NAJWYŻSZA IZBA KONTROLI
Departament Porządku i Bezpieczeństwa Wewnętrznego

KPB – KPB-4101-002-04/2014
P/14/043

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
ul. Filtrowa 57, 02-056 Warszawa
T +48 22 444 56 12, F +48 22 444 56 29
kpb@nik.gov.pl
Adres korespondencyjny: Skr. poczt. P-14, 00-950 Warszawa 1

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

Adam Zakrzewski, główny specjalista kontroli państwowej, upoważnienie do kontroli nr 89666 z dnia 09.06.2014 r.

(dowód: akta kontroli strona 1)

Jednostka kontrolowana

Naukowa i Akademicka Sieć Komputerowa, ul Wąwozowa 18, 02-796 Warszawa

Kierownik jednostki kontrolowanej

Maciej Kozłowski, od 28.10.2005r. do 15.11.2009r.

Michał Chrzanowski, od 16.11.2009r. – nadal

(dowód: akta kontroli strony 231,232)

II. Ocena kontrolowanej działalności

Ocena ogólna

Kontrola wykazała[1], że Dyrektor Naukowej i Akademickiej Sieci Komputerowej inicjował i podejmował działania[2], które można określić, jako dobre praktyki związane z ochroną cyberprzestrzeni Rzeczypospolitej Polskiej (cRP). Dotyczyły one w szczególności:

Uzasadnienie oceny ogólnej

- Powołania w NASK komórki organizacyjnej Computer Emergency Response Team Polska (CERT) Polska zajmującej się zdarzeniami naruszającymi bezpieczeństwo w sieci Internet.
- Pełnienia, w ramach posiadanych zasobów, roli - nieutworzonego formalnie w Polsce - narodowego zespołu CERT[3], wypełniania jego obowiązków w ramach międzynarodowych organizacji i przedsięwzięć.
- Ustanowienia i utrzymywania kanałów wymiany informacji o incydentach komputerowych obejmujących różne grupy użytkowników, w szczególności: systemu zbierania zgłoszeń dotyczących incydentów bezpieczeństwa teleinformatycznego, platformy n6, Abuse-Forum, kontaktów bezpośrednich

---

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 (19 września 2014 r.)

3 Narodowy zespół CERT - Zespół reagowania na incydenty pełniący rolę krajowego punktu kontaktowego - organizującego wymianę informacji o incydentach i podatnościach pomiędzy krajowymi i zagranicznymi zespołami CERT oraz koordynującego prace tych zespołów w przypadku obsługi istotnych lub rozległych incydentów. Powinien posiadać oficjalne - uzyskane od krajowej administracji - potwierdzenie swojej pozycji.

i nieformalnych oraz uczestnictwa w międzynarodowych spotkaniach i konferencjach.

- Propagowania i weryfikowania - w ramach prowadzonej działalności gospodarczej - rozwiązań zwiększających bezpieczeństwo systemów komputerowych.
- Brania udziału w ćwiczeniach dotyczących systemu bezpieczeństwa cyberprzestrzeni.
- Współpracy i utrzymywania roboczych kontaktów z innymi - krajowymi i zagranicznymi – organizacjami i podmiotami związanymi z ochroną cyberprzestrzeni, w tym z zespołem CERT.GOV.PL.
- Stworzenia i rozwijania systemu wczesnego ostrzegania o zagrożeniach wykrytych w Internecie.
- Prowadzenia działalności szkoleniowej, informacyjnej i edukacyjnej dotyczącej bezpieczeństwa w cyberprzestrzeni.
- Udziału w projektach naukowo badawczych dotyczących zwiększenia bezpieczeństwa w cyberprzestrzeni.

III. Opis ustalonego stanu faktycznego

1.1. Ramy prawne systemu ochrony cyberprzestrzeni RP.

Opis stanu faktycznego

Naukowa i Akademicka Sieć Komputerowa jest instytutem badawczym działającym na podstawie ustawy z dnia 30 kwietnia 2010r. o instytutach badawczych[4]. Wykonuje prace badawcze związane, z jakością usług teleinformatycznych oraz bezpieczeństwem systemów informatycznych. W ramach działalności gospodarczej projektuje, buduje i utrzymuje systemy teletransmisyjne, świadczy usługi w zakresie bezpieczeństwa sieciowego. NASK pełni również rolę krajowego rejestru nazw internetowych w domenie ".pl".

W ramach struktury NASK kontrolą objęto dwie komórki organizacyjne uczestniczące bezpośrednio w realizacji zadań związanych z ochroną cRP: Zespół Integracji i Bezpieczeństwa Systemów oraz CERT Polska, w skład którego wchodzą: Zespół Reagowania na Incydenty Naruszające Bezpieczeństwo Teleinformatyczne, Zespół Projektów Bezpieczeństwa oraz Laboratorium Ekspertyz i Certyfikacji.

Stwierdzony w trakcie kontroli udział NASK w systemie ochrony cRP nie jest bezpośrednio powiązany z wymaganiami zapisanymi w aktach prawnych. Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej (Polityka) nie nakłada na NASK żadnych szczególnych obowiązków, wskazując jedynie na jej rolę w wytworzeniu, wymagającego rozbudowy, systemu wczesnego ostrzegania ARAKIS-GOV oraz na możliwość udziału w procesach obsługi incydentów, dla których Zespół CERT.GOV.PL realizuje zadania głównego narodowego zespołu odpowiadającego za ich koordynację. Zgodnie z zapisami Polityki, ustanowiony przez Rząd RP Krajowy System Reagowania na Incydenty Komputerowe zapewnia wymianę informacji pomiędzy zespołami administracji publicznej oraz zespołami CERT, w tym CERT Polska.

NASK nie bierze udziału w współtworzeniu projektów aktów prawnych związanych z systemem ochrony cRP. W przypadku projektów aktów prawnych mających związek z działalnością NASK bierze natomiast udział w konsultacjach społecznych.

---

[4] Dz. U. Nr 96, poz. 618 ze zm. Poprzednio - ustawa z dnia 25 lipca 1985 r. o jednostkach badawczo-rozwojowych (Dz. U. z 2008 r. Nr 159, poz. 993 ze zm.)

Dowód: akta kontroli strony 127-134

Ustalone nieprawidłowości

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

1.2. Opracowanie projektów szczegółowych określających sposób realizacji Polityki.

Opis stanu faktycznego

W kontrolowanym okresie NASK nie brała udziału w opracowywaniu projektów szczegółowych określających sposób i zakres realizacji zdefiniowanych w Polityce procesów w zakresie ochrony cRP. Realizacja projektu ARAKIS 2.0, zakończona w kwietniu 2014r. oraz podpisana z ABW umowa na wdrożenie, do października 2015r. systemu ARAKIS 2.0 GOV, pomimo zbieżności z zapisanym w punkcie 3.6.3 Polityki projektem szczegółowym „Rozbudowa systemu wczesnego ostrzegania oraz wdrożenie i utrzymanie rozwiązań prewencyjnych" jest realizowana przez NASK, jako przedsięwzięcie niezwiązane z tym projektem.

Dowód: akta kontroli strony 127-134

Ustalone nieprawidłowości

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

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

Opis stanu faktycznego

Zespół CERT Polska opiera stosowaną przez siebie klasyfikację incydentów na publicznej wersji opracowanej w ramach projektu eCSIRT.net. Jest ona upubliczniona w treści internetowego formularza pozwalającego na zgłaszanie incydentów do CERT Polska. Stanowi ona również podstawę statystyk i zestawień publikowanych przez Zespół w corocznych raportach. Próby ujednolicenia klasyfikacji podejmowane w ramach prac Abuse-Forum zakończyły się niepowodzeniem z powodu różnej specyfiki incydentów obsługiwanych przez poszczególne podmioty. Problem niejednolitej klasyfikacji incydentów nie jest specyficzny dla Polski – dotyczy wielu organizacji i forów skupiających zespoły reagujące.

Dowód: akta kontroli strony 108,109,209-211,

Podstawowym projektem realizowanym przez NASK w ramach wspierania budowy systemu wymiany informacji jest platforma „n6" umożliwiająca dzielenie się, w sposób zautomatyzowany, dotyczącą całego polskiego Internetu wiedzą operacyjną o incydentach, gromadzoną, z różnych źródeł, przez zespół CERT Polska. Zgodnie z uzyskanymi wyjaśnieniami Dyrektora NASK, żaden inny zespół w kraju nie gromadzi takich informacji, a nawet nie ubiegał się o dostęp do nich. Odbiorcami informacji mogą być właściciele sieci, ich operatorzy i administratorzy. Platforma pozwala im na codziennie pobieranie informacji o zagrożeniach w podległej im infrastrukturze. Dostęp do „n6" jest bezpłatny i nie wymaga posiadania specjalistycznego oprogramowania. Charakterystyka „n6", wraz z informacjami o sposobie uzyskania dostępu, są upublicznione na stronie internetowej Zespołu. Z 9 przedsiębiorców telekomunikacyjnych o szczególnym znaczeniu gospodarczo-obronnym[5], dla których łącznie w bazie platformy „n6", w okresie od 1.08.2013r. do 31.07.2014r. zgromadzono około 44,5 miliona zapisów dotyczących incydentów lub zagrożeń, z dostępu do tej platformy korzystało w kontrolowanym okresie dwóch. Pozostali przedsiębiorcy, w odpowiedzi na

[5] Przedsiębiorcy wymienieni w części V załącznika do rozporządzenia Rady Ministrów z dnia 4 października 2010 r. w sprawie wykazu przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym (Dz. U. z 2014 r., poz. 303)

zapytanie kontrolera, dotyczące braku zainteresowania zgromadzonymi informacjami, wyjaśnili to różnorodnymi przyczynami: brakiem wiedzy o istnieniu „n6", stosowaniem innych metod wykrywania incydentów i zagrożeń, a także wątpliwościami, co do jakości zgromadzonych tam danych.
Platforma „n6" pozwalała również Zespołowi CERT Polska na wypełnianie niektórych zadań krajowego punktu kontaktowego (będącego zwykle domeną nieistniejącego formalnie w Polsce CERT'u narodowego) – do momentu zakończenia kontroli z zapisanych w „n6" informacji dotyczących sieci krajowych korzystało 26 zagranicznych zespołów reagowania. Innym z działań Zespołu, realizującym zadania krajowego punktu kontaktowego, jest podejmowanie interwencji w przypadku braku właściwej reakcji lokalnych administratorów na incydenty dotyczące polskich sieci.

Dowód: akta kontroli strony 23, 24, 99-120, 135-163, 236-251

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości

1.4. Udział w procesach szacowania ryzyka.

Opis stanu faktycznego

NASK i zespół CERT Polska nie uczestniczył formalnie w procesach szacowania ryzyka, związanego z zdarzeniami występującymi w cyberprzestrzeni, realizowanych przez inne podmioty państwowe (w szczególności MAiC i Rządowe Centrum Bezpieczeństwa - RCB). W roku 2008 RCB jednorazowo konsultowało z Zespołem CERT Polska definicje zagrożeń dla teleinformatycznej infrastruktury krytycznej.

Dowód: akta kontroli strony 135-148

Ustalone nieprawidłowości

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

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

Opis stanu faktycznego

NASK nie opracowała i nie upublicznia formalnego zbioru dobrych praktyk w zakresie bezpieczeństwa teleinformatycznego. Powyższe wynika z faktu, że propagowanie dobrych praktyk i bezpiecznych rozwiązań wśród swoich klientów stanowi dla NASK jedną z form działalności gospodarczej. Zgodnie z uzyskanymi przez kontrolującego wyjaśnieniami, wiedza ta, stanowi istotne aktywa i jako takie, musi być, w warunkach konkurencji, właściwie chroniona. Do pewnego stopnia za propagowanie dobrych praktyk można jednak uznać opracowywanie i upublicznianie przez Zespół informacji o istotnych zdarzeniach i incydentach oraz corocznych raportów. Omówione w nich mechanizmy poszczególnych zagrożeń pozwalają użytkownikom cyberprzestrzeni na łatwiejszą ich identyfikację i podjęcie odpowiednich kroków zaradczych.

Dowód: akta kontroli strony 21-23, 127-130

Ustalone nieprawidłowości

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

1.6. Organizacja ćwiczeń i testów systemu bezpieczeństwa cyberprzestrzeni.

Opis stanu faktycznego

W latach 2012 - 2014 Zespół CERT Polska nie był organizatorem ćwiczeń w zakresie systemu bezpieczeństwa cyberprzestrzeni, dwukrotnie brał natomiast udział w takich ćwiczeniach organizowanych przez inne podmioty (w 2012 roku „Coalition Warrior Interoperability Exploration Experimentation & Examination

Exercises" organizowane przez NATO Joint Force Training Center oraz w 2014 roku „Locked Shields" organizowane przez NATO Cooperative Cyber Defence Centre of Excellence), raz odmówił (z powodu niekorzystnego zbiegu terminów) uczestnictwa w ćwiczeniach zorganizowanych w 2014 roku przez RCB. Uczestnictwo w ćwiczeniach nie wpływa bezpośrednio na zewnętrzną działalność NASK - pozwala jednak na utrzymywanie kontaktów międzynarodowych oraz podnoszenie kompetencji i kwalifikacji specjalistów z Zespołu CERT Polska.
W latach 2012 – 2014 Zespół CERT Polska przeprowadził 5 testów bezpieczeństwa, które dotyczyły różnych zagadnień, określanych każdorazowo przez zamawiającego. W jednym przypadku test dotyczył jednostki państwowej. W tym samym okresie Zespół Integracji i Bezpieczeństwa Systemów NASK przeprowadził w 22 jednostkach, w tym 10 państwowych, audyty bezpieczeństwa teleinformatycznego.

Dowód: akta kontroli strony 102-103, 233-235

Ustalone nieprawidłowości

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

1.7. Ustanowienie systemu reagowania na incydenty w cyberprzestrzeni.

Opis stanu faktycznego

Zespół CERT Polska jest komórką organizacyjną NASK ukierunkowaną przede wszystkim na obsługę incydentów dotyczących sieci NASK i klientów NASK. W ramach posiadanych sił i środków obsługiwane są również incydenty dotyczące innych sieci w domenie ".pl". Obsługując te incydenty Zespół stara się ustalić właściwego adresata informacji o incydencie i przekazać mu sprawę do dalszego prowadzenia. W przypadku incydentów o istotnym znaczeniu – niosących za sobą straty dla zaatakowanych (w szczególności finansowe) Zespół podejmuje działania dla wyjaśnienia sprawy i udzielenia pomocy zaatakowanemu. Oprócz bezpośredniego reagowania na incydenty, Zespół prowadzi również stałą analizę aktualnych zagrożeń i podatności dostosowując do nich swoje metody działania. Informacje określające aktualne zadania, zakres odpowiedzialności oraz katalog odbiorców usług Zespołu, publikowane są na jego stronach internetowych. Wybrany zakres informacji charakteryzujących CERT Polska jest również publikowany w katalogach zespołów CERT na stronach internetowych organizacji skupiających takie zespoły (Trusted Introducer, ENISA CERT Invertory). W związku z przyjęciem i wdrażaniem Polityki zakres odpowiedzialności, zadania i katalog odbiorców usług Zespołu CERT Polska nie uległ zmianie i zmiany takie nie są aktualnie planowane.
Ponieważ Zespół CERT Polska nie posiada osobowości prawnej, w zakresie formalnym współpracę i podział zadań reguluje umowa ramowa z 03.03.2010r. pomiędzy NASK i ABW. W związku z przyjęciem i wdrażaniem Polityki w zapisach tej umowy nie dokonano żadnych zmian.

Dowód: akta kontroli strony 138-163, 255, 256

Zgodnie z wyjaśnieniami Dyrektora Operacyjnego NASK, wieloletnia skuteczna działalność Zespołu spowodowała, że jest on rozpoznawany i wysoko oceniany przez różnorodne grupy, instytucje i firmy wykonujące zadania związane z bezpieczeństwem cyberprzestrzeni. Wieloletnia obecność Zespołu CERT Polska na arenie międzynarodowej (powiązana z brakiem innych polskich przedstawicieli) spowodowała, że w wielu sytuacjach, mając na względzie ważny interes społeczny, Zespół podejmował rolę polskiego CERT'u narodowego. Starał się on, w ramach posiadanych zasobów, wypełnić lukę w członkostwie w międzynarodowych organizacjach i wspólnych przedsięwzięciach. Powyższe rozwiązanie jest jednak,

w ocenie kierownictwa NASK jedynie tymczasowym - Zespół w obecnej sytuacji prawnej i ekonomicznej nie planuje podejmowania kroków dla potwierdzenia swojego de facto narodowego charakteru. Jest jednak gotowy do podjęcia współpracy w zakresie oficjalnego reprezentowania kraju na arenie międzynarodowej, jeżeli zostanie ona odpowiednio sformalizowana i zostaną dla niej zabezpieczone adekwatne środki i zasoby.

Dowód: akta kontroli strony 255, 256

Głównymi źródłami informacji o zagrożeniach, podatnościach i incydentach są dla Zespołu przede wszystkim własne systemy:

- wczesnego ostrzegania - ARAKIS,
- kategoryzujący strony internetowe pod względem stopnia i rodzaju zagrożenia dla użytkownika - HSN,
- blokujący infrastrukturę zarządzania złośliwym oprogramowaniem - oparty o mechanizm skinhole
- monitorujący funkcjonowanie sieci botnetu - Zeus P2P crawler.

Uzupełniające informacje pochodzą od współpracujących instytucji komercyjnych i organizacji niezależnych oraz z własnej pracy operacyjnej.

Dowód: akta kontroli strony 109,110

W Zespole CERT Polska została opracowana jedna procedura obsługi incydentów - jej zastosowanie nie jest związane z rodzajem lub wagą incydentu. Do rejestracji zgłoszeń oraz prowadzenia rejestru incydentów w Zespole wykorzystywany jest program komputerowy Request Tracker for Incident Response opracowany przez Best Practical Solutions LLC. Na potrzeby Zespołu program został odpowiednio sparametryzowany, w sposób pozwalający wspomagać realizację stosowanego procesu obsługi incydentów. W programie prowadzony jest rejestr zgłoszeń zawierający informacje przekazywane do Zespołu za pośrednictwem różnych kanałów w szczególności formularza znajdującego się na stronie www.cert.pl oraz przesyłek email. Program stanowi jedyne źródło informacji o stanie oczekujących zgłoszeń, zakończonych i prowadzonych aktualnie prac. Na podstawie informacji zarejestrowanych w programie sporządzane są zestawienia statystyczne dotyczące Zespołu CERT Polska, w tym w szczególności coroczne raporty z działalności.

Dowód: akta kontroli strony 164, 165, 212

W latach 2012 – 2013 pracownicy Zespól CERT Polska obsłużyli bezpośrednio (bez uwzględnienia rejestracji wykonywanych przez zautomatyzowane systemy) 2 301 incydentów, z których 8 uznano za poważne – mające lub potencjalnie mogące mieć: dużą skalę, poważne konsekwencje lub powodujące istotne straty dla zaatakowanych. Kontrolujący wybrał celowo 3 spośród poważnych incydentów i sprawdził, jakie działania zostały podjęte przez Zespół w związku z ich wykryciem;

- „Działalność botnetu Citadel" – kradzieże kilku milionów złotych, głównie klientów jednego z banków – sprawa wraz z dowodami została przekazana w marcu 2013r. do organów ścigania;
- „Błąd w panelu zarządzającym konfiguracją sygnalizacji świetlnej" – zagrożony podmiot został we wrześniu 2013r. poinformowany przez CERT Polska o zidentyfikowanym ryzyku telefonicznie. W trakcie rozmowy wyjaśniona została natura zagrożenia oraz przedstawiono sugerowane działania naprawcze. W listopadzie 2013r., w związku z brakiem reakcji na rozmowę telefoniczną,

informacje przekazano ponownie listownie i faksem. Na tą korespondencję Zespól nie otrzymał odpowiedzi;

- „Celowy atak na użytkowników bankowości elektronicznej, w większości księgowych i skarbników w urzędach samorządowych" – w wyniku analizy informacji pochodzących z centrum zarządzającego złośliwego oprogramowania Citadel, które Zespół uzyskał z serwisu ZeusTracker, zidentyfikowano dane dotyczące 191 komputerów. Opracowanie przez Zespół całego materiału w zakresie umożliwiającym identyfikację wszystkich ofiar było, ze względu na brak zasobów, niemożliwe. Zidentyfikowano spośród nich jednak Urząd Gminy Łowicz oraz inne urzędy samorządowe. Niezwłocznie po dokonaniu tych identyfikacji poinformowano telefonicznie Urząd Gminy Łowicz o fakcie przestępczego przejęcia jednego ze znajdujących się w sieci urzędu komputerów, przekazując drogą mailową dodatkowe informacje. Na powyższy sygnał Urząd Gminy nie odpowiedział. Ponadto dane dotyczące wszystkich ustalonych urzędów samorządowych zostały przekazane do Zespołu CERT.GOV.PL. Wójt Gminy Łowicz wyjaśnił kontrolującemu, że po otrzymaniu od NASK informacji o szkodliwym oprogramowaniu podjął działania likwidujące zagrożenie oraz usprawnił system zabezpieczeń w sieci komputerowej Urzędu.

Dowód: akta kontroli strony 48-50, 109, 237, 238, 253

Aktualnie w Zespole CERT Polska jest zatrudnionych 16 osób. W związku z interwencyjnym charakterem jego działania, oszacowanie niezbędnych dla funkcjonowania zasobów jest trudne i wymaga odpowiedniego reagowania na zmieniające się obciążenie. W praktyce podstawowymi wskaźnikami realizacji zadań dla Zespołu są:

- liczba incydentów obsługiwanych przez Zespół z uwzględnieniem ich wagi;
- liczba kierowanych do Zespołu zapytań na adres info@cert.pl oraz zapytań od prasy;
- liczba przygotowywanych opracowań dotyczących zagrożeń, w tym publikowanych raportów i prezentacji na konferencjach.

Bieżący monitoring ww. wskaźników pozwala na zapotrzebowanie dodatkowych zasobów lub przeznaczenie części do działalności projektowej i badawczo rozwojowej.

Dowód: akta kontroli strony 138-163

W opinii Kierownictwa NASK istotną rolę w aktualnym systemie ochrony polskiej cyberprzestrzeni pełni zorganizowany w ABW Zespół CERT.GOV.PL. Podejmuje on działania w zakresie zagrożeń i incydentów dotyczących obszarów cyberprzestrzeni związanych z funkcjonowaniem administracji rządowej, administracji samorządowej i innych urzędów. Dzięki swojemu umiejscowieniu Zespół ten posiada możliwość znacznie szerszej i bezpośredniej współpracy z administratorami i użytkownikami „rządowej" cyberprzestrzeni, określania i egzekwowania zasad i wytycznych oraz szybkiego interweniowania w sytuacjach zagrożeń. Ważnym elementem jest także możliwość powiązania, w przypadku incydentów bezpieczeństwa związanych z naruszeniem prawa, działań związanych z usunięciem skutków z wykrywaniem ich sprawców.

Dowód: akta kontroli strony 255-256

Zespół CERT Polska (a formalnie NASK, jako podmiot praw i obowiązków, w ramach, którego funkcjonuje Zespół) jest członkiem następujących organizacji realizujących zadania w zakresie bezpieczeństwa cyberprzestrzeni:

- TERENA TF-CSIRT - otwarta grupa robocza zespołów reagujących przy zrzeszeniu sieci akademickich (http://www.terena.org/activities/tf-csirt/: http://www.trusted-introducer.org/); pełne członkostwo od 2001 r.
- FIRST - międzynarodowe forum zespołów reagujących na incydenty (http://www.first.org/); pełne członkostwo od 1997 r.
- APWG (Antiphishing Working Group) - międzynarodowa grupa robocza podmiotów zainteresowanych walką z cyberprzestępczością (m.in. podmioty akademickie, firmy komercyjne, zespoły reagujące, organizacje płatnicze) (http://www.antiphishing.org): partner badawczo-rozwojowy od 2010 r.
- FI-ISAC (Financial Institutions - Information Sharing and Analysis Centre) - zamknięta grupa podmiotów zainteresowanych zwalczaniem nadużyć w sektorze finansowym; członek od 2008 r.,

Dowód: akta kontroli strony 138–163, 166-203

Zespół CERT Polska nie gromadzi w sposób scentralizowany danych kontaktowych administratorów systemów teleinformatycznych, które pozwalają na wymianę informacji i bieżące koordynowanie działań w sytuacji zagrożenia lub wystąpienia incydentu. W trakcie kontroli zidentyfikowano trzy rozproszone źródła takich danych obejmujące łącznie 180 kontaktów: użytkownicy platformy „n6", członkowie Abuse-Forum oraz osoby, z którymi współpracowano przy obsłudze zgłoszeń, uczestnicy konferencji, warsztatów, szkoleń itp. Kontakty te nie podlegają żadnej selekcji i weryfikacji. Zespół planuje uporządkowanie danych kontaktowych poprzez rozbudowę funkcjonalności platformy „n6".
Zespół CERT Polska nie dysponuje danymi kontaktowymi pełnomocników do spraw bezpieczeństwa powołanych w jednostkach administracji rządowej.
Zespół CERT Polska nie prowadzi działań wspierających tworzenie sektorowych punktów kontaktowych.

Dowód: akta kontroli strony 3-20, 34-44, 47-82, 97-121, 83-98

Ustalone nieprawidłowości

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

1.8. System wczesnego ostrzegania.

Opis stanu faktycznego

Jednym z niewielu miejsc, w których Polityka odnosi się do funkcjonowania NASK jest rozdział dotyczący systemu wczesnego ostrzegania. Wskazano w nim na genezę eksploatowanego obecnie systemu ARAKIS-GOV oraz konieczność dokonania jego rozbudowy. System ten powstał, jako wynik rozpoczętego w 2003r. projektu badawczego ARAKIS oraz potrzeb ABW związanych z koniecznością ochrony systemów i sieci teleinformatycznych administracji publicznej. System został zrealizowany w roku 2005 i od tego czasy eksploatowany jest z wykorzystaniem sprzętu Agencji oraz merytorycznego wsparcia NASK. Pomimo niezmienionych głównych celów projektu ARAKIS-GOV ciągła ewolucja metod i kierunków ataków wymusza nieustanny jego rozwój i dodawanie kolejnych funkcjonalności. W trakcie prac nad powyższymi rozwiązaniami NASK nie stosował formalnych mierników realizacji celów. Obecnie w wyniku wieloletniego wykorzystywania systemu można jednak stwierdzić, że główne cele projektu zostały osiągnięte. Skala zagrożeń wykrywanych przez system jest okresowo publikowana w raportach CERT.GOV.PL i CERT Polska.
W systemie ARAKIS.GOV wyborem lokalizacji i dystrybucją sond zajmuje się CERT.GOV.PL. Po fizycznym zainstalowaniu sond CERT Polska na podstawie otrzymanych z ABW informacji podłącza (konfiguruje połączenia i parametry

w systemie) taką sondę do systemu. Zespół nie zanotował trudności związanych z realizacją projektu ARAKIS.GOV.

Dowód: akta kontroli strony 104-108

Ustalone nieprawidłowości

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

1.9. Szkolenie i działania edukacyjne.

Opis stanu faktycznego

Wiedza z zakresu szeroko rozumianego bezpieczeństwa teleinformatycznego i ochrony cyberprzestrzeni stanowi wiedzę wysoko specjalistyczną. W opinii NASK powyższe może być przyczyną sytuacji, w której, w procesie rekrutacji nowych pracowników na stanowiska związane z kwestiami bezpieczeństwa i ochrony cyberprzestrzeni, NASK napotyka trudności ze znalezieniem kandydatów dysponujących niezbędna wiedzą fachową i doświadczeniem w tym zakresie.
NASK nie uczestniczy samodzielnie, ani we współudziale z innymi podmiotami, w tworzeniu sformalizowanego systemu szkoleń dla specjalistów w obszarze ochrony cyberprzestrzeni. Niemniej jednak, wykorzystując kompetencję i specjalistyczną wiedzę swoich pracowników, opracowuje programy szkoleń i przeprowadza szkolenia dedykowane dla poszczególnych grup odbiorców, takich jak organy wymiaru sprawiedliwości, organy ścigania, pedagodzy, a ponadto organizuje lub współuczestniczy w organizacji konferencji, warsztatów, spotkań dla specjalistów z zakresu bezpieczeństwa IT. W okresie od roku 2012 do czasu zakończenia kontroli NASK przeprowadziła 11 szkoleń, których tematyka dotyczyła szeroko rozumianego bezpieczeństwa w cyberprzestrzeni. Wszystkie organizowane szkolenia, jak również bieżąca działalność NASK, np. w zakresie edukacji komputerowej seniorów i najmłodszych, są podejmowane z inicjatywy NASK i według autorskich koncepcji NASK. NASK nie otrzymywała w tym zakresie wytycznych, zaleceń, itp.

Dowód: akta kontroli strony 129-134

W NASK nie przeprowadza się szkoleń dla własnych pracowników dedykowanych bezpieczeństwu IT. Każdy, rozpoczynając pracę w NASK, otrzymuje podstawowe przeszkolenie w ramach bezpieczeństwa danych, w tym przetwarzanych w systemach teleinformatycznych. Kierownictwo NASK biorąc pod uwagę jej działalność, jako instytutu badawczego, uważa, że w związku z pełnioną przez nią rolą centrum kompetencyjnego zorientowanego na szkolenie innych osób prawnych i fizycznych w zakresie funkcjonowania w cyberprzestrzeni, nie istnieje rzeczywista potrzeba opracowywania systemów szkoleń dla pracowników.

Dowód: akta kontroli strona 132

Od 2005 roku NASK bierze udział w realizacji Programu Komisji Europejskiej Safer Internet, rozpoczętego w 1999 r. i mającego na celu promocję bezpiecznego korzystania z nowych technologii i Internetu wśród dzieci i młodzieży. W ramach programu prowadzone są również działania na rzecz zwalczania nielegalnych treści i spamu w Internecie. Od 2005 r. do programu włączona została problematyka związana z zagrożeniami wynikającymi z użytkowania telefonów komórkowych, gier on-line, wymianą plików P2P i innymi formami komunikacji on-line w czasie rzeczywistym (czaty i komunikatory). Priorytetem programu na lata 2009-2013 było zwalczanie cyberprzemocy i uwodzenia dzieci w Internecie. Polskie Centrum Programu Safer Internet (PCPSI) powołane zostało w 2005 r. tworzą je Fundacja Dzieci Niczyje (FDN) oraz NASK (jako koordynator PCPSI). Centrum podejmuje szereg kompleksowych działań na rzecz bezpieczeństwa dzieci i młodzieży korzystających z Internetu i nowych technologii. Obecnie realizowane są 3 projekty:

- Saferinternet.pl - którego celem jest zwiększanie społecznej świadomości na temat zagrożeń, jakie niosą ze sobą najnowsze techniki komunikacji. Wśród podejmowanych działań priorytetem jest edukacja, zarówno dzieci, jak i rodziców, a także podnoszenie kompetencji profesjonalistów w zakresie bezpiecznego korzystania z Internetu. Projekt realizowany przez FDN i NASK we współpracy z Fundacją Orange.
- Helpline.org.pl - w ramach, którego udzielana jest pomoc młodym internautom, rodzicom i profesjonalistom w przypadkach zagrożeń związanych z korzystaniem z Internetu oraz telefonów komórkowych przez dzieci i młodzież. Projekt realizowany przez FDN oraz Fundację Orange.
- Dyżurnet.pl - punkt kontaktowy, tzw. hotline, do którego można anonimowo zgłaszać przypadki występowania w Internecie treści zabronionych prawem, takich jak pornografia dziecięca, pedofilia, treści o charakterze rasistowskim i ksenofobicznym. Projekt realizowany przez NASK. Współdziałanie narodowych zespołów hotline następuje w ramach stowarzyszenia INHOPE (The Association of Internet Hotline Providers). Należą do niego europejskie zespoły hotline, a także zespoły spoza Europy.

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę, iż niewprowadzenie w NASK wewnętrznego systemu szkoleń z zakresu bezpieczeństwa IT dedykowanego dla poszczególnych grup pracowników wpływa na wzrost ryzyka dotyczącego zasobów i procesów biznesowych tej instytucji. Wprawdzie, jak wskazano w wyjaśnieniach, NASK dysponuje unikalnym poziomem wiedzy w obszarze bezpieczeństwa teleinformatycznego, to jednak wiedza taka nie jest dostępna w równym stopniu dla wszystkich pracowników Instytutu. Jednocześnie zajmowana przez NASK pozycja, pełniona rola oraz podejmowane działania, szczególnie w obszarze bezpieczeństwa, w istotny sposób zwiększają ryzyko skierowania przeciw niej różnorodnych ataków.

[...][6]

Ocena cząstkowa

W okresie objętym kontrolą NASK podejmowała liczne i aktywne działania, które należy zdefiniować, jako dobre praktyki wypływające pozytywnie na stan bezpieczeństwa cyberprzestrzeni RP. Ustalono natomiast, że działania NASK w zakresie bezpieczeństwa teleinformatycznego państwa były ściśle związane z realizowanymi przez ten podmiot procesami biznesowymi i podlegały wynikającym z tego faktu ograniczeniom, w tym finansowym. Należy również wskazać, iż działania NASK (CERT Polska) w znacznym stopniu miały charakter nieformalny i „tymczasowy", co wynikało z dużego dorobku tej instytucji w obszarze bezpieczeństwa IT i jej rozpoznawalności na arenie międzynarodowej, przy jednoczesnym braku formalnego i kompleksowego systemu działań organów państwowych w zakresie ochrony cyberprzestrzeni RP.

IV. Uwagi i wnioski

NIK odstąpiła od formułowania wniosków pokontrolnych.

---

[6] Na podstawie art. 5 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2014 r. poz. 782) i art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U z 2003 r. Nr 153, poz. 1503 ze zm.) NIK wyłączyła jawność informacji w zakresie szkoleń i realizacji umów handlowych. Wyłączenia tego dokonano w interesie przedsiębiorcy.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

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

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

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK proszę o poinformowanie Najwyższej Izby Kontroli, w terminie 21 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag 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 30.09 2014 r.

Najwyższa Izba Kontroli
Departament Porządku
i Bezpieczeństwa Wewnętrznego

Kontroler
Adam Zakrzewski
Główny specjalista kontroli państwowej

Adam Zakrzewski
podpis

Dyrektor
Marek Bieńkowski

Najwyższa Izba Kontroli
Departament Porządku
i Bezpieczeństwa Wewnętrznego

Marek Bieńkowski
podpis