PREZES
NAJWYŻSZEJ IZBY KONTROLI
Krzysztof Kwiatkowski

KPB.410.004.06/2015
P/15/042

WYSTĄPIENIE POKONTROLNE

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli	P/15/042 – Zapewnienie bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych.
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Departament Porządku i Bezpieczeństwa Wewnętrznego
Kontroler	Mariusz Perzyna, specjalista kontroli państwowej, upoważnienie do kontroli nr 93496 z dnia 29 maja 2015 r.
	(dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Komenda Główna Straży Granicznej, 02 – 514 Warszawa, Al. Niepodległości 100
Kierownik jednostki kontrolowanej	Gen. dyw. SG Dominik Tracz, Komendant Główny Straży Granicznej

II. Ocena kontrolowanej działalności

W oparciu o stosowany w metodyce CobiT 4.1 Model dojrzałości[1] NIK ocenia poziom zarządzania procesem „zapewnienie bezpieczeństwa systemów teleinformatycznych" w Komendzie Głównej Straży Granicznej (KGSG) jako „początkowy/doraźny".

Na powyższą ocenę przede wszystkim wpływ miało niezbudowanie przez Komendanta Głównego formalnych podstaw do zapewnienia bezpieczeństwa w szczególności rzetelnej polityki bezpieczeństwa oraz systemu rejestrowania i obsługi incydentów. W okresie objętym kontrolą (od 1 stycznia 2014 do 1 października 2015) Komendant Główny Straży Granicznej nie wprowadził uregulowań dotyczących zarządzania procesem bezpieczeństwa pomimo, że opracowanie takich procedur zalecali audytorzy wewnętrzni KGSG już w październiku 2013 r. Zapewnienie bezpieczeństwa oparte było głównie na powszechnie obowiązujących przepisach dotyczących ochrony danych osobowych oraz ochrony informacji niejawnych. Kontrolowana jednostka dopiero rozpoczęła budowanie formalnych podstaw systemu zarządzania bezpieczeństwem informacji. W KGSG bezpieczeństwo IT nie podlegało pomiarowi ze względu na nieokreślenie mierników bezpieczeństwa informacji i zasad jego monitorowania. Nie opracowano również formalnych podstaw systemu zarządzania ryzykiem w zakresie bezpieczeństwa jawnych informacji obejmującego m.in. szacowanie ryzyka, postępowania z ryzykiem oraz systematyczne monitorowanie i przeglądanie ryzyka.

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

III. Wyniki kontroli

1. Zarządzanie bezpieczeństwem IT oraz podstawowe dokumenty dotyczące bezpieczeństwa informacji.

Określenie odpowiedzialności w zakresie bezpieczeństwa informacji

Opis stanu faktycznego

Analiza zakresów obowiązków osób odpowiedzialnych za bezpieczeństwo IT oraz regulaminów organizacyjnych komórek KGSG nie wykazała nieprawidłowości w zakresie przypisania odpowiedzialności. Zapewnienie bezpieczeństwa systemów teleinformatycznych należało do obowiązków dyrektora Biura Łączności i Informatyki[2].

Decyzją nr 73[3] z dnia 28 kwietnia 2015 roku Komendant Główny Straży Granicznej powołał Komitet do spraw Bezpieczeństwa Teleinformatycznego Straży Granicznej składający się z 8 osób oraz Zespół Security Operations Center Straży Granicznej, w skład którego wchodziło 12 osób. Członkami zarówno Komitetu jak i Zespołu w większości byli pracownicy Biura Łączności i informatyki KGSG (BŁiI KGSG) oraz Biura Ochrony Informacji Niejawnych KGSG (BOI KGSG). Do zadań Komitetu do spraw Bezpieczeństwa Teleinformatycznego Straży Granicznej należało m.in. opracowywanie, rozwijanie i kreowanie szeroko rozumianej polityki bezpieczeństwa. Do dnia 23 października br. odbyło się jedno spotkanie Komitetu ds. Bezpieczeństwa Teleinformatycznego w dniu 15 lipca 2015 r.

(dowód: akta kontroli str. 5-13, 391 płyta CD)

Polityka bezpieczeństwa

Opis stanu faktycznego

KGSG dopiero w II kwartale 2015 r. realnie rozpoczęła budowę formalnych podstaw systemu zapewnienia bezpieczeństwa informacji. Powyższe przedsięwzięcie realizowane jest we współpracy z NASK (Naukową i Akademicką Siecią Komputerową) na podstawie umowy podpisanej w dniu 22 maja 2015 roku przez Dyrektora Biura Łączności i Informatyki KGSG z NASK. Jednym z istotnych elementów, które będą objęte współpracą pomiędzy NASK a SG będzie wspólne wykonanie polityki bezpieczeństwa IT.
W ramach współpracy z NASK Straż Graniczna zamierza m.in.:

1. Stworzyć nowy zewnętrzny portal internetowy,
2. Opracować i wdrożyć politykę bezpieczeństwa informacji,
3. Opracować i wdrożyć System Zarządzania Bezpieczeństwem Informacji.

NIK zauważa, że opracowanie tego systemu powinno być poprzedzone dogłębną analizą infrastruktury oraz wszystkich obowiązujących uregulowań prawnych mających wpływ na bezpieczeństwo teleinformatyczne. Powyższy pogląd potwierdził Komendant Główny SG w piśmie z dnia 11 czerwca 2015 r. (KG 01 460/VII/15).

(dowód: akta kontroli str. 13)

Zdaniem NIK wdrożenie tego systemu wymaga przeprowadzenia rzetelnej analizy ryzyka utraty informacji (po uprzednim wprowadzeniu formalnych podstaw szacowania i postępowania z ryzykiem) oraz określenia i wdrożenia systemu monitorowania procesów związanych z bezpieczeństwem informacji.
Zakończony w październiku 2013 r. audyt pn. *zarządzanie bezpieczeństwem systemów teleinformatycznych w KGSG* stwierdził, że w KGSG brak jest polityki bezpieczeństwa informacji, jak również polityki bezpieczeństwa teleinformatycznego, która obejmowałaby wszystkie systemy teleinformatyczne

---

[2] Zgodnie z § 5 pkt 3 załącznika do zarządzenia nr 21 Komendanta Głównego Straży Granicznej z dnia 8 marca 2012 r. w sprawie regulaminu organizacyjnego BŁiI.
[3] Decyzja niepublikowana.

funkcjonujące w jednostce. Jak wskazali audytorzy brak formalnego dokumentu określającego politykę bezpieczeństwa teleinformatycznego w KGSG stanowi ryzyko braku odpowiednich mechanizmów kontrolnych m.in. w zakresie zapewnienia odpowiedniej ochrony sprzętu przekazanego do użytkowania funkcjonariuszom KGSG, okresowych przeglądów praw dostępu użytkowników do poszczególnych systemów teleinformatycznych, czy sposobu postępowania z incydentami.

(dowód: akta kontroli str. 672-712)

Ustalone nieprawidłowości

W okresie objętym kontrolą nie wprowadzono rzetelnej, powiązanej z innymi regulacjami wewnętrznymi polityki bezpieczeństwa. W zakresie dotychczasowych regulacji stanowiących podstawę zapewnienia bezpieczeństwa informacji w KGSG wyjaśniono, iż na całościową politykę bezpieczeństwa informacji składa się cały dorobek prawny Komendanta Głównego Straży Granicznej, *cała dokumentacja bezpieczeństwa oraz wszystkie instrukcje, zalecenia, opinie kierowników komórek organizacyjnych KGSG i jednostek organizacyjnych SG, wydawane na podstawie zadań określonych w regulaminach organizacyjnych.* W szczególności wskazywano na Decyzję Nr 129 Komendanta Głównego Straży Granicznej z dnia 11 czerwca 2014 r. w sprawie ochrony danych osobowych przetwarzanych w Straży Granicznej[4]. Z ustaleń kontroli jednakże wynika, że w SG funkcjonują również systemy nieprzetwarzające danych osobowych m.in. SIP[5], portal zewnętrzny i portal wewnętrzny. Zgodnie z regulaminem organizacyjnym opracowanie procedur należy do zadań Biura Łączności i Informatyki[6].

(dowód: akta kontroli str. 96)

Zdaniem NIK zbiór dokumentów będących, wg wyjaśnień, planem bezpieczeństwa informacji SG jest złożony z elementów o różnym zakresie, szczegółowości i przedmiocie. Takie rozproszenie informacji, zdaniem NIK utrudnia praktyczne korzystanie z informacji użytkownikom systemów informatycznych SG zobowiązanych do zapoznania się i przestrzegania zasad bezpieczeństwa. W tym zbiorze nie została również jasno określona hierarchia dokumentów tj. nadrzędności jednych aktów nad drugimi oraz powiązania między nimi. Zdaniem NIK rzetelne opracowanie podstawowych dokumentów zapewniających bezpieczeństwo informacji polega m.in. na zapewnieniu czytelności, przejrzystości jak również precyzyjnego określenia powiązań i zależności z innymi regulacjami wewnętrznymi. Brak wskazania takich powiązań i zależności powoduje trudności w aktualizacji tych dokumentów.

Z uzyskanych wyjaśnień wynika, że dowództwo SG ma świadomość potrzeby opracowania polityki bezpieczeństwa, *która będzie dokumentem realnie wykorzystywanym w codziennym funkcjonowaniu formacji, a nie tylko „pozycją biblioteczną".* W ocenie NIK powyższy stan rzeczy nie uległ zasadniczej poprawie po wprowadzeniu (mimo początkowych wątpliwości co do zasadności takiego dokumentu w SG[7]), w dniu *25 czerwca 2015 r. Polityki Bezpieczeństwa Informacji w Straży Granicznej.* Zgodnie z treścią tej Polityki jest to ogólny dokument gromadzący i definiujący podstawowe informacje, które w przyszłości będą stanowiły podstawę do budowy systemu bezpieczeństwa SG a na podstawie Polityki

---

[4] Dz. Urz. KGSG poz. 90.

[5] System Informacji Prawnej

[6] Zgodnie z § 2 pkt 7 załącznika do zarządzenia nr 21 Komendanta Głównego Straży Granicznej z dnia 8 marca 2012 r. w sprawie regulaminu organizacyjnego BŁiI KGSG Biuru Łączności i Informatyki przypisano obowiązek opracowywania procedur, standardów oraz systemowych rozwiązań organizacyjnych w zakresie teleinformatyki, w tym w zakresie infrastruktury klucza publicznego oraz przyjętych rozwiązań w zakresie bezpieczeństwa systemów teleinformatycznych

[7] Komendant Główny SG poinformował w piśmie z dnia 30 czerwca 2015, ze początkowo nie podpisywał Polityki bezpieczeństwa ze względu na fakt, iż niecelowym wydawało się aby centralny organ administracji rządowej deklarował, że będzie realizował zadania nakazane przepisami prawa.

Bezpieczeństwa i zawartych w niej ogólnych zasad bezpieczeństwa zostaną opracowane szczegółowe polityki, procedury i instrukcje oraz regulaminy.
Ustalono, że podpisanie Polityki miało czynić zadość zaleceniom wynikającym z norm. NIK zwraca uwagę, że zgodnie z normą grupy PN-ISO/IEC 27001: 2014-12 organizacja powinna ustanowić politykę bezpieczeństwa informacji zawierając w niej m.in. cele bezpieczeństwa informacji (pkt. 5.2), ustanowionym celom w zakresie bezpieczeństwa informacji sformułowanym przez organizację winny być przypisane mierniki oraz harmonogram ich wprowadzenia (pkt. 6.2). Powyższe działanie powinno uwzględniać wyniki rzetelnie przeprowadzonego szacowania ryzykiem i postępowania z ryzykiem (pkt. 6.2 lit. c). Przedłożona kontrolerowi NIK Polityka nie zawierała ww. elementów.

(dowód: akta kontroli str. 92 – 120, 391)

Zapewnienie przypisania informacjom odpowiedniego poziomu ochrony, zgodnego z ich wagą dla organizacji.

Opis stanu faktycznego

Komendant Główny Straży Granicznej zarządzeniem nr 1 z dnia 2 stycznia 2015 r. w sprawie sposobu i trybu gromadzenia i przetwarzania informacji z zakresu ochrony granicy państwowej, kontroli ruchu granicznego oraz zapobiegania i przeciwdziałania nielegalnej migracji[8], określił sposób i tryb gromadzenia i przetwarzania w Straży Granicznej informacji, w tym:

- tworzenie zbiorów informacji oraz przetwarzanie w nich informacji;
- zasady zapewniające właściwe funkcjonowanie oraz bezpieczeństwo systemów informatycznych;
- sposób weryfikacji i okresy przechowywania informacji.

Zgodnie z § 5 ust. 2 zarządzenia w zakresie zasad zapewniających właściwe funkcjonowanie oraz bezpieczeństwo systemów informatycznych określono między innymi, iż zapewnia się w zależności od kategorii informacji, zachowanie właściwego poziomu ochrony i bezpieczeństwa przetwarzanym informacjom przez zastosowanie środków technicznych i organizacyjnych odpowiednich do zagrożeń.
W KGSG nie określono kluczowych informacji dla realizowanych przez SG zadań. Komendant Główny wyjaśnił, że kluczowe zadania SG określa ustawa[9] i tym samym to ustawa identyfikuje kluczowe dla SG informacje.
Ponadto wyjaśnił: *Dla każdego z Biur KGSG istotne są inne informacje, każdy zarząd lub biuro ma swoją specyfikę.*

(dowód: akta kontroli str. 225-226)

Ustalone nieprawidłowości

W KGSG nie dokonano szczegółowej analizy przetwarzanych informacji wraz z przypisaniem im istotności dla funkcjonowania SG. NIK podziela pogląd Komendanta Głównego, iż najważniejsze informacje są chronione na podstawie ustawy o ochronie informacji niejawnych. Jednakże nie sposób zgodzić się ze stwierdzeniem, iż w systemach jawnych SG nie przetwarza się kluczowych informacji, więc nadzór nad nimi jest mniejszy. Zdaniem NIK kluczowe informacje dla SG mogą być zawarte również w dokumentach i systemach jawnych.

(dowód: akta kontroli str. 321-322)

Zarządzanie ryzykiem

Opis stanu faktycznego

W KGSG nie opracowano i nie wdrożono procedury regulującej szacowanie ryzyka w obszarze bezpieczeństwa informacji. Szacowanie ryzyka dla poszczególnych systemów niejawnych oparte jest na zaleceniach ABW. Zgodnie z wyjaśnieniami szacowanie ryzyka w obszarze bezpieczeństwa cyberprzestrzeni realizowane jest na podstawie wytycznych przekazywanych przez Ministerstwo Administracji

[8] Dz. Urz. KGSG poz. 1.
[9] Ustawa z dnia 12 października 1990 o Straży Granicznej (Dz. U. z 2014 r. poz. 1402 ze zm.)

i Cyfryzacji. Przedłożone przez KG SG wyniki oceny ryzyka nie obejmują wszystkich systemów nie posiadają też przypisanego właściciela ryzyka.

Ustalone nieprawidłowości

Zgodnie z § 20 ust. 2 pkt. 3 rozporządzenia KRI[10] Kierownik jednostki jest zobowiązany zapewnić przeprowadzanie okresowych analiz ryzyka utraty informacji oraz podejmowania działań minimalizujących te ryzyko, stosownie do czynników przeprowadzonej analizy. Norma PN-ISO/IEC 27001:2014-12 zaleca, aby organizacja opracowała i wdrożyła proces szacowania ryzyka w bezpieczeństwie informacji (pkt. 6.1.2) oraz opracowała i wdrożyła proces postępowania z ryzykiem (pkt. 6.1.3).
Komendant Główny Straży Granicznej nie opracował i nie wdrożył metodologii procesu szacowania ryzykiem bezpieczeństwa informacji oraz postępowania z ryzykiem, w tym systematycznego monitorowania i przeglądania ryzyka.
Co prawda dokonywano analizy ryzyka na podstawie wytycznych i zaleceń podmiotów zewnętrznych (MAiC), ale w ocenie NIK przedstawione kontrolerowi oceny ryzyka nie spełniają przytoczonych wyżej uregulowań, tzn. była to analiza ryzyka na poziomie strategicznym, na potrzeby realizacji wymagań Polityki ochrony cyberprzestrzeni RP.

(dowód: akta kontroli str. 76-90; 223)

Ocena badanego obszaru

NIK ocenia 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 jako „początkowy/doraźny". Powyższą ocenę uzasadniają brak podstawowych dokumentów umożliwiających ustalenie zasad bezpieczeństwa wraz z efektywnymi mechanizmami ich egzekwowania, które obejmowałyby wszystkie systemy w SG, co oznacza, że bezpieczeństwo zapewniane jest na doraźnych zasadach. Zdaniem NIK Komenda Główna Straży Granicznej dopiero rozpoczęła opracowanie formalnych podstaw budowy Systemu Zarządzania Bezpieczeństwem Informacji, o którym mowa m.in. w § 20 ust. 1 rozporządzenia KRI. NIK negatywnie odnosi się do dwuletniej zwłoki w realizacji zaleceń audytu zarządzania bezpieczeństwem systemów teleinformatycznych w Komendzie Głównej Straży Granicznej zakończonego w październiku 2013 r.

2. Testowanie, nadzorowanie i monitorowanie bezpieczeństwa oraz zbieranie i analizowanie incydentów bezpieczeństwa

Opis stanu faktycznego

Oprócz audytów przeprowadzanych na podstawie ustawy o ochronie danych osobowych oraz ochrony informacji niejawnych oraz przywołanego wyżej audytu pn. *zarządzanie bezpieczeństwem systemów teleinformatycznych w KGSG* w latach 2013-2014 przeprowadzone były przez audytorów wewnętrznych z Inspektoratu Kontroli i Audytu Wewnętrznego KGSG, zadania audytowe w zakresie związanym z bezpieczeństwem systemów teleinformatycznych:

1. „Audyt bezpieczeństwa informacji w KGSG" (2013 r.). Celem zadania audytowego była analiza i ocena adekwatności, skuteczności efektywności systemu zarządzania bezpieczeństwem informacji w Komendzie Głównej Straży Granicznej, w obszarze „Bezpieczeństwo fizyczne i środowiskowe – obszary bezpieczne".

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

2. „Audyt bezpieczeństwa informacji w KGSG" (2014 r.). Celem zadania audytowego była analiza i ocena adekwatności, skuteczności i efektywności systemu zarządzania bezpieczeństwem informacji w Komendzie Głównej Straży Granicznej, w obszarze „Bezpieczeństwo fizyczne i środowiskowe – bezpieczeństwo sprzętu".

Szczegółowe ustalenia oraz rekomendacje z powyższych czynności audytowych zawarto w sprawozdaniach oznaczonych klauzulą „ zastrzeżone". Wg złożonych wyjaśnień w KGSG zostały zrealizowane zalecenia audytowe zawarte w sprawozdaniach z ww. zadań audytowych. Do działań podjętych w zakresie realizacji zalecenia audytorów wewnętrznych należy między innymi zadanie opracowania polityki bezpieczeństwa w zakresie systemów teleinformatycznych, które powierzone zostało Komitetowi do spraw Bezpieczeństwa Teleinformatycznego Straży Granicznej.

(dowód: akta kontroli str. 92 – 98, 672– 712)

Kontrolerowi nie przedłożono procedur określających jak często i w jakim zakresie weryfikowana jest poprawność działania systemu (CBD SG SWK[11]).

(dowód: akta kontroli str. 200)

Ustalone nieprawidłowości

Ustalono, że incydenty bezpieczeństwa dotyczące infrastruktury technicznej są gromadzone i analizowane. Jednakże w KGSG nie zbudowano formalnych podstaw systemu zbierania i analizy incydentów bezpieczeństwa. Nie opracowano procedur jednoznacznie precyzujących kiedy i komu należy zgłaszać incydenty bezpieczeństwa (w tym incydenty teleinformatyczne), nie określono obowiązku tworzenia rejestru incydentów czy osób odpowiedzialnych za ich analizę. Zdaniem NIK powyższy stan faktyczny nie spełnia wymagań § 20 ust. 2 pkt. 13 rozporządzenia KRI[12]. NIK zauważa, że Norma PN-IEC 27001:2014-12 w pkt. A 16.1.1 zaleca ustanowienie odpowiedzialności kierownictwa oraz procedur zapewniających szybką, skuteczną i zorganizowaną reakcję na incydenty związane z bezpieczeństwem informacji.

W trakcie trwania czynności kontrolnych w KG SG opracowano „Plan zarządzania incydentami związanymi z bezpieczeństwem informacji w Straży Granicznej", (Plan zarządzania) zaakceptowany przez Komendanta Głównego w dniu 25 czerwca 2015. Powyższy dokument zawiera m.in. definicję incydentu i plan przygotowania i wdrożenia docelowego systemu zarządzania incydentami bezpieczeństwa. W pkt. 2 Planu zarządzania zapisano, że stanowi on podstawę tworzenia szczegółowych procedur reagowania na incydenty. NIK podziela tezę zawartą w planie, że jego kompletność wymaga opracowania dalszych, szczegółowych instrukcji i procedur zarządzania incydentami oraz współpracy z innymi podmiotami. Zgodnie z Decyzją 61 Komendanta Głównego SG z dnia 3 kwietnia 2015 r. nadzór nad opracowaniem i wdrażaniem procedur reagowania na incydenty komputerowe, które będą obowiązywały w SG powierzono Pełnomocnikowi KGSG ds. Bezpieczeństwa Cyberprzestrzeni w Straży Granicznej.

NIK zwraca uwagę Pana Komendanta, że wg ustaleń kontroli część osób będących w zespole reagowania na incydenty jest jednocześnie administratorami systemów teleinformatycznych[13], co oznacza, że sami nadzorują swoją działalność. Takie rozdzielenie obowiązków zaleca norma PN-IEC 27001:2014-12 w pkt. A.6.1.2 mówiąca, że obowiązki i odpowiedzialności pozostające ze sobą w konflikcie należy rozdzielić celem ograniczenia okazji do nadużyć.

(dowód: akta kontroli str. 107-120, 204-211)

---

[11] Centralna Baza Danych Straży Granicznej Systemu Wspomagania Kierowania.

[12] Kierownik jednostki zapewnia bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry wiadomy sposób, umożliwiający szybkie podjęcie działań korygujących.

Ocena badanego obszaru

NIK ocenia - w oparciu o stosowany w metodyce CobiT 4.1 Model dojrzałości - poziom zarządzania procesem bezpieczeństwa systemów teleinformatycznych w badanym obszarze jako „początkowy/doraźny", tj. KG SG dostrzega potrzebę zapewnienia bezpieczeństwa IT, jednakże jest ono zapewniane na doraźnych zasadach i nie podlega pomiarowi. Zdaniem NIK nie jest to wystarczający i akceptowalny poziom zarządzania bezpieczeństwem informacji w badanym obszarze. Na powyższą ocenę wpływ miało przede wszystkim niezapewnienie formalnych warunków do gromadzenia i analizy incydentów bezpieczeństwa jako istotnego elementu procesu zarządzania bezpieczeństwem informacji. Nie stworzono również metod pomiaru bezpieczeństwa, które wspomagałyby zarządzanie procesami związanymi z zapewnieniem bezpieczeństwa.

3. Stosowanie narzędzi zabezpieczeń oraz zarządzanie tożsamością

Zarządzanie kluczami kryptograficznymi

Ustalone nieprawidłowości

W procedurach wewnętrznych KGSG nie określono polityki używania zabezpieczeń kryptograficznych oraz zarządzania kluczami kryptograficznymi. W ocenie NIK nieopracowanie takiej polityki stanowiło działanie nierzetelne i pozbawia KG SG realnej możliwości oceny czy zakres stosowania mechanizmów kryptograficznych jest adekwatny do zagrożeń. Ponadto norma PN-ISO/IEC 27001:2014-12 w pkt. A.10.1.1 zaleca, aby opracować i wdrożyć politykę stosowania zabezpieczeń kryptograficznych do ochrony informacji.
Jak wyjaśniono techniki kryptograficzne wykorzystywane są w systemach IT służących do przetwarzania i przesyłania informacji niejawnych, a zasady korzystania z tych technik zostały określone w dokumentacjach tych systemów. Ponadto Komendant wyjaśnił, że informacje objęte klauzulą tajności „zastrzeżone", dane osobowe oraz informacje służbowe przesyłane są za pomocą środków ochrony kryptograficznej dopuszczonych do poziomu „zastrzeżone" w ramach sieci TOPAZ 2.

(dowód: akta kontroli str. 235)

Ochrona przed złośliwym oprogramowaniem, jego wykrywanie i wprowadzanie poprawek

Opis stanu faktycznego

W celu ujednolicenia i zabezpieczenia przed różnorodną konfiguracją stanowisk dostępowych zostały przygotowane obrazy systemów zarówno dla stanowisk stacjonarnych, jak i mobilnych. Na wszystkie stacje, są wgrywane z usługi katalogowej Active Directory polityki lokalne, które uniemożliwiają zwykłym użytkownikom domenowym, nie posiadającym uprawnień administracyjnych nadanych centralnie, modyfikację ustawień dot. zabezpieczeń w komputerze lokalnym. Dodatkowo użytkownicy przy dostępie do sieci Internet są dodatkowo chronieni z wykorzystaniem rozwiązania IronPort.
W związku z ograniczeniem możliwości dostępu do sieci Internet jedynie poprzez stanowiska komputerowe zarządzane przez domenę strazgraniczna.pl wyświetla się komunikat wpisany w rejestrze systemu operacyjnego, który jest widoczny przed logowaniem się użytkownika do systemu.
Styk z siecią Internet jest dodatkowo chroniony za pomocą IBM Proventia. Systemy IPS w urządzeniach sieciowych poprzez analizę ruchu sieciowego wykrywają i raportują aktywne sieciowo szkodliwe oprogramowanie.

(dowód: akta kontroli str. 37 – 45, 221 – 236, 391)

Konfiguracja sprzętu sieciowego podlega procesowi zarządzania konfiguracją w oparciu o elektroniczny rejestr zmian konfiguracji. Elementy niejawnych sieci funkcjonujących w SG i nadzorowanych przez KGSG objęte są zarządzaniem konfiguracją zgodnie z zasadami określonymi w dokumentacjach bezpieczeństwa sieci niejawnych.

(dowód: akta kontroli str. 232)

Bezpieczeństwo sieciowe

Fizyczny dostęp do systemów sieciowych jest możliwy tylko dla uprawnionych osób i w przypadku centralnych systemów oparty o dwustopniowe uwierzytelnienie (karta dostępu, sprawdzanie tęczówki oka).

Konfiguracja sprzętu sieciowego podlega procesowi zarządzania konfiguracją w oparciu o elektroniczny rejestr zmian konfiguracji.

Bezpieczeństwo dla systemów mobilnych realizowane jest przez implementowanie polityk związanych z szyfrowaniem nośników danych, zmiany haseł dostępowych i ograniczeń w systemie operacyjnym zredukowanych do poziomu użytkownika standardowego.

(dowód: akta kontroli str. 231-233)

Zarządzanie tożsamością

W zakresach obowiązków funkcjonariuszy i pracowników, mających styczność z bezpieczeństwem informacji, określono zasady odpowiedzialności za bezpieczeństwo informacji oraz zobowiązano do przestrzegania tajemnicy służbowej oraz ochrony danych osobowych i informacji niejawnych.

W umowach z kontrahentami znajdują się zapisy zobowiązujące ich do zachowania w tajemnicy wszystkich informacji i danych, w których posiadanie wejdą w trakcie wykonywania umowy, przestrzeganie zasad ochrony informacji niejawnych. W umowach związanych z przetwarzaniem informacji niejawnych oraz danych osobowych instrukcje bezpieczeństwa przemysłowego stanowią załączniki do tych umów.

(dowód: akta kontroli str. 391, 333 – 352)

Uprawnienia dostępu do zbiorów informacji nadawane są funkcjonariuszom Straży Granicznej lub pracownikom Straży Granicznej, na wniosek ich właściwych przełożonych, w zakresie niezbędnym do wykonywania przez nich pracy lub pełnienia służby na danym stanowisku, co wynikało z § 2 ust. 3 zarządzania Nr 1 Komendanta Głównego Straży Granicznej z dnia 2 stycznia 2015 r. w sprawie sposobu i trybu gromadzenia i przetwarzania informacji z zakresu ochrony granicy państwowej, kontroli ruchu granicznego oraz zapobiegania i przeciwdziałania nielegalnej migracji.

W przypadkach zmiany obowiązków użytkowników lub zmian kadrowych administratorzy informowani są o zaistniałych sytuacjach oraz konieczności podejmowania działań z nich wynikających tj. nadanie uprawnień/ utworzenie konta użytkownika, zawieszenie/usunięcie konta użytkownika w systemie ewentualna modyfikacja uprawnień użytkownika. Działania takie realizowane są przede wszystkim na podstawie wniosków kierowników komórek organizacyjnych KGSG i jednostek organizacyjnych SG i mają charakter ciągły. W przypadku systemów zewnętrznych w których funkcjonariusze/pracownicy KGSG pełnią rolę użytkownika

informacje dotyczące kwestii nadania, wycofania lub modyfikacji uprawnień wraz z wymaganymi wnioskami wysyłane są do administratorów zarządzających użytkownikami danego systemu z podmiotów zewnętrznych, którzy na podstawie tych informacji dokonują zmian w systemach.

Zdarzenia systemowe nieposiadające krytycznego znaczenia dla funkcjonowania systemu są rejestrowane w bazie danych przedmiotowego systemu.

Dane związane z działaniami w aplikacji CBD SG SWK są przechowywane w bazie danych logów SWK i w chwili obecnej są przechowywane od początku rozpoczęcia użytkowania systemu czyli od 1 kwietnia 2012 roku. Informacje przechowuje się przez okres niezbędny do osiągnięcia celu przetwarzania, nie dłużej niż 10 lat, liczony od momentu dokonania wpisu informacji w zbiorze informacji, a w przypadku odnotowania wpisu informacji, który był modyfikowany, ostatniej modyfikacji dotyczącej tego wpisu, co wynikało z § 6 ust. 5 zarządzenia nr 1 Komendanta Głównego SG z dnia 2 stycznia 2015 r.

Zdarzenia związane z działaniem systemu operacyjnego, jeżeli nie są objęte mechanizmem ACS (np. na stacji klienckiej, na której uruchamiana jest aplikacja SWK), są nadpisywane po osiągnięciu rozmiaru 20 MB. Logi są przetrzymywane standardowo w strukturze plików systemu Windows.

W KGSG procedura nadawania uprawnień opiera się na wniosku skierowanym przez przełożonego osoby, która ma mieć dostęp, do Dyrektora BŁiI KGSG o przydzielenie usługi zdalnego dostępu wraz z uzasadnieniem oraz na wniosku o wygenerowanie certyfikatu. Przesłane wnioski weryfikowane są w Biurze Łączności i Informatyki KGSG, następnie inspektorzy punktu rejestracji PKI w KGSG generują dodatkowy certyfikat.

Obecnie w systemie CBD SG SWK (dostęp do aplikacji) założonych jest 13726 kont użytkowników.

Logowanie do aplikacji CBD SG SWK przebiega dwuetapowo – w pierwszej kolejności użytkownik musi dokonać autoryzacji na stacji lokalnej, która podłączona jest do usługi katalogowej – w przypadku logowania za pomocą karty konieczne jest podanie PIN. Możliwe jest również zalogowanie się do systemu operacyjnego z wykorzystaniem loginu i hasła. Na poziomie usługi katalogowej wdrożona jest polityka złożoności haseł, która wymusza również okresową zmianę hasła.

Autoryzacja użytkowników systemu CBD SG SWK w aplikacji następuje za pomocą certyfikatu przechowywanego na karcie PKI. W jednym z modułów SWK, w którym użytkownicy SWK sprawdzają swój grafik pracy przez przeglądarkę www, uruchomiony jest mechanizm Single Sign On – tzn. jednorazowego logowania.

(dowód: akta kontroli str. 192 – 198, 391, 387 – 390)

Zbiór procedur zarządzania kontami oraz powiązanymi uprawnieniami użytkowników systemu CBD SG SWK zawarty jest w poniższych dokumentach:

- Polityka Bezpieczeństwa Centralnej Bazy Danych Straży Granicznej System Wspomagania Kierowania,
- Instrukcja Zarządzania Systemem Informatycznym Centralnej Bazy Danych Straży Granicznej System Wspomagania Kierowania,
- Załącznik do Instrukcji Zarządzania Systemem Informatycznym Centralnej Bazy Danych Straży Granicznej System Wspomagania Kierowania.

W dokumentach tych określono między innymi:

- procedury nadawania uprawnień rejestrowania uprawnień w systemie oraz osoby odpowiedzialne za te czynności,
- stosowane metody i środki uwierzytelniania w systemie oraz procedury związane z ich zarządzaniem i użytkowaniem,
- procedury rozpoczęcia, zawieszenia i zakończenia pracy dla użytkowników systemu,
- procedury zarządzania uprawnieniami użytkowników i administratorów,
- zarządzanie systemem,
- sposób, miejsce i okres przechowywania nośników elektronicznych zawierających informacje CBD SG SWK.

Ustalone nieprawidłowości

W procedurach nie określono obowiązku okresowych przeglądów nadanych uprawnień. Jak wyjaśnił Komendant Główny Straży Granicznej w piśmie z dnia 21 lipca 2015 r. przeglądy użytkowników systemów teleinformatycznych eksploatowanych w KGSG prowadzone są na bieżąco. Z przedłożonej dokumentacji nie wynika, żeby takie okresowe przeglądy obejmujące wszystkie systemy były prowadzone w SG[14]. Zdaniem NIK rzetelne zapobieganie nieuprawnionemu dostępowi wymaga wprowadzenia takiego obowiązku jak również wprowadzenia mechanizmu nadzoru nad jego wykonaniem. Ponadto pkt. A.9.2.5 Normy PN-ISO/IEC 27001:2014-12 zaleca, aby właściciele aktywów przeglądali prawa dostępu użytkowników w regularnych odstępach czasu.

(dowód: akta kontroli str. 192 – 198, 391)

Ocena badanego obszaru

W oparciu o stosowany w metodyce CobiT 4.1 Model dojrzałości, NIK ocenia poziom zarządzania procesem „zapewnienie bezpieczeństwa systemów informatycznych" w badanym obszarze jako „powtarzalne lecz intuicyjne". Zdaniem NIK stwierdzone nieprawidłowości wskazują na brak rzetelności przy zapewnieniu właściwego i skutecznego wykorzystania kryptografii do ochrony poufności, autentyczności i integralności informacji oraz nierzetelne zapobieganie nieuprawnionemu dostępowi do systemów i usług, co w sposób istotny obniża poziom bezpieczeństwa informacji w SG. Dodatkowo na ocenę w tym obszarze, zgodnie z zastosowaną metodyką CobiT 4.1., wpływ miały oceny działalności KGSG w obszarach przedstawionych w pkt. 1 i 2 niniejszego wystąpienia. NIK dostrzega wdrażanie i stosowanie zaawansowanych technik zabezpieczeń w SG jednakże, brak ustanowionych formalnych podstaw systemu bezpieczeństwa[15], zdaniem NIK uniemożliwia stwierdzenie adekwatności zastosowanych rozwiązań oraz ocenę ich wpływu na poziom bezpieczeństwa.

IV. Uwagi i wnioski

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

1. Opracowanie i wdrożenie, zgodnego z powszechnie przyjętymi standardami,

[14] Wg ustaleń kontroli realizowano obowiązkowe cykliczne przeglądy systemów przetwarzających informacje niejawne.
[15] W szczególności brak formalnych podstaw szacowania i postępowania z ryzykiem jak również brak podstawowych dokumentów SZBI – Polityka bezpieczeństwa, procedura postępowania z incydentami.
[16] Dz. U. z 2015 r., poz. 1096.

Systemu Zarządzania Bezpieczeństwem Informacji uwzględniającego wprowadzenie mierników procesu zarządzania bezpieczeństwem.
2. Opracowanie i wdrożenie procesu szacowania ryzyka w bezpieczeństwie informacji oraz procesu postępowania z tym ryzykiem.

V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK, przysługuje Panu Komendantowi 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, 28 grudnia 2015 r.

Prezes
Najwyższej Izby Kontroli
Krzysztof Kwiatkowski

WICEPREZES
Najwyższej Izby Kontroli

z up. .....

Wojciech Kutyła