NAJWYŻSZA IZBA KONTROLI

REALIZACJA PRZEZ PODMIOTY PAŃSTWOWE ZADAŃ W ZAKRESIE OCHRONY CYBERPRZESTRZENI RP

Wstępne wyniki kontroli przeprowadzonej w 2014 r.

Departament Porządku i
Bezpieczeństwa Wewnętrznego
NAJWYŻSZA IZBA KONTROLI
www.nik.gov.pl

Warszawa, 26.11.2014 r.

Zadania NIK

Najwyższa Izba Kontroli jest naczelnym i niezależnym organem kontroli państwowej.

NIK kontroluje legalność, gospodarność, celowość i rzetelność wydatkowania pieniędzy publicznych.

Misją NIK jest realizowanie kontroli odpowiadających na aktualne problemy społeczne i gospodarcze.

Proces kontrolny

Proces kontrolny realizowany przez NIK obejmuje:

- przygotowanie tematyki kontroli;
- badania prowadzone w jednostkach kontrolowanych;
- opracowanie wystąpień pokontrolnych;
- sporządzenie i opublikowanie zbiorczej informacji o wynikach kontroli.

Kontrola, której dotyczy niniejsze wystąpienie nie została jeszcze zakończona. W związku z powyższym prezentujemy wstępne wyniki kontroli oraz sporządzony na potrzeby konferencji wstępny zarys informacji o wynikach kontroli.

Nasz Departament

Departament Porządku i Bezpieczeństwa Wewnętrznego

Kontrolujemy zadania związane z bezpieczeństwem wewnętrznym państwa oraz z wymiarem sprawiedliwości.

Swoimi działaniami obejmujemy między innymi:

- Agencję Bezpieczeństwa Wewnętrznego;
- Agencję Wywiadu;
- Centralne Biuro Antykorupcyjne;
- Policję;
- Prokuraturę;
- Ministerstwo Sprawiedliwości;
- Sądy Powszechne.

Pomysł na temat kontroli

Kontrola będąca tematem bieżącej prezentacji jest prowadzona z własnej inicjatywy NIK.

Przyczynami objęcia tego tematu kontrolą były:

- postępujący rozwój społeczeństwa informacyjnego skutkujący jednocześnie wzrostem zagrożeń występujących w cyberprzestrzeni;
- zdefiniowanie cyberprzestrzeni, jako nowego obszaru działań podmiotów państwowych związanych z szeroko rozumianym bezpieczeństwem państwa, który nie był wcześniej kontrolowany przez Izbę;
- niska świadomość obywateli i instytucji publicznych w zakresie zagrożeń związanych z bezpieczeństwem IT.

Przygotowanie tematyki kontroli

Kontrole prowadzone przez NIK wymagają określenia tak zwanego „wyznacznika”, pozwalającego na dokonanie oceny kontrolowanej działalności.

Wyznacznikiem mogą być np. przepisy prawa lub zbiory dobrych praktyk.

W przypadku kontroli będącej tematem niniejszej prezentacji, określenie takiego „wyznacznika” było trudne i wymagało podjęcia szeregu różnorodnych działań.

Przygotowanie kontroli: kwerenda aktów prawnych

Przeprowadzona kwerenda aktów prawnych wykazała:

- brak kompleksowych regulacji prawnych;
- rozproszenie zadań związanych z ochroną cyberprzestrzeni między różne podmioty państwowe i prywatne.

Podstawowymi regulacjami zdefiniowanymi w tym obszarze były:

- Prawo telekomunikacyjne;
- Ustawa o zarządzaniu kryzysowym;
- Ustawa o informatyzacji podmiotów realizujących zadania publiczne;
- Ustawa o świadczeniu usług drogą elektroniczną;
- Prawo Bankowe.

Przygotowanie kontroli: analiza projektów narodowej strategii bezpieczeństwa w cyberprzestrzeni

W latach 2008-2011 opracowano siedem kolejnych projektów narodowej strategii bezpieczeństwa w cyberprzestrzeni.

Żaden z ww. siedmiu dokumentów programowych nie został zatwierdzony przez Radę Ministrów i przyjęty formalnie do realizacji.

Przygotowanie kontroli: analiza narodowej strategii bezpieczeństwa w cyberprzestrzeni

W dniu 25 czerwca 2013 roku, tj. ponad pięć lat po rozpoczęciu prac nad przygotowaniem narodowej strategii bezpieczeństwa w cyberprzestrzeni, Rada Ministrów przyjęła dokument pt. „Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej".

Analiza treści ww. dokumentu wykazała problemy z jego interpretacją oraz liczne braki merytoryczne, stawiające pod dużym znakiem zapytania jego użyteczność oraz możliwość praktycznego zastosowania.

Przygotowanie kontroli: poszukiwanie zbiorów dobrych praktyk

W celu zdefiniowania zbiorów dobrych praktyk w obszarze ochrony cyberprzestrzeni, zainicjowano konsultacje z następującymi podmiotami:

- ENISA;
- MAiC, ABW, MF, KPRM, MNiSW, RCB, MIR, MON, NCBiR, MSW;
- najwyższe organy kontrolne z innych państw;
- niezależni eksperci;
- przedstawiciele nauki;
- zespoły CERT;
- przedstawiciele biznesu;
- ABUSE forum.

Przygotowanie kontroli: rezultaty

Przeprowadzone analizy pozwoliły na stwierdzenie, że ogólna diagnoza dotycząca stanu cyberbezpieczeństwa w Polsce jest wysoce niepokojąca. W szczególności stwierdzono brak systemowych działań instytucji publicznych w celu podniesienia poziomu bezpieczeństwa państwa i obywateli w cyberprzestrzeni.

Zakres kontroli: ryzyka

Celem kontroli było zweryfikowanie ryzyk zidentyfikowanych w działalności państwa w zakresie bezpieczeństwa IT, dotyczących:

- braku spójnego systemu działań;
- braku szacowania ryzyk;
- nieustanowienia mechanizmów współpracy z komercyjnymi użytkownikami i administratorami cyberprzestrzeni;
- braku podziału kompetencji;
- nieprzydzielenia zasobów do realizacji zadań;
- braku mechanizmów koordynacji i wymiany informacji.

Zakres kontroli: podmioty i okres czasowy

Kontrolą objęto:

- Ministerstwo Administracji i Cyfryzacji;
- Ministerstwo Spraw Wewnętrznych;
- Agencję Bezpieczeństwa Wewnętrznego - Zespół CERT.GOV.PL;
- Ministerstwo Obrony Narodowej;
- Urząd Komunikacji Elektronicznej;
- Rządowe Centrum Bezpieczeństwa;
- Policję;
- Naukową i Akademicką Sieć Komputerową - Zespół CERT Polska.

Okres objęty kontrolą: lata 2008-2014

Ustalenia kontroli w MSW:

1. Nie została określona rola Ministra Spraw Wewnętrznych w ramach systemu ochrony cyberprzestrzeni RP.
2. W MSW brak było świadomości jakichkolwiek obowiązków związanych z bezpieczeństwem państwa w cyberprzestrzeni.
3. Ministerstwo nie uczestniczyło w budowie systemu ochrony cyberprzestrzeni państwa.
4. MSW nie realizowało żadnych zadań skierowanych do użytkowników i administratorów cyberprzestrzeni spoza resortu spraw wewnętrznych.
5. Nie dokonano formalnego przekazania dokumentacji i zadań z byłego MSWiA do MSW i MAiC.

Ustalenia kontroli w MSW cd.:

6. W MSW w ogóle nie wdrożono zapisów Polityki Ochrony Cyberprzestrzeni RP.
7. Zadania związane z ochroną resortowych systemów teleinformatycznych były realizowane nierzetelnie, tj.:
   - nie oszacowano ryzyka dla własnych zasobów IT;
   - nie określono zasobów niezbędnych do ich ochrony;
   - nie zdefiniowano zasad i wymagań bezpieczeństwa informacji.
8. MSW nie realizowało obowiązków w zakresie kontroli systemów teleinformatycznych.

Ustalenia kontroli w Komendzie Głównej Policji

Podstawowe obszary działań Policji w zakresie bezpieczeństwa cyberprzestrzeni dotyczyły:

- zwalczania przestępczości komputerowej;
- aktywności informacyjnej i edukacyjnej na temat zagrożeń związanych z korzystaniem z Internetu.

Ustalenia kontroli w Komendzie Głównej Policji cd.:

Nieprawidłowości i problemy systemowe dotyczące ochrony policyjnych systemów teleinformatycznych:

1.Brak kompleksowego systemu reagowania na incydenty komputerowe w jednostkach Policji.

2.Brak ewidencjonowania informacji o incydentach.

3.Brak zespołu CERT.

4.Brak właściwej realizacji zadań wynikających z Polityki Ochrony Cyberprzestrzeni RP.

Ustalenia kontroli w MON

Działania MON związane z ochroną cyberprzestrzeni dotyczyły:

- aktywnego uczestnictwa w budowie systemu ochrony cyberprzestrzeni;
- powołania resortowego systemu reagowania na incydenty komputerowe oraz Zespołu CERT.MIL;
- określenia resortowych wymogów bezpieczeństwa IT;
- aktywnej wymiany informacji z innymi podmiotami;
- wdrażania zapisów Polityki Ochrony Cyberprzestrzeni RP;
- rozwijania potencjału w zakresie ochrony cyberprzestrzeni.

Ustalenia kontroli w MON cd.

W działalności MON stwierdzono problemy i ryzyka o charakterze systemowym dotyczące:

- częstych zmian struktur organizacyjnych;
- podporządkowania całego resortowego systemu bezpieczeństwa IT Narodowemu Centrum Kryptologii oraz personalnie jednej osobie;
- braku oszacowania zasobów niezbędnych do realizacji zadań w zakresie ochrony cyberprzestrzeni;
- nieopracowania całościowego, docelowego modelu organizacyjnego systemu ochrony cyberprzestrzeni resortu obrony narodowej.

Ustalenia kontroli w ABW

Działania ABW związane z ochroną cyberprzestrzeni dotyczyły:

- powołania Zespołu CERT.GOV.PL.;
- wdrażania systemu wczesnego ostrzegania ARAKIS;
- wymiany informacji z innymi podmiotami;
- aktywnej działalności szkoleniowej i edukacyjnej;
- przeprowadzania testów bezpieczeństwa;
- aktywnego uczestnictwa w budowie systemu ochrony cyberprzestrzeni;
- wdrażania zapisów Polityki Ochrony Cyberprzestrzeni RP.

Ustalenia kontroli w ABW cd.

W działalności ABW stwierdzono problemy o charakterze systemowym dotyczące:

- ograniczonych zasobów ludzkich i finansowych;
- brak umocowania prawnego Zespołu CERT.GOV.PL.;
- kontrowersyjnego usytuowania Zespołu CERT.GOV.PL.

Ustalenia kontroli w NASK

NASK podejmowała działania związane z ochroną cyberprzestrzeni dotyczące w szczególności:

- powołania CERT Polska – de facto narodowego Zespołu CERT;
- ustanowienia kanałów wymiany informacji o incydentach;
- propagowania i weryfikowania bezpieczeństwa IT;
- utrzymywania kontaktów z innymi podmiotami krajowymi i zagranicznymi zaangażowanymi w bezpieczeństwo IT;
- stworzenia i rozwijania systemu ARAKIS;
- działalności szkoleniowej, informacyjnej i edukacyjnej;
- projektów naukowo-badawczych.

Ustalenia kontroli w NASK cd.

W działalności NASK stwierdzono problemy o charakterze systemowym dotyczące:

- ograniczeń działalności NASK wynikających z uwarunkowań biznesowych;
- tymczasowego i nieformalnego charakteru działań NASK w zakresie ochrony cyberprzestrzeni oraz niechęci do potwierdzenia narodowego charakteru zespołu CERT Polska.

Ustalenia kontroli RCB

W działalności RCB zdefiniowano dobre praktyki związane z ochroną cyberprzestrzeni dotyczące:

- zawarcia w Narodowym Programie Ochrony Infrastruktury Krytycznej ogólnych rekomendacji dotyczących ochrony teleinformatycznej obiektów infrastruktury krytycznej;
- propozycji ustanowienia stopni alarmowych związanych ze zdarzeniami w cyberprzestrzeni;
- publikowania informatora o teleinformatycznej infrastrukturze krytycznej;
- wdrażania Polityki Ochrony Cyberprzestrzeni RP.

Ustalenia kontroli RCB cd.:

1. Brak spójności systemów zarzadzania kryzysowego i ochrony cyberprzestrzeni.
2. Brak współpracy RCB i MAiC w zakresie analizy ryzyka i identyfikacji systemów krytycznej infrastruktury IT.
3. Nieadekwatność procedur zarządzania kryzysowego w stosunku do zagrożeń w cyberprzestrzeni

Ustalenia kontroli UKE

W UKE podejmowano działania mające na celu wdrożenie postanowień Polityki Ochrony Cyberprzestrzeni RP, tj.:

- oszacowano ryzyka dla systemów teleinformatycznych Urzędu;
- powołano Pełnomocnika ds. bezpieczeństwa cyberprzestrzeni;
- budowano system zarządzania bezpieczeństwem informacji.

Ustalenia kontroli UKE cd.

W wyniku kontroli w UKE stwierdzono brak możliwości wykorzystania obowiązujących przepisów Prawa telekomunikacyjnego w ramach realizacji zadań związanych z ochroną cyberprzestrzeni , tj.:

- brak informacji na temat incydentów w cyberprzestrzeni;
- brak realizacji obowiązku informacyjnego wobec konsumentów;
- nieadekwatność planów działań przedsiębiorców telekomunikacyjnych w sytuacjach szczególnych zagrożeń.

Ustalenia kontroli MAiC

Kontrola wykazała brak przygotowania organizacyjnego i merytorycznego MAiC do realizacji zadań związanych z ochroną cyberprzestrzeni, w szczególności:

1.Brak świadomości obowiązków w zakresie ochrony cyberprzestrzeni.

2.Działania prowadzone ad hoc, bez właściwego przygotowania.

Ustalenia kontroli MAiC cd.:

3. Brak wystarczających zasobów do realizacji zadań.
4. Brak podstawowej ciągłości w realizacji zadań Urzędu.

Ustalenia kontroli MAiC cd.:

5. Przyjęcie podejścia polegającego na biernym oczekiwaniu na dyrektywę NIS.
6. Brak wdrożenia Polityki Ochrony Cyberprzestrzeni RP w Ministerstwie.

Ustalenia kontroli MAiC cd.

Minister Administracji i Cyfryzacji w praktyce nie koordynował i nie inicjował zadań związanych z ochroną cyberprzestrzeni. Ograniczone zadania w tym zakresie są prowadzone dopiero od lutego 2014 r.

Podsumowanie

Kontrola wykazała, że w chwili obecnej, podmioty państwowe nie prowadzą spójnych i systemowych działań związanych z ochroną cyberprzestrzeni RP. Jako działania pozytywne i wzory dobrych praktyk można wskazać jedynie „fragmentaryczne" działania poszczególnych instytucji np. powołanie i utrzymywanie na wysokim poziomie Zespołów CERT przez ABW, MON oraz NASK.

Podsumowanie – problemy systemowe

Podstawowymi problemami w realizacji zadań państwa związanych z ochroną cyberprzestrzeni są:

1.Brak świadomości nowych zagrożeń u decydentów politycznych i kierownictwa administracji rządowej oraz brak zainteresowania kwestiami bezpieczeństwa IT ze strony najważniejszych osób w państwie.

2.Działania bez przygotowania i spójnej wizji systemowej.

3.Brak ośrodka decyzyjnego i koordynacyjnego.

4.Rozproszenie kompetencji i brak współpracy instytucji państwowych.

Podsumowanie – problemy systemowe cd.:

5. Brak kompleksowych regulacji prawnych.
6. Niewykorzystywanie istniejących przepisów.
7. Przyjęcie podejścia polegającego na biernym oczekiwaniu na dyrektywę NIS.
8. Brak CERT'u narodowego.
9. Braki i wady Polityki ochrony cyberprzestrzeni RP.

Wnioski na przyszłość

W ocenie NIK stan faktyczny ustalony w ramach kontroli wskazuje na pilną potrzebę podjęcia na najwyższym szczeblu wiążących decyzji odnośnie strategii i modelu ochrony cyberprzestrzeni w Polsce.

Modyfikacji wymaga również dominujące obecnie podejście biernego oczekiwania z decyzjami na dyrektywę NIS.

Dziękuję za uwagę!