WICEPREZES
NAJWYŻSZEJ IZBY KONTROLI
Wojciech Kutyła

KPB – 4101-002-07/2014
P/14/043

WYSTĄPIENIE POKONTROLNE

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli	P/14/043 – Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Departament Porządku i Bezpieczeństwa Wewnętrznego
Kontroler	Mirosław Kuśmierczak, główny specjalista k.p., upoważnienie do kontroli nr 89661 z dnia 30 maja 2014 r. (dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Komenda Główna Policji (zwana dalej KGP), 02-624 Warszawa, ul. Puławska 148/150
Kierownik jednostki kontrolowanej	Generalny Inspektor dr Marek Działoszyński Komendant Główny Policji (dowód: akta kontroli str.3)

II. Ocena kontrolowanej działalności

Ocena ogólna

Kontrola wykazała[1], że Komendant Główny Policji podejmował działania[2] mające na celu ustanowienie systemu realizacji zadań jednostek organizacyjnych Policji w zakresie ochrony cyberprzestrzeni RP. Wyodrębniono i rozwijano struktury organizacyjne dedykowane do zwalczania przestępczości komputerowej oraz odpowiadające za bezpieczeństwo sieci i systemów teleinformatycznych Policji. Komendant Główny Policji występował z inicjatywą zmian legislacyjnych, mających na celu usprawnienie działania organów ścigania wobec sprawców przestępstw komputerowych oraz podejmował czynności mające na celu oszacowanie ryzyk dla policyjnych systemów teleinformatycznych. Przeprowadzono także szereg działań informacyjno-edukacyjnych dotyczących zagrożeń w sieci oraz bezpiecznego korzystania z Internetu.

Ustalono natomiast, że nie został wdrożony kompleksowy system reagowania na zagrożenia i incydenty występujące w cyberprzestrzeni, obejmujący zadania z zakresu ujawniania, przeciwdziałania, analizowania i monitorowania sposobu rozpatrywania incydentów teleinformatycznych. W przypadku zdarzeń dotyczących jawnych systemów i sieci teleinformatycznych, Biuro Łączności i Informatyki KGP ograniczało się jedynie do zbierania danych i przekazywania informacji do właściwych jednostek i komórek organizacyjnych Policji, bez podejmowania dalszych działań wyjaśniających i monitorujących sposób załatwienia danego incydentu. Komendant Główny Policji nie zorganizował w KGP wewnętrznego zespołu reagowania na incydenty komputerowe (CERT), a także nie wyegzekwował przestrzegania, zatwierdzonej przez Dyrektora Biura Łączności i Informatyki KGP, procedury dotyczącej raportowania i ewidencjonowania incydentów występujących w jawnych systemach teleinformatycznych Policji. Stwierdzono także opóźnienia[3]

---

1 Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna. Jeżeli sformułowanie oceny ogólnej według proponowanej skali byłoby nadmiernie utrudnione, albo taka ocena nie dawałaby prawdziwego obrazu funkcjonowania kontrolowanej jednostki w zakresie objętym kontrolą, stosuje się ocenę opisową, bądź uzupełnia ocenę ogólną o dodatkowe objaśnienie.

2 Kontrolą objęto okres od początku 2008 r. do dnia zakończenia czynności kontrolnych, tj. do dnia 29 sierpnia 2014 r.

3 Analiza dotycząca szacowania ryzyka dla policyjnych systemów teleinformatycznych została sporządzona i przekazana do Ministerstwa Administracji i Cyfryzacji z opóźnieniem wynoszącym 4 miesiące.

oraz brak realizacji części zadań wynikających z *Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*[4] (zwanej dalej *Polityką*).

III. Opis ustalonego stanu faktycznego

1.System działań KGP w obszarze ochrony cyberprzestrzeni RP.

1.1. Określenie ram prawnych systemu ochrony cyberprzestrzeni RP.

Opis stanu faktycznego

W ocenie Komendanta Głównego Policji priorytetowymi kierunkami działań legislacyjnych umożliwiającymi realizację zadań w zakresie ochrony cyberprzestrzeni RP oraz skuteczne ściganie sprawców przestępstw popełnianych w sieci Internet są w szczególności:

1. Zmiany legislacyjne w zakresie ujednolicenia przepisów prawa dla przedsiębiorców telekomunikacyjnych i podmiotów świadczących usługi drogą elektroniczną. Proponowane zmiany dotyczą nałożenia na przedsiębiorców świadczących usługi drogą elektroniczną[5] obowiązku zatrzymywania i przechowywania danych o nawiązanych połączeniach (ustanowienia okresu retencji danych).
2. Działania mające na celu uregulowanie obszarów zapewniających przestępcom anonimowość w sieci. Postulowane zmiany dotyczą m.in. wprowadzenia do Prawa telekomunikacyjnego[6] obowiązku rejestracji usług pre-paid oraz wyłączenia (poprzez uregulowania międzynarodowe) możliwości stosowania narzędzi anonimizujących w sieci Internet.
3. Wypracowanie krajowego dokumentu, stanowiącego podstawę ochrony cyberprzestrzeni RP, w kontekście zagrożeń militarnych i pozamilitarnych.

(dowód: akta kontroli: str. 12-15,18-19)

W dniu 15 kwietnia 2009 r. Komendant Główny Policji wystąpił do Ministra Spraw Wewnętrznych i Administracji z prośbą o rozpoczęcie procesu legislacyjnego w zakresie zmiany ustawy o świadczeniu usług drogą elektroniczną polegającej m.in. na zobowiązaniu przedsiębiorców świadczących usługi drogą elektroniczną do zatrzymywania i przechowywania danych o nawiązanych połączeniach, w tym bezpłatnego udostępniania tych danych Policji. Pomimo wielokrotnych monitów przekazywanych w ww. sprawie do MSWiA (MSW) i UKE, do dnia zakończenia kontroli proponowane przez Komendanta Głównego Policji zmiany ww. ustawy nie zostały uwzględnione w procesie legislacyjnym.

(dowód: akta kontroli str. 15-16, 18-19, 432-488)

1.2. Przypisanie zasobów do realizacji zadań związanych z ochroną cyberprzestrzeni RP.

Oszacowanie zasobów Policji niezbędnych do realizacji zadań związanych z ochroną cyberprzestrzeni RP zostało dokonane m.in. w oparciu o dane statystyczne za lata 2008-2014 r. dotyczące liczby przestępstw komputerowych, których zwalczanie należy do zadań Policji. W ocenie Kierownictwa KGP w najbliższych latach należy przewidywać dalszy wzrost liczby przestępstw popełnianych z wykorzystaniem zaawansowanych technologii informatycznych.

(dowód: akta kontroli str. 8-9, 314-321, 568-570)

---

4 Przyjętej uchwałą Rady Ministrów nr 111/2013 z dnia 25 czerwca 2013 r.

5 Wymienionych w art. 2 pkt. 6 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r., poz. 1422.).

6 Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2014 r., poz. 243).

W ramach zasobów Policji dedykowanych do realizacji zadań związanych z ochroną cyberprzestrzeni RP można wyodrębnić trzy piony organizacyjne, tj.:

1. Pion kryminalny, w którego skład wchodzą Biuro Służby Kryminalnej KGP oraz komórki organizacyjne i funkcjonariusze wskazani w poszczególnych komendach wojewódzkich Policji odpowiadający za realizację zadań związanych ze zwalczeniem przestępczości komputerowej.
2. Pion informatyczny, tj. Biuro Łączności i Informatyki KGP realizujące zadania związane z ochroną jawnych systemów teleinformatycznych wykorzystywanych przez jednostki organizacyjne Policji oraz funkcjonariusze i pracownicy realizujący te zadania w terenowych jednostkach organizacyjnych Policji.
3. Gabinet Komendanta Głównego Policji realizujący zadania związane z bezpieczeństwem systemów teleinformatycznych Policji wykorzystywanych do przetwarzania informacji niejawnych i danych osobowych.

Ad. 1 W ramach Biura Służby Kryminalnej KGP[7] (BSK KGP) wyodrębniony został Wydział Wsparcia Zwalczania Cyberprzestępczości[8] (liczący 25 funkcjonariuszy), do którego zadań należało w szczególności:

- rozpoznawanie i monitorowanie obszarów zagrożonych cyberprzestępczością;
- współdziałanie z administratorami i właścicielami sieci komputerowych, przedsiębiorcami telekomunikacyjnymi oraz podmiotami świadczącymi usługi drogą elektroniczną, w ramach czynności operacyjno-rozpoznawczych;
- identyfikowanie dla krajowych i zagranicznych organów ścigania, sprawców przestępstw o znacznym stopniu skomplikowania, popełnianych z wykorzystaniem technologii informatycznych;
- inicjowanie wdrażania narzędzi informatycznych służących zwalczaniu cyberprzestępczości;
- usprawnianie systemu wymiany informacji o ustaleniach związanych z cyberprzestępczością.

Równolegle we wszystkich komendach wojewódzkich oraz w Komendzie Stołecznej Policji (KSP) wyznaczono kilkuosobowe (od 2 do 12 funkcjonariuszy) zespoły lub sekcje zaangażowane w zwalczanie przestępczości komputerowej. Ww. zespoły były umiejscowione w ramach różnych wydziałów komend wojewódzkich zajmujących się w szczególności przestępczością gospodarczą i wywiadem kryminalnym. W 4 komendach wojewódzkich, na podstawie *Koncepcji organizacji zwalczania cyberprzestępczości, program pilotażowy*[9] powołane zostały pilotażowe Zespoły Wsparcia Zwalczania Cyberprzestępczości.

Łączna liczba funkcjonariuszy Policji zajmujących się zwalczaniem przestępczości komputerowej wg stanu na dzień 6 czerwca 2014 r. wyniosła 145 osób (z tego 25 w KGP oraz 120 w komendach wojewódzkich i w KSP).

Koszty związane z wyposażeniem Wydziału Wsparcia Zwalczania Cyberprzestępczości BSK KGP w latach 2012-2014 wyniosły ok. 167,9 tys. zł i dotyczyły zakupu stanowisk komputerowych oraz specjalistycznego oprogramowania do informatyki śledczej. Na wyposażenie zespołów pilotażowych w 4 komendach wojewódzkich Policji wydatkowano łączne ok. 717 tys. zł.

(dowód: akta kontroli str. 9-12, 24-25, 44, 128-203, 260-313, 322-390, 571-580)

---

7 Biuro Służby Kryminalnej KGP zostało powołane na podstawie zarządzenia Nr 8 Komendanta Głównego Policji z dnia 15 marca 2013 r. w sprawie regulaminu Komendy Głównej Policji (Dz. Urz. KGP z 2013 r., poz. 25.) Poprzednio, w okresie objętym kontrolą, zadania ww. komórki organizacyjnej KGP w zakresie zwalczania cyberprzestępczości realizowało Biuro Kryminalne KGP.

8 Ww. Wydział funkcjonował od maja 2010 r. Wcześniej, w okresie objętym kontrolą, wyodrębniona była Sekcja Wsparcia Zwalczania Cyberprzestępczości w Wydziale Zaawansowanych Technologii Biura Kryminalnego KGP.

9 Dokument z dnia 13 grudnia 2012 r., zatwierdzony przez Zastępcę Komendanta Głównego Policji.

W trakcie kontroli, w KGP prowadzone były prace mające na celu usprawnienie realizacji zadań Policji związanych ze zwalczaniem przestępczości komputerowej. Od dnia 15 lipca 2014 r.[10], na bazie dotychczasowego Wydziału Wsparcia Zwalczania Cyberprzestępczości BSK KGP utworzony został Wydział do Walki z Cyberprzestępczością, w strukturze którego wyodrębniono zespoły: operacyjny, wsparcia technicznego i ustaleniowy. Jak wyjaśnił Komendant Główny Policji, zadania nowego Wydziału zmierzają do bardziej ofensywnych działań oraz podejmowania współpracy z podmiotami sektora publicznego i prywatnego, w tym ustalania kanałów oraz sposobu gromadzenia i wymiany informacji o przestępstwach.

W czwartym kwartale 2014 r., w komendach wojewódzkich i w KSP planowane jest także powołanie struktur organizacyjnych do walki z cyberprzestępczością, wobec których Wydział do Walki z Cyberprzestępczością BSK KGP będzie realizował m.in. zadania w zakresie koordynacji działań[11].

W KGP dokonano wstępnego oszacowania wydatków związanych z realizacją zadań Policji dotyczących zwalczania przestępczości komputerowej. W ocenie BSK KGP ww. wydatki powinny wynieść 2 213,7 tys. zł i zostać przeznaczone przede wszystkim na zakup odpowiednich urządzeń, sprzętu komputerowego i oprogramowania.

(dowód: akta kontroli str. 583-584, 633-634, 1109, 1232-1246,1423)

Ad. 2 W ramach Biura Łączności i Informatyki Policji KGP (BŁiI KGP) wyodrębniono Wydział Ochrony Systemów Informatycznych[12], do którego zadań należy w szczególności:

- planowanie, wdrażanie, nadzorowanie i koordynowanie rozwiązań bezpieczeństwa systemów i sieci teleinformatycznych w komórkach organizacyjnych KGP oraz określanie zaleceń standaryzacyjnych w tym zakresie dla jednostek terenowych Policji;
- tworzenie, uzgadnianie, wdrażanie oraz modyfikowanie dokumentacji bezpieczeństwa systemów teleinformatycznych organizowanych, wdrażanych i eksploatowanych w Biurze, we współpracy z właściwymi komórkami organizacyjnymi KGP oraz jednostkami terenowymi Policji;
- zapewnienie zgodności systemu zarządzania bezpieczeństwem systemów teleinformatycznych, eksploatowanych w biurze z normą PN-ISO/IEC 27001:2007, w tym okresowe szacowanie ryzyka na podstawie przyjętych kryteriów.

Ww. zadania, wg stanu na dzień 6 sierpnia 2014 r., realizowało 11 funkcjonariuszy oraz 15 pracowników cywilnych Wydziału Ochrony Systemów Informatycznych BŁiI KGP. W pozostałych jednostkach organizacyjnych Policji, analogiczne zadania realizowało 83 funkcjonariuszy i pracowników Policji.

W latach 2012-2014[13], wydatki związane z realizacją zadań komórki organizacyjnej BŁiI KGP odpowiadającej za ochronę sieci i systemów teleinformatycznych wyniosły łącznie 24 480,5 tys. zł i były przeznaczone na zakupy usług, naprawy środków trwałych i materiałów.

(dowód: akta kontroli str. 820-841,1124-1125, 1146-1231, 1302, 1315)

---

10 Na podstawie Decyzji Dyrektora BSK KGP z dnia 29 lipca 2014 r. w sprawie szczegółowej struktury organizacyjnej i schematu organizacyjnego Biura Służby Kryminalnej KGP, podziału zadań między dyrektorem a jego zastępcami oraz katalogu zadań komórek organizacyjnych.

11 Polecenie Zastępcy Komendanta Głównego Policji.

12 Wydział Ochrony Systemów Informatycznych został powołany na podstawie Decyzji nr 81 Dyrektora BŁiI KGP z dnia 10 maja 2013 r. w sprawie szczegółowej struktury organizacyjnej i schematu organizacyjnego BŁiI KGP, podziału zadań między dyrektorem a jego zastępcami oraz katalogu zadań komórek organizacyjnych. Poprzednio, w okresie objętym kontrolą, ww. zadania były realizowane przez Wydział Bezpieczeństwa Systemów Teleinformatycznych BŁiI KGP.

13 Wg stanu na dzień 31 lipca 2014 r.

Ad. 3 Od dnia 17 kwietnia 2013 r. zadania związane z bezpieczeństwem systemów teleinformatycznych Policji wykorzystywanych do przetwarzania informacji niejawnych i danych osobowych realizuje Wydział Bezpieczeństwa Teleinformatycznego[14] usytuowany w Gabinecie Komendanta Głównego Policji[15]. Zadania ww. Wydziału obejmują w szczególności:

- realizację obowiązków przewidzianych dla inspektora bezpieczeństwa teleinformatycznego, o których mowa w przepisach o ochronie informacji niejawnych oraz administratora bezpieczeństwa informacji, o których mowa w przepisach o ochronie danych osobowych;
- koordynowanie opracowywania szczególnych wymagań bezpieczeństwa dla systemów teleinformatycznych Policji przetwarzających informacje niejawne;
- koordynowanie wdrażania rozwiązań ochrony informacji niejawnych w systemach i sieciach teleinformatycznych, monitorowanie niejawnych systemów teleinformatycznych oraz konsultowanie rozwiązań bezpieczeństwa w tym zakresie.

Zadania dotyczące bezpieczeństwa teleinformatycznego w Wydziale Bezpieczeństwa Teleinformatycznego Gabinetu Komendanta Głównego Policji realizowało 6 osób.
(dowód: akta kontroli str. 36-37, 86, 128-203, 261-282,1060-1095, 1103, 1108-1123)

Do dnia zakończenia kontroli Komendant Główny Policji nie zrealizował obowiązku wymienionego w pkt 5. Polityki dotyczącego przekazania Ministrowi Administracji i Cyfryzacji (po zatwierdzeniu tego dokumentu) informacji na temat wykonanych dotychczas zadań związanych z ochroną cyberprzestrzeni oraz wydatków poniesionych na ich realizację. Nie przekazywano również ww. podmiotowi informacji na temat wydatków planowanych do poniesienia w latach kolejnych.

Komendant Główny Policji wyjaśnił, że powodem nieopracowania i nieprzekazywania ww. informacji Ministrowi Administracji i Cyfryzacji był brak zainteresowania ze strony Ministerstwa Administracji i Cyfryzacji (MAiC). Zdaniem Komendanta Głównego Policji, Policja nie była zobowiązana do przekazywania tego typu informacji do MAiC.

(dowód: akta kontroli str. 1320)

1.3 Opracowanie mierników oraz projektów szczegółowych określających sposób realizacji zadań w ramach ochrony cyberprzestrzeni RP.

Biuro Służby Kryminalnej KGP w latach 2012-2013 przekazywało do MAiC informacje, publikowane w biuletynach Ministerstwa zawierające m.in. dane statystyczne dotyczące przestępstw komputerowych oraz nowych zagrożeń bezpieczeństwa cyberprzestrzeni.

Komendant Główny Policji nie zrealizował natomiast zadania określonego w pkt 6. *Polityki* dotyczącego przekazania Ministrowi Administracji i Cyfryzacji, w ciągu roku od przyjęcia *Polityki*, informacji o przyjętych i osiągniętych przez Policję procentowych wskaźnikach realizacji zadań wynikających z wdrażania tego dokumentu.
Komendant Główny Policji wyjaśnił, że powodem nieopracowania i nieprzekazania do MAiC informacji na temat przyjętych i osiągniętych wskaźników realizacji zadań związanych z ochroną cyberprzestrzeni był fakt, że MAiC nie wzywało KGP do przekazania tego typu informacji.

(dowód: akta kontroli str. 545, 583, 585-612, 1104,1295, 1320)

---

[14] Poprzednio, w okresie objętym kontrolą, Sekcja Bezpieczeństwa Teleinformatycznego i Ochrony Danych Osobowych.

[15] Poprzednio, w okresie objętym kontrolą, komórka organizacyjna odpowiadająca za bezpieczeństwo systemów wykorzystywanych do przetwarzania informacji niejawnych i danych osobowych była usytuowana w Biurze Ochrony Informacji Niejawnych KGP.

W dniu 28 sierpnia 2014 r. Komendant Główny Policji, w związku z pismem Ministra Administracji i Cyfryzacji z dnia 13 sierpnia 2014 r., przedstawił propozycje wkładu Policji do *Planu działań w zakresie zapewnienia bezpieczeństwa w cyberprzestrzeni* oraz wskazał p.o. obowiązki Zastępcy Naczelnika Wydziału Ochrony Systemów Informatycznych BŁiI KGP, jako osobę upoważnioną do bieżących kontaktów. Proponowane na lata 2014-2016 działania Policji w zakresie ochrony cyberprzestrzeni obejmowały:

- modernizację Centralnego Węzła Internetowego KGP (CWI) – przebudowa i integracja systemu CWI i RBD (Redundantna Brama Dostępowa) w zakresie podniesienia bezpieczeństwa, wydajności i niezawodności realizowanych usług – koszt ok. 3 500 tys. zł;
- zakup, instalację i uruchomienie urządzenia chroniącego przed atakami DDoS i DoS dla CWI – koszt ok. 600 tys. zł;
- migrację lokalnych węzłów internetowych komend wojewódzkich Policji do CWI;
- konsolidację infrastruktury sieci intranetowych LAN jednostek terenowych Policji z wykorzystaniem OST112.

(dowód: akta kontroli str. 1405-1415)

W okresie objętym kontrolą KGP nie opracowała i nie uczestniczyła w opracowaniu projektów szczegółowych dotyczących celów i założeń *Polityki*.

Z udzielonych wyjaśnień wynika, że przedstawiciele Komendanta Głównego Policji nie uczestniczyli w pracach zespołu tworzącego projekt *Polityki* i brali udział tylko w uzgodnieniach międzyresortowych tego dokumentu. W latach 2008 – 2011 funkcjonariusze ówczesnego Biura Kryminalnego KGP uczestniczyli również w uzgodnieniach tworzonego w ABW projektu *Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2011-2020.* Propozycje zmian zgłaszanych przez Policję dotyczyły ujednolicenia wykonywania obowiązków na rzecz obronności przez podmioty świadczące usługi drogą elektroniczną, włączenia podmiotów świadczących usługi drogą elektroniczną do reagowania na incydenty oraz zmian legislacyjnych w ustawie o świadczeniu usług drogą elektroniczną.
Policja uczestniczyła także w spotkaniach dotyczących cyberbezpieczeństwa, odbywających się w formule strategicznych Forów Bezpieczeństwa, organizowanych przez Biuro Bezpieczeństwa Narodowego.

(dowód: akta kontroli str. 6,16, 586-588,591-594)

1.4. Ustanowienie kanałów wymiany informacji oraz krajowego systemu reagowania na incydenty komputerowe.

Klasyfikacja i sposoby identyfikacji incydentów, przestępstw komputerowych oraz procedury reagowania.

W zakresie ścigania przestępstw komputerowych Policja realizuje zadania zgodnie z przepisami ustawy o Policji[16], Kodeksu Karnego[17] (kk), Kodeksu Postępowania Karnego[18] (kpk), związane z przeciwdziałaniem, zapobieganiem oraz wykrywaniem sprawców następujących przestępstw:

- art. 190a §2 kk - podszywanie się pod inną osobę, fałszywe profile,
- art. 202 kk - dot. treści pedofilskich,
- art. 256 kk - ekstremizm polityczny – treści faszystowskie,
- art. 267 § 1 kk - nieuprawnione uzyskiwanie informacji (hacking),
- art. 267 § 2 kk - podsłuch komputerowy (sniffing),
- art. 268 § 2 kk - udaremnienie uzyskania informacji,
- art. 268a kk - udaremnienie dostępu do danych informatycznych,

---

16 Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2011 r., Nr 287, poz. 1687 ze zm.).
17 Dz. U. z 1997 r., Nr 88, poz. 553 ze zm.
18 Dz. U. z 1997 r. Nr 89, poz. 555 ze zm.

- art. 269 § 1 i 2 kk - sabotaż komputerowy,
- art. 269a kk - rozpowszechnianie złośliwych programów oraz cracking,
- art. 269b kk - narzędzia hackerskie,
- art. 271 kk - handel fikcyjnymi kosztami,
- art. 286 kk - oszustwo popełniane za pośrednictwem Internetu,
- *art. 287 kk* - oszustwo komputerowe (phishing).

Procedury reagowania na przestępstwa opierają się na przepisach regulujących czynności operacyjno-rozpoznawcze oraz postępowanie przygotowawcze.

Informacje o przestępstwie Policja uzyskuje w drodze: oficjalnych zawiadomień (obywateli, instytucji), informacji operacyjnych, czynności dochodzeniowo-śledczych, informacji anonimowych, informacji ze środków masowego przekazu oraz w drodze własnych ustaleń i spostrzeżeń.

Z danych Policji (Krajowy System Informacyjny Policji) wynika, że: w 2012 r. odnotowano 17 380 przestępstw komputerowych, z czego wykryto 13 731 (wykrywalność 79%), w 2013 r. odnotowano 22 042 przestępstwa komputerowe, (wzrost o 26,8%), z czego wykryto 15 586 (wykrywalność 70,7%). W okresie od stycznia do maja 2014 r. odnotowano 9 809 przestępstw komputerowych, wykryto 7 414 (wykrywalność 75,58%).

(dowód: akta kontroli str. 391-431, 545-549, 552-567)

Współpraca w celu ujednolicenia klasyfikacji incydentów/przestępstw komputerowych i procedur reagowania.

Policja od 2006 r. uczestniczy w projekcie *Hotline*, podpisanym przez Naukową i Akademicką Sieć Komputerową (NASK) oraz Komisję Wspólnot Europejskich – Dyrektoriat Generalny ds. Społeczeństwa Informacyjnego w sprawie utworzenia w Polsce punktu kontaktowego do przyjmowania zgłoszeń szkodliwych treści występujących w Internecie. Zorganizowany przez NASK punkt kontaktowy *Dyżurnet.pl* nosi oficjalną nazwę NIFC[19] Hotline Polska. Współpraca narodowych zespołów Hotline następuje w ramach stowarzyszenia INHOPE (The Assotiation of Internet Hotline Providers), do którego należą różne zespoły Hotline. Zespół *Dyżurnet.pl* jest punktem kontaktowym działającym przy NASK, przyjmującym zgłoszenia dotyczące nielegalnych treści w Internecie. Zgłoszenia do Policji trafiają do Wydziału Wsparcia Zwalczania Cyberprzestępczości BSK KGP, gdzie są oceniane pod kątem wyczerpania znamion przestępstwa określonego w zgłoszeniu. W ramach przesyłanych informacji funkcjonuje osiem kategorii zgłaszanych incydentów: treści pornograficzne z udziałem małoletniego, pedofilska aktywność użytkownika, treści pornograficzne dostępne dla osób poniżej 15 roku życia, treści rasistowskie lub ksenofobiczne, zagrażające bezpieczeństwu publicznemu, inne nielegalne treści, promujące niebezpieczne zachowania oraz znęcanie się nad zwierzętami.

Policja współdziała ponadto z kilkudziesięcioma stowarzyszeniami, towarzystwami, firmami, przedsiębiorcami świadczącymi usługi drogą elektroniczną w zakresie ujawniania przestępstw komputerowych.

(dowód: akta kontroli str.349-350)

System wymiany informacji o incydentach/przestępstwach komputerowych.

W zakresie wymiany informacji o incydentach/przestępstwach komputerowych BSK KGP uczestniczyło w procesie uzgodnień *Polityki Ochrony Cyberprzestrzeni RP*, otrzymuje także informacje z systemu wczesnego ostrzegania o zagrożeniach w sieci Internet ARAKIS-GOV, którego głównym administratorem jest Agencja Bezpieczeństwa Wewnętrznego.

---

[19] National Initiative for Children.

Wydział Ochrony Systemów Informatycznych BŁiI KGP, realizuje zadania dotyczące zwalczania zagrożeń dla bezpieczeństwa sieci policyjnych poprzez Centralny Węzeł Internetowy (CWI), podłączony do systemu ARAKIS.GOV.PL. Jak wyjaśniono, w momencie otrzymania informacji z CERT.GOV.PL[20] o wykryciu zagrożenia dla CWI, BŁiI KGP przekazuje informację do właściwej komórki organizacyjnej KGP, celem podjęcia kroków zaradczych. Administratorzy CWI współpracują z CERT.GOV.PL poprzez wymianę informacji drogą mailową oraz telefoniczną. Zgłaszane z CERT.GOV.PL informacje dotyczą m.in.: ujawnionych adresów IP, które wykorzystywane są do działań przestępczych (adresy dopisywane są do listy blokowanych przez KGP adresów IP), ujawnionych połączeń do sieci BotNet z sieci LAN jednostek Policji (zgłoszenia przesyłane są do administratorów lokalnych celem podjęcia czynności, informacja o podjętych działaniach przesyłana jest do CERT.GOV.PL), możliwości przeprowadzenia ataku typu DDoS, DoS na serwisy lub usługi Policji pracujące w sieci Internet, innych działaniach naruszających lub mogących naruszyć komunikację elektroniczną sieci Internet, w zakresie infrastruktury Policji.
Jak wyjaśniono, przedmiotowe działania realizowane są w trybie roboczym, nie mają określonej procedury, która sformalizowałaby przyjęty sposób postępowania.

W Komendach Wojewódzkich Policji komórki odpowiedzialne za zwalczanie cyberprzestępczości funkcjonują w systemie wymiany informacji Policji, korzystając z policyjnej sieci telefonicznej i poczty elektronicznej LOTUS w oparciu o służbę dyżurną. W BSK funkcjonuje służba dyżurna Wydziału Wsparcia Zwalczania Cyberprzestępczości oraz na Stanowisku Koordynacji Obserwacji Krajowej Wydziału Techniki Operacyjnej.

(dowód: akta kontroli str. 550-551, 842-850)

Do chwili obecnej nie opracowano specyficznych procedur łączności pomiędzy Policją a ABW w zakresie bezpieczeństwa cyberprzestrzeni oraz zwalczania przestępczości komputerowej o charakterze kryminalnym. Współpraca opiera się na dotychczasowych, roboczych mechanizmach wymiany informacji. Dane o incydentach publikowane są w dziennym biuletynie informacyjnym CERT.GOV.PL i dotyczą m.in. zainfekowania komputerów oraz prób uzyskania danych z domen GOV.

(dowód: akta kontroli str. 549, 631-632)

Ustalone nieprawidłowości

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

Uwagi dotyczące badanej działalności

W okresie objętym kontrolą KGP nie zrealizowała obowiązków wymienionych w pkt 5. i 6. *Polityki* dotyczących przekazania Ministrowi Administracji i Cyfryzacji informacji na temat wydatków poniesionych i planowanych w związku z ochroną cyberprzestrzeni oraz przyjętych przez Policję w tym obszarze wskaźników realizacji zadań. Brak działań w ww. zakresie wyjaśniano nieotrzymaniem korespondencji z MAiC bezpośrednio wskazującej na obowiązek przekazania tego rodzaju informacji. NIK zwraca uwagę, że *Polityka* została przyjęta przez Radę Ministrów i w związku z tym jest dokumentem obowiązującym podmioty administracji rządowej. W przypadku wątpliwości, co do interpretacji jego zapisów oraz określonych w nim obowiązków, zasadne jest wystąpienie do Ministra Administracji i Cyfryzacji, który odpowiada za wdrażanie *Polityki,* o przedstawienie stosownych wytycznych dotyczących realizacji tego dokumentu.

Ocena cząstkowa

Kontrola wykazała, że Komendant Główny Policji podjął działania mające na celu ustanowienie systemu realizacji zadań jednostek organizacyjnych Policji w zakresie

[20] Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, działający w ramach Agencji Bezpieczeństwa Wewnętrznego.

ochrony cyberprzestrzeni RP. W szczególności wyodrębniono i rozwijano struktury organizacyjne dedykowane do zwalczania przestępczości komputerowej oraz odpowiadające za bezpieczeństwo systemów teleinformatycznych Policji. Komendant Główny Policji występował również z inicjatywą zmian legislacyjnych, mających na celu usprawnienie działania organów ścigania wobec sprawców przestępstw komputerowych. Nie zrealizowano natomiast zadań wymienionych w pkt 5. i 6. *Polityki* dotyczących przekazania Ministrowi Administracji i Cyfryzacji informacji na temat zadań wykonanych dotychczas w obszarze ochrony cyberprzestrzeni, wskaźników ich realizacji oraz poniesionych i planowanych wydatków.

2. Szacowanie ryzyk występujących w cyberprzestrzeni.

Opis stanu faktycznego

Wydział Ochrony Systemów Informatycznych BŁiI KGP w okresie objętym kontrolą dokonał oszacowania ryzyk, związanych z zagrożeniami dla środowiska przetwarzania danych administrowanego przez BŁiI KGP. Do szacowania ryzyka wykorzystano m.in. narzędzie udostępnione przez ABW[21]. Jak wyjaśniła Naczelnik Wydziału, narzędzie to bazuje na metodyce szacowania ryzyka MAGERIT wersja 2 i zgodnie z zaleceniami ABW może być wykorzystywane na potrzeby szacowania ryzyka dla dużych systemów teleinformatycznych. Ponadto w BŁiI KGP opracowano autorską metodę szacowania ryzyka oraz narzędzie i szablon „.xls." Szacowanie przeprowadzono na potrzeby systemu zarządzania bezpieczeństwem informacji, budowanego w oparciu o wymagania Polskiej Normy PN-SIO/IEC27001:2007.

W związku z pkt 3.1. *Polityki,* wyniki szacowania ryzyka przekazano Ministrowi Administracji i Cyfryzacji, natomiast ww. zadanie zostało zrealizowane dopiero w trakcie kontroli NIK, tj. z 4-miesięcznym opóźnieniem w stosunku do terminu określonego przez MAiC[22]. Komendant Główny Policji wyjaśnił, że powodem opóźnienia w przekazaniu wyników szacowania ryzyka było spiętrzenie zadań realizowanych przez Wydział Ochrony Systemów Informatycznych BŁiI KGP.

(dowód: akta kontroli str. 667,1316-1318,1321, 1329-1369

KGP dokonywała również analizy przykładowych ryzyk i zagrożeń dla systemów teleinformatycznych Policji w dokumentach sporządzanych na podstawie ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[23], tj.:

- w raportach cząstkowych Komendanta Głównego Policji o zagrożeniach bezpieczeństwa narodowego[24] zidentyfikowano zagrożenia w zakresie cyberterroru oraz zagrożenia dla systemów łączności. Wskazano przewidywane scenariusze przebiegu zagrożeń oraz cele strategiczne i programowanie zadań w zakresie poprawy bezpieczeństwa;
- w Planach Zarządzania Kryzysowego Komendanta Głównego Policji[25] wskazano m.in. potencjalne zagrożenia dla funkcjonowania systemów teleinformatycznych oraz zagrożenia związane z cyberterroryzmem. Ponadto przypisano komórkom organizacyjnym KGP zadania z zakresu monitorowania i zarządzania tymi zdarzeniami.

(dowód: akta kontroli str. 859,903-914, 915-916, 917-939, 940-949, 952-957, 959-993, 1026-1059, 1098-1101)

---

21 PILAR (4.1.2-14.3.2008).

22 Zgodnie z pkt 3.1. *Polityki* wyniki szacowania ryzyka powinny zostać przekazane ministrowi właściwemu ds. informatyzacji w terminie do 31 stycznia każdego roku. Zgodnie z terminem wyznaczonym przez MAiC szacowanie ryzyka za 2013 r. (pierwszy rok obowiązywania *Polityki*) miało być przeprowadzone do końca marca 2014 r.

23 Dz. U. z 2013 r., poz. 1166.

24 Raporty z 11 sierpnia 2010 r., 3 sierpnia 2012 r. oraz 29 lipca 2014 r.

25 Z 29 sierpnia 2011 r. oraz 30 października 2013 r.

Ustalone nieprawidłowości

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

Uwagi dotyczące badanej działalności

NIK zwraca jednak uwagę na znaczne opóźnienie w realizacji zadania wymienionego w pkt 3.1. *Polityki*, dotyczącego oszacowania ryzyka dla systemów teleinformatycznych KGP. Wyniki szacowania ryzyka zostały przekazane Ministrowi Administracji i Cyfryzacji dopiero w trakcie kontroli NIK, z 4 - miesięcznym opóźnieniem w stosunku do terminu określonego przez MAiC.

Ocena cząstkowa

Kontrola wykazała, że Komendant Główny Policji podejmował czynności mające na celu oszacowanie ryzyk i zagrożeń dla policyjnych systemów teleinformatycznych. Wyniki szacowania ryzyka zostały przedstawione m.in. w sprawozdaniu przekazanym do MAiC oraz w dokumentacji sporządzanej na podstawie ustawy o zarządzaniu kryzysowym.

3. Działania KGP w zakresie bezpieczeństwa systemów teleinformatycznych.

3.1.Ustanowienie i kontrola podstawowych wymogów w zakresie bezpieczeństwa cyberprzestrzeni.

Decyzją Nr 35 z dnia 25 lutego 2013 r. Dyrektora BŁiI KGP przyjęto dokument pt. *Polityka Systemu Bezpieczeństwa Informacji w Biurze Łączności i Informatyki* oraz *Deklarację stosowania dla Systemu Bezpieczeństwa Informacji.*
W ramach *Systemu Bezpieczeństwa Informacji* opracowano następujące polityki szczegółowe i procedury:

- *Polityka dostępu stron zewnętrznych do centrów przetwarzania danych BŁiI KGP;*
- *Polityka nadawania uprawnień do niestandardowych treści internetowych, usług, bądź zasobów;*
- *Zarządzanie zdarzeniami związanymi z bezpieczeństwem informacji;*
- *Zarządzanie zmianami typu aktualizacja oprogramowania, instalacja poprawek oprogramowania, aktualizacja certyfikatów w systemach teleinformatycznych i sieciach;*
- *Niszczenie nośników informacji, bezpieczne zbywanie lub przekazanie do ponownego użycia;*
- *Dostęp stron zewnętrznych do aktywów teleinformatycznych BŁiI KGP.*

Ponadto w BŁiI KGP opracowany został dokument pt. *Zalecenia dotyczące standardów technicznych, użytkowych oraz bezpieczeństwa, stosowanych w Policji, w zakresie informatyki i łączności*[26], który stanowi zbiór dobrych praktyk i standardów w zakresie bezpieczeństwa teleinformatycznego. Ww. dokument wprowadzono do stosowania we wszystkich jednostkach organizacyjnych Policji decyzją Zastępcy Komendanta Głównego Policji.

Wszystkie ww. dokumenty opracowane w BŁiI KGP udostępniono funkcjonariuszom i pracownikom Policji na portalu wewnętrznym Policji – Lotus Quickr.

(dowód: akta kontroli str. 667-819)

3.2. Organizacja ćwiczeń i testów systemu bezpieczeństwa cyberprzestrzeni.

W okresie objętym kontrolą BSK KGP uczestniczyło w ćwiczeniach CYBEREXE 2012[27] oraz CMX 2012[28]. Ćwiczenia miały na celu sprawdzenie reakcji na cyberatak.

(dowód: akta kontroli str. 585, 589-590, 630-631)

---

26 Ostatnia wersja dokumentu pochodzi z 10 grudnia 2013 r.
27 Ćwiczeniami dotyczące ochrony przed cyberatakiem na strategiczną infrastrukturę państwa.
28 Ćwiczenia NATO dot. m.in. reakcji na cyberataki.

3.3.Ustanowienie systemu reagowania na incydenty w cyberprzestrzeni.

W Komendzie Głównej Policji nie funkcjonuje sformalizowany wewnętrzny zespół reagowania na incydenty komputerowe (CERT). Zbliżone zadania przypisane są Wydziałowi Ochrony Systemów Informatycznych BŁiI KGP – nie podejmuje on jednak działań w zakresie analizy zagrożeń i rozpatrywania incydentów.

Komendant Główny Policji wyjaśnił, że powołanie zespołu CERT nie jest obligatoryjne, współpraca z CERT.GOV.PL przebiegała bardzo dobrze i nie zauważono potrzeby ustanawiania takiego Zespołu w KGP. Ponadto BŁiI KGP nie posiadało wystarczających zasobów kadrowych do realizacji zadań w zakresie analizy przyczyn występujących incydentów oraz wyjaśniania alarmów zgłaszanych przez CERT.GOV.PL. Zaznaczył jednocześnie, że *(...) Dyrektor BŁiI KGP rozważy możliwości organizacyjne i finansowe powołania takiego zespołu w przyszłości.*

(dowód: akta kontroli str. 16, 489-494, 585-586, 1106, 1312-1313)

Zgodnie z udzielonymi wyjaśnieniami, źródłami informacji, wykorzystywanymi przez Wydział Ochrony Systemów Informatycznych BŁiI KGP o zagrożeniach, podatnościach i incydentach, są raporty CERT.GOV.PL o stanie bezpieczeństwa cyberprzestrzeni RP, raporty komercyjnych dostawców rozwiązań w zakresie bezpieczeństwa IT[29] oraz opracowania organizacji stanowiących standardy w zakresie bezpieczeństwa teleinformatycznego[30]. Źródłem informacji o incydentach są raporty dyżurnych Sekcji ds. Obsługi Całodobowej Wydziału Utrzymania Systemów Teleinformatycznych BŁiI KGP, prowadzących całodobowe dyżury w Centrum Przetwarzania Danych, gdzie spływają informacje m.in. o ewentualnych tzw. *incydentach*, od użytkowników systemów administrowanych przez Biuro Łączności i Informatyki a także z Biura Służby Kryminalnej.

(dowód: akta kontroli str. 1293)

W BŁiI KGP prowadzony jest, w ramach przygotowywanego tzw. *Planu Ciągłości Działania*, załącznik zawierający aktualne dane teleadresowe administratorów krytycznych systemów teleinformatycznych, administrowanych przez BŁiI KGP. Danymi telefonicznymi umożliwiającymi kontakt z administratorami systemów teleinformatycznych dysponują również Dyżurni Sekcji ds. Całodobowego Wydziału Utrzymania Systemów Informatycznych BŁiI KGP.

(dowód: akta kontroli str. 1303)

W latach 2012-2014 Wydział Ochrony Systemów Informatycznych BŁiI KGP[31] otrzymał z Zespołu CERT.GOV.PL 1 807 informacji na temat zagrożeń i incydentów zidentyfikowanych w jawnych, policyjnych systemach teleinformatycznych. Na podstawie ww. danych BŁiI KGP przekazywało informacje o zagrożeniach do właściwych komórek organizacyjnych KGP oraz komend wojewódzkich i KSP. Nie były natomiast podejmowane żadne dalsze działania mające na celu badanie i wyjaśnianie zdarzeń. BŁiI KGP nie żądało także od jednostek organizacyjnych Policji, którym przekazano komunikaty o incydentach, informacji zwrotnych dotyczących podjętych przez nie działań. W związku z powyższym Wydział Ochrony Systemów Informatycznych BŁiI KGP nie dysponował faktyczną wiedzą na temat działań podjętych w związku z zagrożeniami i incydentami stwierdzonymi w jawnych, policyjnych sieciach i systemach teleinformatycznych.

Komendant Główny Policji wyjaśnił, że Stan kadrowy zespołu ds. Centralnego Węzła Internetowego (2 administratorów) nie pozwalał na rozszerzenie zadań

---

29 Microsoft, Symantec, TrendMicro, Cisco.

30 National Vulnerability Database, SANS Institute, ISACA, Bundesamt für Sicherheit in der Informationstechnik, Open Web Application Security Project, ISO.

31 Wcześniejszy Wydział Bezpieczeństwa Systemów Teleinformatycznych.

o działania analityczno-koordynacyjne w zakresie zaistniałych naruszeń bezpieczeństwa, dlatego też incydenty w jawnych systemach i sieciach nie były badane ani wyjaśniane.

(dowód: akta kontroli str. 1267, 1310-1311)

W dniu 28 listopada 2011 r. Dyrektor BŁiI KGP zatwierdził procedurę WBST – A.13.2 *Zarządzanie zdarzeniami związanymi z bezpieczeństwem informacji,* w ramach normy *System zarządzania bezpieczeństwem informacji PN-ISO/IEC 27007:2007* z mocą obowiązującą w BŁiI KGP od 1 grudnia 2011 r. Ww. procedura nakładała obowiązki dotyczące raportowania o zdarzeniach związanych z bezpieczeństwem informacji[32] w jawnych sieciach i systemach teleinformatycznych Policji oraz prowadzenia rejestru incydentów.

W wyniku przeprowadzonych oględzin ustalono, że w rejestrze incydentów dotyczących jawnych systemów teleinformatycznych Policji, który powinien być prowadzony w Wydziale Ochrony Systemów Informatycznych BŁiI KGP, nie zarejestrowano żadnych zdarzeń.

Naczelnik Wydziału Ochrony Systemów Informatycznych BŁiI KGP stwierdziła, że: *pomimo że procedura została przekazana naczelnikom wszystkich wydziałów utrzymaniowych wydaje się, że nie ma pełnej świadomości, co do roli tej procedury. (...)* Dyrektor BŁiI KGP potwierdził, że sposób wprowadzenia procedury okazał się nieskuteczny, w związku z czym przygotowywany jest projekt decyzji Dyrektora BŁiI KGP wprowadzający stosowanie ww. procedury. Stwierdził także konieczność jej rozszerzenia na pozostałe jednostki organizacyjne Policji. Poinformował, że rejestr incydentów teleinformatycznych jest uzupełniany na podstawie informacji zgromadzonych w odrębnych zasobach.

(dowód: akta kontroli str.1268-1271, 1295, 1301, 1305-1307, 1403, 1417-1418)

W latach 2010-2014 w systemach teleinformatycznych Policji wykorzystywanych do przetwarzania informacji niejawnych i danych osobowych stwierdzono łącznie 241 incydentów bezpieczeństwa IT[33]. Komendant Główny Policji pismem z dnia 18 kwietnia 2012 r. wprowadził do stosowania formularz zgłoszenia incydentów dla niejawnych systemów teleinformatycznych eksploatowanych w komórkach organizacyjnych KGP. Ponadto w Wydziale Bezpieczeństwa Teleinformatycznego Gabinetu Komendanta Głównego Policji, od dnia 8 maja 2014 r.[34] prowadzony jest elektroniczny Rejestr Naruszeń, obejmujący naruszenia przepisów dotyczących informacji niejawnych oraz ochrony danych osobowych, w tym dotyczące bezpieczeństwa teleinformatycznego.

(dowód: akta kontroli str. 1285-1289,1290-1293, 1299, 1308-1309, 1322, 1430-1431)

W Komendzie Głównej Policji nie został powołany pełnomocnik ds. bezpieczeństwa cyberprzestrzeni[35]. Komendant Główny Policji wyjaśnił, że regulacje prawne o których mowa w pkt 3.3 Polityki, dające podstawy do podejmowania dalszych działań w ramach wdrażania zapisów tego dokumentu nie zostały opracowane,

---

32 W załączniku do ww. procedury określono formularz raportowania o incydentach.

33 Jednym z incydentów było stwierdzone przez kontrolerów NIK, w trakcie kontroli P/13/100 *Działania Policji na rzecz bezpieczeństwa obywateli w ruchu drogowym*, przetwarzanie rzeczywistych danych osobowych w tzw. szkolnej wersji sytemu SEWIK. W zakresie wyjaśniania incydentu stwierdzono brak aktualizacji procedur w zakresie bezpieczeństwa danych osobowych. Przeprowadzono procedurę anonimizacji danych, przeprowadzono procedurę wyznaczenia administratora bezpieczeństwa informacji i upoważnienia do wykonywania zadań administratora danych osobowych w Biurze Prewencji i Ruchu Drogowego KGP.

34 Na podstawie decyzji nr 7 Pełnomocnika Komendanta Głównego Policji ds. Ochrony Informacji Niejawnych z dnia 8 maja 2014 r. w sprawie trybu prowadzenia działań zmierzających do wyjaśnienia okoliczności naruszenia w Komendzie Głównej Policji przepisów o ochronie informacji niejawnych.

35 Zasadność powołania w poszczególnych jednostkach administracji rządowej pełnomocnika ds. bezpieczeństwa cyberprzestrzeni została wskazana w pkt 3.4.3. *Polityki.*

w związku z czym podstawą działań KGP w tym zakresie jest pismo MAiC z 13 lutego br.[36] W trakcie kontroli przygotowano jednak projekt decyzji powołującej pełnomocnika ds. bezpieczeństwa cyberprzestrzeni, którym będzie p.o. zastępcy naczelnika Wydziału Ochrony Systemów Informatycznych BŁiI KGP. Projekt przesłano do Gabinetu Komendanta Głównego Policji celem nadania biegu legislacyjnego.

(dowód: akta kontroli str.1107, 1321-1322, 1324-1328)

3.4. System wczesnego ostrzegania.

KGP uczestniczy w projekcie ARAKIS. Sonda systemu ARAKIS została zainstalowana przez specjalistów ABW w infrastrukturze Centralnego Węzła Internetowego. W sieciach teleinformatycznych Policji funkcjonowały i funkcjonują ponadto sondy systemów wykrywania i zapobiegania włamaniom Intrusion Detection Systems/Intrusion Prevention Systems, które spełniają podobną rolę, jak sondy systemu ARAKIS, monitorują ruch sieciowy pod kątem anomalii i potencjalnych zagrożeń dla bezpieczeństwa systemów teleinformatycznych.

(dowód: akta kontroli str. 614-615, 1313)

3.5. Szkolenia i działania edukacyjne

Komendant Główny Policji stwierdził, że uwzględniając prognozowany wzrost przestępczości popełnianej z wykorzystaniem Internetu i zaawansowanych technologii, na chwilę obecną liczba funkcjonariuszy - specjalistów posiadających wystarczające kwalifikacje w obszarze zwalczania przestępczości komputerowej jest adekwatna. Jednak z uwagi na bardzo szerokie spektrum cyberprzestępczości, obejmującej znaczną ilość zagadnień przestępczości gospodarczej i kryminalnej, należy brać pod uwagę ryzyko, że liczba lub kwalifikacje tych osób okażą się niewystarczające. Wymagana wiedza i umiejętności bardzo wysoce specjalistyczne muszą być nabywane przez dłuższy okres czasu, w trakcie szkoleń i poprzez praktykę.

(dowód: akta kontroli str. 615, 632)

System wynagrodzeń Policjantów i pracowników cywilnych nie pozwala na pozyskanie i utrzymanie wystarczającej liczby odpowiednio wykwalifikowanych specjalistów w obszarze ochrony cyberprzestrzeni.
System wynagrodzeń policjantów i pracowników Policji nie przewiduje odrębnej siatki płac dla osób realizujących zadania związane z ochroną cyberprzestrzeni. Funkcjonariusze realizujący zadania w Wydziale Wsparcia Zwalczania Cyberprzestępczości BSK KGP, z uwagi na posiadanie specjalnych kwalifikacji mają najwyższe, dla stanowisk wykonawczych grupy zaszeregowania (eksperci i specjaliści), co zdaniem Komendanta Głównego Policji *(...) wydaje się najbardziej optymalna polityką finansową w środowisku policyjnym dla tego typu specjalności.*
Stosowane są również dodatkowe zachęty i formy wynagradzania, takie jak: nagrody, podwyżki dodatku służbowego na określony czas, krótkoterminowe urlopy dodatkowe, odznaki resortowe, przedterminowe mianowanie na wyższy stopień.
W ramach wyróżnienia funkcjonariusze BSK KGP zwalczający cyberprzestępczość biorą także udział w specjalistycznych szkoleniach i konferencjach, także poza granicami kraju.

(dowód: akta kontroli str. 632-633,1106)

Podstawą prawną systemu szkoleń funkcjonariuszy Policji realizujących zadania związane ze zwalczeniem nielegalnej działalności w sieci jest Decyzja nr 872

---

[36] Pismo z dnia 13 lutego 2014 r. Pana Romana Dmowskiego, Podsekretarza Stanu w Ministerstwie Administracji i Cyfryzacji (znak: DSI-WSE.550.1.2014.JŁ) dotyczące szacowania ryzyka oraz powołania w jednostkach administracji rządowej pełnomocników ds. bezpieczeństwa cyberprzestrzeni.

Komendanta Głównego Policji z dnia 5 grudnia 2007 r. *w sprawie programu kursu specjalistycznego w zakresie uzyskiwania informacji z Internetu dla policjantów zwalczających przestępczość komputerową*[37]. Program kursu został opracowany przez przedstawicieli Wyższej Szkoły Policji w Szczytnie, we współpracy z Centralnym Biurem Śledczym KGP oraz specjalistycznymi organizacjami pozapolicyjnymi[38]. Celem kursu jest poszerzenie wiedzy policjantów służby kryminalnej z zakresu przestępczości komputerowej i uzyskiwania informacji z Internetu, służące usprawnianiu prowadzenia postępowań przygotowawczych w sprawach o przestępstwa komputerowe.
W 2012 r. ze względu na organizację EURO 2012 nie organizowano szkoleń z zakresu przestępczości komputerowej, ponieważ priorytetem były podstawowe szkolenia zawodowe. W 2013 r. przeprowadzono 13 edycji ww. kursu, na których przeszkolono 151 funkcjonariuszy, a w 2014 r.[39] 12 edycji dla 143 funkcjonariuszy. Do końca 2014 r. planuje się przeprowadzenie 16 edycji kursu dla 191 słuchaczy.

(dowód: akta kontroli str. 615-616, 632-635)

Funkcjonariusze zajmujący się zwalczaniem cyberprzestępczości uczestniczą ponadto w specjalistycznych szkoleniach z dziedziny informatyki śledczej, organizowanych przez podmioty zewnętrzne. W 2013 r. 7 wyróżniających się funkcjonariuszy Wydziału Wsparcia Zwalczania Cyberprzestępczości BSK KGP oraz 4 z komend wojewódzkich uczestniczyło w organizowanym przez firmę ProCertiv szkoleniu na temat *Sztuka Hackingu – Atak i Obrona.* Ponadto 19 policjantów (w tym 3 z BSK KGP) w 2014 r. uczestniczyło w szkoleniu organizowanym przez FBI dot. oszustw dokonywanych poprzez sieć Internet.

(dowód: akta kontroli str. 632, 637-639, 640)

Wydział Bezpieczeństwa Systemów Teleinformatycznych BŁiI KGP, we Współpracy z Wydziałem Bezpieczeństwa Teleinformatycznego Gabinetu Komendanta Głównego Policji, przeprowadził w 2013 r. cykl szkoleń dla ok. 140 policjantów i pracowników KGP, w oparciu o program opracowany przez specjalistów BŁiI KGP. Szkolenia obejmowały podstawowe zasady bezpieczeństwa podczas pracy na stanowiskach komputerowych. Planowana jest realizacja tego typu szkoleń w kolejnych latach (po modyfikacji programu uwzględniającej nowe zagrożenia) dla wszystkich użytkowników systemów teleinformatycznych w KGP oraz udostępnienie programów szkoleń Komendom Wojewódzkim Policji.
Wydział Ochrony Systemów Informatycznych BŁiI KGP podjął współpracę z Wydziałem Zarządzania Politechniki Warszawskiej w ramach projektu rozwojowego nr OR00004011 dotyczącego optymalizacji organizacji zarządzania w Policji, m.in. w obszarze problematyki bezpieczeństwa informacji przetwarzanych w systemach informatycznych Policji. W ramach projektu zorganizowano szkolenia dla funkcjonariuszy i pracowników jednostek organizacyjnych Policji (KGP, KSP, KWP, szkół policyjnych), w 2011 r. dla 45 osób oraz w 2012 r. dla 49 osób, z zakresu zarządzania bezpieczeństwem informacji i audytowania systemu zarządzania bezpieczeństwem Informacji. Uczestnicy szkoleń, po zdaniu egzaminu, uzyskali zaświadczenia Polskiego Centrum Badań i Certyfikacji S.A. w zakresie audytora wewnętrznego systemu zarządzania bezpieczeństwem informacji zgodnie z normą PN-ISO/IEC 27001:2007 oraz audytora wewnętrznego systemu zarządzania ciągłością działania według normy ISO 22301:2012. BŁiI KGP rozważa także wykorzystanie platformy typu e-lerning dla celów prowadzenia kampanii informacyjno-edukacyjnej w zakresie bezpieczeństwa teleinformatycznego.

(dowód: akta kontroli str. 666)

---

37 Dz. Urz. KGP Nr 23, poz. 185 ze zm.
38 CERT Polska, Katedra Prawa Karnego UMK w Toruniu, QXL Poland – właściciel serwisu allegro.pl.
39 Wg stanu na dzień 8 lipca 2014 r.

Policja nie opracowywała centralnie i nie uczestniczyła w pracach nad założeniami kampanii informacyjno-edukacyjnej prowadzonej przez inne instytucje mającej na celu dotarcie do użytkowników z informacją o potencjalnych zagrożeniach pochodzących z cyberprzestrzeni i metodach zabezpieczenia się przed nimi. KGP rekomendowała komendom wojewódzkim (m.in. w ramach programu *Razem bezpieczniej*), wypracowanie działań profilaktycznych w partnerstwie międzyinstytucjonalnym, przy uwzględnieniu potrzeb lokalnych wynikających z analizy stanu zagrożenia, m.in. w zakresie bezpieczeństwa w sieci, cyberprzestępczości. W latach 2012-2014 Policja przeprowadziła szereg takich działań dla kilkuset tysięcy osób, w szczególności w formie prelekcji dla uczniów, rodziców i nauczycieli dotyczących zagrożeń w sieci, bezpiecznego korzystania z Internetu oraz odpowiedzialności za przestępstwa komputerowe.

Wyższa Szkoła Policji w Szczytnie, w zakresie problematyki ochrony cyberprzestrzeni, realizowała zadania w ramach działalności edukacyjnej, wydawniczej, naukowo-badawczej oraz udziału w pracach grup eksperckich, grup roboczych i w międzynarodowych konferencjach naukowych.

(dowód: akta kontroli str. 618-625, 634-636, 1247-1266)

Biuro Służby Kryminalnej KGP realizuje działania profilaktyczne poprzez zamieszczanie na stronach internetowych Policji informacji uświadamiających obywateli w zakresie przestępczości komputerowej. Publikowane materiały dotyczyły w szczególności następujących zagadnień: *Phishing a pranie pieniędzy, Uwaga-hakerzy podszywają się pod Policję, Jak uniknąć oszustwa nigeryjskiego, Ochrona informatyczna danych - phishing i kradzież tożsamości, Kompendium jak nie dać się oszukać w Internecie, Cyberprzestępczość, Internetowe oszustwa aukcyjne, Nowa metoda wyłudzania pieniędzy – numery Premium, Handel organami ludzkimi w Internecie, Być świadomym i bezpiecznym użytkownikiem Internetu, Oszustwa Internetowe – jak się bronić?*

(dowód: akta kontroli str. 615)

3.6. Wspieranie badań i rozwoju w obszarze ochrony cyberprzestrzeni.

Wyższa Szkoła Policji w Szczytnie (WSPol) realizuje w partnerstwie projekt CAMINO – Comprahensive Approach to Cyber Roadmap Coordination and Development (Kompleksowe podejście do stworzenia i rozwoju mapy dotyczącej cyberbezpieczeństwa), ze środków finansowych 7 Programu Ramowego Komisji Europejskiej. Liderem projektu jest firma ITTI Sp. z o.o. w Poznaniu. Celem projektu jest stworzenie realistycznego planu działania poprzez wypracowanie systemu ochrony przed cyberprzestępczością i cyberterroryzmem. Efektem końcowym ma być opracowanie mapy oraz wdrożenie projektu poprzez warsztaty, seminaria i działania zmierzające ku zwiększeniu świadomości społeczeństwa na tego typu zagrożenia. Projekt jest realizowany od 1 kwietnia 2014 r. i ma być zakończony 31 maja 2016 r. Całkowity koszt projektu wyniesie 1 162,9 tys. euro, w tym z budżetu WSPol 41,4 tys. euro.

Ponadto WSPol realizuje zadania badawcze w obszarze ochrony cyberprzestrzeni w ramach działalności statutowej ze środków Ministerstwa Nauki i Szkolnictwa Wyższego:

- Opracowanie wymagań techniczno-organizacyjnych i prawnych do utworzenia w WSPol centrum doskonalenia zwalczania cyberprzestępczości;
- Identyfikacja pozytywnych i negatywnych czynników wpływających na wykrywalność sprawców oszustw komputerowych i telekomunikacyjnych.

(dowód: akta kontroli str. 625-626, 629-630, 644-664)

3.7. Współpraca międzynarodowa.

W zakresie zwalczania cyberprzestępczości Policja współpracuje z funkcjonującymi w ramach Europolu European Cybercrime Centre (EC3) i European Cybercrime Tasc Force (EUCTF). Współpraca w ramach Europolu, wg. wyjaśnień Komendanta Głównego Policji, polega na wymianie tzw. *dobrych praktyk* (eksperci specjalizujący się w zwalczaniu cyberprzestępczości prezentują sprawy oraz sposoby ich rozwiązania), wymianie informacji o *modus operandi* sprawców, czy o narzędziach służących do popełniania cyberprzestępstw. Istnieje też możliwość nawiązania bezpośrednich kontaktów pomiędzy ekspertami w dziedzinie przestępczości komputerowej. Wskazywane są także narzędzia (darmowe i płatne) wspomagające pracę Policji w zwalczaniu tego rodzaju przestępstw.
Funkcjonariusze KGP i WSPol w Szczytnie uczestniczą w realizowanych, głównie w Hadze, konferencjach i szkoleniach Europolu.

(dowód: akta kontroli str. 626-627, 640, 1103)

Ustalone nieprawidłowości

Kontrola wykazała, że w KGP nie została wdrożona procedura pt. *Zarządzanie zdarzeniami związanymi z bezpieczeństwem informacji*[40], która nakładała obowiązek raportowania o zdarzeniach związanych z bezpieczeństwem informacji oraz prowadzenia rejestru incydentów. Od dnia zatwierdzenia ww. procedury przez Dyrektora Biura Łączności i Informatyki KGP (28 listopada 2011 r.) nie była ona w ogóle stosowana, co skutkowało m.in. brakiem rzetelnej i usystematyzowanej wiedzy na temat incydentów bezpieczeństwa występujących w jawnych sieciach i systemach teleinformatycznych Policji.

Odpowiedzialność za powstanie opisanej powyżej nieprawidłowości ponoszą osoby kierujące w latach 2011 – 2014 Biurem Łączności i Informatyki KGP.

Uwagi dotyczące badanej działalności

NIK zwraca uwagę, że w KGP nie został zorganizowany formalny, wewnętrzny zespół reagowania na incydenty komputerowe (CERT). W rezultacie, KGP nie dysponowała m.in. zasobami pozwalającymi na podejmowanie aktywnych działań w sytuacji wystąpienia zagrożeń i incydentów bezpieczeństwa dotyczących jawnych, policyjnych sieci i systemów teleinformatycznych[41]. Zorganizowane działania mające na celu weryfikację informacji o zagrożeniach oraz reagowanie na incydenty miały miejsce tylko w przypadku zdarzeń związanych z policyjnymi systemami przetwarzającymi informacje niejawne i dane osobowe. Zdaniem NIK, zasadne jest zatem podjęcie działań mających na celu wzmocnienie zdolności Policji w zakresie reagowania na incydenty komputerowe, m.in. poprzez powołanie policyjnego zespołu CERT (analogicznie np. do Zespołu MIL-CERT funkcjonującego od kilku lat w resorcie obrony narodowej). Zintensyfikowanie działań w ww. zakresie wpłynęłoby pozytywnie na bezpieczeństwo sieci i systemów teleinformatycznych Policji, których prawidłowe funkcjonowanie jest niezbędne dla realizacji zadań służbowych tej formacji.

Ocena cząstkowa

W okresie objętym kontrolą Komendant Główny Policji podejmował działania, które które należy zdefiniować, jako dobre praktyki związane z ochroną cyberprzestrzeni RP. W szczególności opracowano procedury systemu bezpieczeństwa informacji przetwarzanych przez Policję oraz podjęto szereg działań informacyjno-edukacyjnych dotyczących zagrożeń w sieci, bezpiecznego korzystania z Internetu oraz odpowiedzialności za przestępstwa komputerowe. Ustalono natomiast, że nie został wdrożony kompleksowy system reagowania na zagrożenia i incydenty występujące w cyberprzestrzeni, obejmujący zadania z zakresu ujawniania, przeciwdziałania, analizowania i monitorowania sposobu rozpatrywania incydentów teleinformatycznych. W przypadku zdarzeń dotyczących jawnych systemów i sieci

---

[40] Wprowadzona w ramach normy *System zarządzania bezpieczeństwem informacji PN-ISO/IEC 27007:2007.*

[41] W latach 2012-2014 otrzymano z Zespołu CERT.GOV.PL 1 807 informacji na temat zagrożeń i incydentów zidentyfikowanych w jawnych, policyjnych systemach teleinformatycznych.

teleinformatycznych, BŁiI KGP ograniczało się do zbierania danych i przekazywania informacji do właściwych jednostek i komórek organizacyjnych Policji, bez podejmowania dalszych działań wyjaśniających i monitorujących sposób załatwienia danego incydentu. W KGP nie został zorganizowany wewnętrzny zespół reagowania na incydenty komputerowe (CERT) oraz nie przestrzegano zatwierdzonej przez Dyrektora BŁiI KGP procedury dotyczącej raportowania i ewidencjonowania incydentów występujących w jawnych systemach teleinformatycznych Policji.

IV. 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[42], wnosi o:

1. Podjęcie działań w celu utworzenia w Policji wewnętrznego zespołu reagowania na incydenty komputerowe.
2. Wdrożenie efektywnych procedur dotyczących raportowania i ewidencjonowania incydentów bezpieczeństwa odnoszących się do wszystkich policyjnych sieci i systemów teleinformatycznych.
3. Realizację zadań wynikających z Polityki, dotyczących przekazania Ministrowi Administracji i Cyfryzacji informacji wymaganych na podstawie pkt 5 i 6 tego dokumentu.

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.

Zgodnie z art. 62 ustawy o NIK proszę o poinformowanie Najwyższej Izby Kontroli, w terminie 21 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 13.10. 2014 r.

Wiceprezes
Najwyższej Izby Kontroli
Wojciech Kutyła

[42] Dz. U. z 2012 r., poz. 82 ze zm.