i awarii systemu skutkujących naruszeniem poufności, integralność i dostępność danych (np. utratą lub uszkodzeniem);
- realizowanie procesów związanych z funkcjonowaniem systemu zgodnie z przyjętymi praktykami, ale bez formalnych procedur lub na podstawie procedur stosowanych lecz nie zatwierdzonych, co wynikało ze słabości zarządzania systemem bezpieczeństwa informacji;
- przygotowanie i częściową implementację dokumentacji systemu, w tym odnoszącej się do jego bezpieczeństwa, w ramach realizacji projektu *Wprowadzenie e-usług w zakresie ksiąg wieczystych*, której zatwierdzenie zostało jednak opóźnione z uwagi na podpisanie z wykonawcą powyższego projektu w dniu 31 sierpnia 2015 r. aneksu nr 8 do umowy z [redacted] co skutkowało nie zakończeniem procesu pełnego wdrożenia systemu EUKW;
- faktyczny brak administratora systemu NKW/EKW od dnia 5 sierpnia 2015 r., co niosło ryzyko braku właściwego nadzoru nad jego funkcjonowaniem, w tym w zakresie zapewnienia jego bezpieczeństwa.

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[125], wnosi o:

1. Uporządkowanie i uproszczenie struktury zarządzania bezpieczeństwem informacji w Ministerstwie Sprawiedliwości, na poziomie organizacyjnym oraz dokumentacji polityk bezpieczeństwa, w tym rozważenie powołania Pełnomocnika odpowiedzialnego za nadzorowanie bezpieczeństwa informacji, wyposażonego w zasoby finansowe i osobowe - grupę ludzi o różnych kompetencjach i zakresie wiedzy z obszaru bezpieczeństwa informacji.
2. Dokończenie, zapoczątkowanego w 2015 r., procesu świadomego budowania systemu zarządzania bezpieczeństwem informacji opartego na identyfikacji aktywów, identyfikacji zagrożeń dla poszczególnych aktywów oraz szacowaniu ryzyka, tak aby przygotowana dokumentacja SZBI w pełni odpowiadała specyfice Ministerstwa Sprawiedliwości, działu IT i innych komórek organizacyjnych.

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

3. Proceduralne i faktyczne rozdzielenie procesu zgłaszania, ewidencjonowania i reagowania na incydenty związane z bezpieczeństwem informacji od zdarzeń dotyczących pomocy użytkownikom w obsłudze stacji roboczych i innych urządzeń IT oraz wykorzystanie analizy tych incydentów do zarządzania bezpieczeństwem informacji w skali danego systemu i w skali całej instytucji.
4. Zoptymalizowanie korzystania z ustaleń i zaleceń audytów w sferze bezpieczeństwa teleinformatycznego, w celu uniknięcia zastępowania audytami (w szczególności zewnętrznymi) rzeczywistych działań koniecznych dla doskonalenia systemu zarządzania bezpieczeństwem informacji.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

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

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do Prezesa Najwyższej Izby Kontroli.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

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

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

Warszawa, dnia 23.XII.2015 r.

Prezes
Najwyższej Izby Kontroli
Krzysztof Kwiatkowski

.....
podpis