WICEPREZES
NAJWYŻSZEJ IZBY KONTROLI
Wojciech Kutyła

KPB – 4101-002-05/2014
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	Janusz Nowaczyk, doradca techniczny, upoważnienie do kontroli nr 89667 z dnia 9 czerwca 2014 r. (dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Urząd Komunikacji Elektronicznej (zwany dalej UKE), 01-211 Warszawa, ul. Marcina Kasprzaka 18/20
Kierownik jednostki kontrolowanej	Pani Magdalena Gaj, Prezes Urzędu Komunikacji Elektronicznej (dowód: akta kontroli str. 308)

II. Ocena kontrolowanej działalności

Ocena

Kontrola wykazała[1], że Prezes Urzędu Komunikacji Elektronicznej[2] podjęła działania mające na celu wdrożenie postanowień *Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*[3] (zwanej dalej *Polityką*). W szczególności zrealizowano zadania dotyczące oszacowania ryzyk dla systemów teleinformatycznych oraz powołania w Urzędzie Pełnomocnika ds. bezpieczeństwa cyberprzestrzeni. Prowadzono również aktywne działania związane z wprowadzeniem w UKE systemu zarządzania bezpieczeństwem informacji.

W działalności kontrolowanej jednostki stwierdzono natomiast problemy o charakterze systemowym, wskazujące na brak możliwości praktycznego wykorzystania obowiązujących obecnie przepisów Prawa telekomunikacyjnego[4] w ramach realizacji zadań związanych z ochroną cyberprzestrzeni RP. Ustalono bowiem, że przedsiębiorcy telekomunikacyjni nie przekazują Prezesowi UKE (poza pojedynczymi przypadkami) informacji na temat naruszeń bezpieczeństwa, integralności sieci lub usług związanych z incydentami występującymi w cyberprzestrzeni. Wypływało to m.in. negatywnie na możliwość realizacji obowiązków UKE dotyczących informowania o tego typu zdarzeniach i zagrożeniach konsumentów oraz podmiotów realizujących zadania związane z ochroną cyberprzestrzeni. Stwierdzono także, że opracowywane przez przedsiębiorców telekomunikacyjnych plany działań w sytuacjach szczególnych zagrożeń, odnoszą się co do zasady do konwencjonalnych niebezpieczeństw. W związku z tym, nie mogą być one wykorzystywane jako analiza ryzyka oraz procedury reagowania związane ze zdarzeniami występującymi w cyberprzestrzeni.

---

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 12 września 2014 r.

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

4 Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2014 r., poz. 243). Regulacje dotyczące ochrony cyberprzestrzeni zostały zamieszczone w szczególności w Dziale VIIa (art. 175a-175e) oraz Dziale VIII (art. 176a) ww. ustawy.

III. Wyniki kontroli

1. Zasoby UKE do realizacji zadań związanych z ochroną cyberprzestrzeni RP.

Opis stanu faktycznego

Zadania UKE, w zakresie ochrony cyberprzestrzeni RP, były realizowane w obszarze wewnętrznym dotyczącym zapewnienia ciągłości funkcjonowania i bezpieczeństwa teleinformatycznego Urzędu oraz w obszarze zewnętrznym, obejmującym w szczególności zbieranie i analizowanie informacji na temat zagrożeń w sieciach przedsiębiorców telekomunikacyjnych.

W ramach struktury UKE można wyróżnić trzy komórki organizacyjne uczestniczące w realizacji zadań związanych z ochroną cyberprzestrzeni RP:

1. Departament Spraw Obronnych realizuje m.in. zadania związane ze zbieraniem przekazywanych przez przedsiębiorców telekomunikacyjnych informacji o przypadkach wystąpienia naruszenia bezpieczeństwa lub integralności sieci lub usług, analizą istotności i charakteru naruszeń, przygotowaniem informacji o wystąpieniu naruszenia w celu przekazania organom regulacyjnym innych państw członkowskich UE i ENISA[5] oraz przygotowaniem do publikacji na stronie internetowej Urzędu informacji o wystąpieniu naruszenia bezpieczeństwa lub integralności sieci lub usług. Dyrektor Departamentu Spraw Obronnych został również zobowiązany[6] do koordynowania współpracy w zakresie bezpieczeństwa cyberprzestrzeni pomiędzy UKE a przedsiębiorcami telekomunikacyjnymi i użytkownikami cyberprzestrzeni RP.
2. Biuro Informatyki realizuje zadania związane m.in. z koordynowaniem budowy i wdrażania systemów informatycznych Urzędu oraz zarządzaniem zasobami informatycznymi UKE zgodnie z wymogami polityki bezpieczeństwa.
3. Biuro Dyrektora Generalnego koordynuje zadania w obszarze zapewnienia funkcjonowania systemu kontroli zarządczej w UKE, w tym w uzgodnieniu z Biurem Informatyki, prowadzi analizę ryzyka z zakresu bezpieczeństwa cyberprzestrzeni.

W styczniu 2007 r. utworzono Stały Dyżur Prezesa UKE, funkcjonujący w ramach systemu 24-godzinnych stałych dyżurów[7]. Zadaniem służby dyżurnej jest m.in. utrzymywanie stałego kontaktu z przedsiębiorcami telekomunikacyjnymi w celu wzajemnego przekazywania informacji, alarmowania i ostrzegania w sytuacji szczególnego zagrożenia, przyjmowanie informacji o zdarzeniach nadzwyczajnych mających istotny wpływ na infrastrukturę telekomunikacyjną przedsiębiorców oraz ciągłość świadczenia usług, jak również realizowanie zadań związanych z podwyższaniem obronności państwa.

(dowód: akta kontroli str. 283-293, 681, 826)

W dniu 9 kwietnia 2014 r. Prezes UKE wyznaczył Dyrektora Biura Informatyki na stanowisko Pełnomocnika do spraw bezpieczeństwa cyberprzestrzeni Urzędu Komunikacji Elektronicznej. Do zadań Pełnomocnika należy m.in. opracowanie i wdrożenie procedur reagowania na incydenty komputerowe, identyfikowanie i prowadzenie cyklicznych analiz ryzyka, przygotowanie planów awaryjnych oraz ich testowanie.

(dowód: akta kontroli str. 309-314, 771-796)

---

[5] Europejska Agencja do spraw Bezpieczeństwa Sieci i Informacji.

[6] Na podstawie Zarządzenia Nr 16 Dyrektora Generalnego UKE z dnia 8 lipca 2014 r. w sprawie wprowadzenia *Zasad ochrony cyberprzestrzeni* oraz powołania *Zespołu do monitorowania ich realizacji* (zarządzenie niepublikowane).

[7] System stałych dyżurów utworzono na podstawie rozporządzenia Rady Ministrów z dnia 21 września 2004 r. w sprawie gotowości obronnej państwa (Dz. U. z 2004 r. Nr 219, poz. 2218) oraz zarządzenia Nr 15 Ministra Administracji i Cyfryzacji z dnia 1 sierpnia 2013 r. w sprawie systemu stałego dyżuru (Dz. Urz. z 2013 r., Nr 27).

W latach 2012-2014 r.[8] wydatki UKE na zakup sprzętu i oprogramowania komputerowego wykorzystywanych do zabezpieczenia systemów teleinformatycznych Urzędu wyniosły 1 781,4 tys. zł. Stwierdzono natomiast, że wg stanu na dzień 18 lipca 2014 r. w UKE nie przeprowadzono kompleksowego szacowania wszystkich zasobów oraz wydatków związanych z ochroną cyberprzestrzeni RP. Przedmiotowe wydatki nie były odrębnie ewidencjonowane, ani wydzielane w ramach planu finansowego Urzędu[9]. W związku z powyższym nie zrealizowano obowiązków określonych w pkt 5. *Polityki* dotyczących 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.

Kierownictwo UKE nie występowało do Ministerstwa Administracji i Cyfryzacji (MAiC) o wytyczne dotyczące planowania wydatków ponoszonych w związku z bezpieczeństwem cyberprzestrzeni.

Prezes UKE wyjaśniła, że w związku z tym, że koszty zdeterminowane są wynikami szacowania ryzyka, informacja na temat zrealizowanych zadań oraz wydatków poniesionych na ochronę cyberprzestrzeni w Urzędzie, zostanie przesłana do MAiC po akceptacji przez Ministerstwo wyników szacowania ryzyka i zakończeniu roku budżetowego 2014 r.

(dowód: akta kontroli str. 10, 806-807)

W trakcie trwania kontroli NIK, Dyrektor Generalny UKE wydał zarządzenie w sprawie wprowadzenia *Zasad ochrony cyberprzestrzeni* oraz powołania Zespołu do monitorowania ich realizacji. Zadaniem Zespołu jest między innymi określenie kosztów niezbędnych do realizacji zadań dotyczących bezpieczeństwa cyberprzestrzeni, koniecznych do ujęcia w budżecie UKE na rok 2015.

(dowód: akta kontroli str. 351-356)

Ustalone nieprawidłowości

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

Uwagi dotyczące badanej działalności

NIK zwraca uwagę, że oszacowanie zasobów i wydatków poszczególnych instytucji realizujących zadania w zakresie bezpieczeństwa teleinformatycznego państwa, jest podstawowym elementem budowy systemu ochrony cyberprzestrzeni RP. Ze względu na fakt, że ww. zadania mają nowatorski charakter oraz są realizowane przez komórki organizacyjne i pracowników UKE równolegle z innymi obowiązkami służbowymi, oszacowanie zasobów i wydatków może być nieprecyzyjne i obarczone znacznym błędem. W związku z powyższym, w celu rzetelnego wykonania obowiązków określonych w pkt 5. *Polityki*, zasadne wydaje się wystąpienie do Ministra Administracji i Cyfryzacji o przedstawienie wytycznych w zakresie ewidencjonowania i szacowania zasobów oraz wydatków związanych z ochroną cyberprzestrzeni, a także trybu przekazywania tych informacji do MAiC.

Ocena cząstkowa

Kontrola wykazała, że zgodnie z zapisami *Polityki*, w UKE powołano Pełnomocnika ds. bezpieczeństwa cyberprzestrzeni, odpowiadającego za ochronę teleinformatyczną Urzędu. Pozostałe zadania UKE związane z ochroną cyberprzestrzeni (w tym dotyczące zbierania i analizy informacji o naruszeniach bezpieczeństwa lub integralności sieci lub usług) były realizowane przez komórki organizacyjne i pracowników Urzędu równolegle z innymi obowiązkami służbowymi. W UKE nie przeprowadzono kompleksowego szacowania zasobów oraz wydatków związanych

[8] Wg stanu na dzień 24 czerwca 2014 r.

[9] Można je wyróżnić jedynie poprzez analizę opisu operacji księgowej.

z ochroną cyberprzestrzeni RP, natomiast działania mające na celu ich zwymiarowanie zostały rozpoczęte w trakcie kontroli NIK.

2. Realizacja zadań UKE wynikających z *Polityki ochrony cyberprzestrzeni RP.*

Opis stanu faktycznego

W lutym 2014 r. UKE został poinformowany pismem MAiC[10], o przyjęciu przez Radę Ministrów w dniu 25 czerwca 2013 r. dokumentu *Polityka ochrony cyberprzestrzeni Rzeczpospolitej Polskiej*. Jak wyjaśniła Prezes UKE, ze względu na charakter dokumentu oraz sposób jego wprowadzenia, w UKE uznano, *(...) iż Polityka nie ma formy powszechnie obowiązującego aktu prawnego, a jedynie zbioru norm, wytycznych oraz dobrych praktyk możliwych do zastosowania w celu realizacji zadań dotyczących ochrony cyberprzestrzeni Rzeczypospolitej Polskiej. Powyższy dokument nie zawiera informacji dotyczących m.in. analizy skutków wprowadzenia regulacji oraz nie przewiduje przyznania dodatkowych środków finansowych w celu realizacji zawartych w nim założeń. W związku z tym podjęto działania mające na celu wdrożenie zaleceń i rekomendacji, w ramach własnych środków finansowych przewidzianych na rozwój lub zakup systemów teleinformatycznych, jak również w ramach kontynuacji dotychczasowej aktywności UKE w obszarze ochrony cyberprzestrzeni.*

(dowód: akta kontroli str. 6)

W ramach realizacji obowiązków wynikających z *Polityki* w UKE realizowano następujące zadania:

- zgodnie z zapisami pkt 3.1. *Polityki* przeprowadzono szacowanie ryzyka związanego z funkcjonowaniem cyberprzestrzeni. Szacowanie ryzyka zostało zrealizowane w oparciu o metodykę otrzymaną w lutym 2014 r. z MAiC i obejmowało systemy teleinformatyczne niezbędne do prawidłowego funkcjonowania UKE. Zidentyfikowano 13 systemów teleinformatycznych, z których 5 określonych zostało jako krytyczne zasoby teleinformatyczne. Identyfikacja ryzyka uwzględniała m.in.: atak zewnętrzny ograniczający dostęp typu DDos, atak socjotechniczny w celu przejęcia danych (phishing), zainstalowanie złośliwego oprogramowania poprzez korespondencję elektroniczną. Wyniki szacowania ryzyka zostały przesłane w dniu 9 kwietnia 2014 r. do MAiC. W piśmie przekazującym wyniki, UKE zwrócił uwagę, iż kluczową rolę w szacowaniu ryzyka powinni pełnić *gestorzy* systemów informatycznych, którzy posiadają niezbędną wiedzę i doświadczenie związane z używaniem danych systemów. Natomiast w procesie wprowadzania mechanizmów zapobiegających materializacji ryzyk kluczową rolę odgrywać powinni pełnomocnicy do spraw bezpieczeństwa cyberprzestrzeni, których odpowiednie umocowanie w organizacji oraz wiedza i doświadczenie pozwolą na sprawną realizację tych zadań;

  (dowód: akta kontroli str.15-37,309, 315-350, 806)

- zgodnie z pkt 3.4.2. *Polityki*, od czwartego kwartału 2013 r., w UKE prowadzone były prace mające na celu wdrożenie kompleksowego systemu zarządzania bezpieczeństwem informacji. W ramach ww. zadania przeprowadzony został, przez konsultantów zewnętrznych audyt, który miał na celu identyfikację niezbędnych działań dotyczących przygotowania UKE do wdrożenia i certyfikacji systemu zarządzania bezpieczeństwem informacji, zgodnie z wymaganiami normy ISO/IEC 27001:2005. Opracowano również wewnętrzne regulacje dotyczące bezpieczeństwa teleinformatycznego, tj.: *Politykę ochrony*

[10] Pismo z dnia 13 lutego 2014 r. Pana Romana Dmowskiego, Podsekretarza Stanu w Ministerstwie Administracji i Cyfryzacji (znak: DSI-WSE.550.1.2014.JŁ).

cyberprzestrzeni Urzędu Komunikacji Elektronicznej[11] oraz procedurę *Zarządzania Incydentami Komputerowymi*, określającą zasady reagowania na incydenty komputerowe oraz współpracy z CERT[12].

(dowód: akta kontroli str. 3, 15-37, 566, 644-648)

- na podstawie pkt 3.4.3. *Polityki* w UKE wyznaczony został Pełnomocnik ds. bezpieczeństwa cyberprzestrzeni.

(dowód: akta kontroli str. 309-314, 771-796)

W UKE nie zrealizowano zadania określonego w pkt 6. *Polityki* dotyczącego przekazania Ministrowi Administracji i Cyfryzacji, w ciągu roku od wejścia w życie tego dokumentu, informacji o przyjętych i osiągniętych procentowych wskaźnikach realizacji zadań Urzędu w obszarze ochrony cyberprzestrzeni.

Prezes UKE wyjaśniła, że nie opracowano dotychczas mierników oceny skuteczności zadań realizowanych w ramach ochrony cyberprzestrzeni RP. Wskazała, że widzi możliwość przyjęcia mierników zaprezentowanych w *Polityce* za docelowe w obszarze działalności UKE, jednakże decyzje w tym zakresie uwarunkowane są otrzymaniem z MAiC oceny oraz wniosków i zaleceń wynikających z dokonanego szacowania ryzyka dla systemów teleinformatycznych Urzędu.

W trakcie trwania kontroli NIK, Dyrektor Generalny UKE wydał zarządzenie w sprawie wprowadzenia *Zasad ochrony cyberprzestrzeni oraz powołania Zespołu do monitorowania ich realizacji.* Zadaniem Zespołu jest m.in. opracowanie mierników umożliwiających ocenę skuteczności zadań UKE realizowanych w obszarze ochrony cyberprzestrzeni.

(dowód: akta kontroli str. 6, 351-356, 433-434, 567)

W UKE nie zrealizowano zadań wymienionych w pkt 5. *Polityki* dotyczących przekazania Ministrowi Administracji i Cyfryzacji informacji na temat wykonanych dotychczas zadań związanych z ochroną cyberprzestrzeni oraz wydatków poniesionych i planowanych na ich realizację (opisano szczegółowo w pkt III.1. wystąpienia pokontrolnego).

Ustalone nieprawidłowości

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

Uwagi dotyczące badanej działalności

NIK zwraca uwagę, iż brak określenia wskaźników realizacji zadań UKE w zakresie bezpieczeństwa teleinformatycznego wskazuje na problem związany ze zdefiniowaniem faktycznej roli Prezesa Urzędu Komunikacji Elektronicznej w budowanym systemie ochrony cyberprzestrzeni RP. Zdaniem NIK, szczególna rola UKE w ramach ww. systemu powinna wynikać z przepisów Prawa telekomunikacyjnego, określających uprawnienia Prezesa UKE wobec przedsiębiorców telekomunikacyjnych oraz obowiązki wobec konsumentów. W powyższym zakresie zasadne jest więc przeprowadzenie rzetelnej analizy, m.in. we współpracy z Ministrem Administracji i Cyfryzacji, w celu określenia zadań UKE w związku z ochroną cyberprzestrzeni RP.

Ocena cząstkowa

Kontrola wykazała, że w UKE zrealizowano większość zadań nałożonych na ten podmiot na podstawie *Polityki*, tj.: przeprowadzono szacowanie ryzyka odnośnie zasobów teleinformatycznych Urzędu, wyznaczono Pełnomocnika ds. bezpieczeństwa cyberprzestrzeni oraz prowadzone były aktywne prace mające na celu wdrożenie systemu zarządzania bezpieczeństwem informacji. Nie zrealizowano

[11] Dokument zatwierdzony przez Prezes UKE w dniu 28 lutego 2014 r.

[12] Procedura zatwierdzona w dniu 28 lipca 2014 r. przez Dyrektora Biura Informatyki UKE. Odrębne procedury zawarto w dokumencie *Zarządzanie incydentami bezpieczeństwa* w zakresie funkcjonowania niezależnego systemu Platformy Lokalizacyjno-Informacyjnej z Centralną Bazą Danych UKE.

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.

3. Realizacja zadań związanych z ochroną cyberprzestrzeni RP, wynikających z ustawy Prawo telekomunikacyjne.

Opis stanu faktycznego

3.1 Informacje o naruszeniach bezpieczeństwa lub integralności sieci i usług związanych z incydentami występującymi w cyberprzestrzeni.

Na podstawie art. 175a. ust. 1 Prawa telekomunikacyjnego, przedsiębiorcy telekomunikacyjni są obowiązani niezwłocznie informować Prezesa UKE o naruszeniu bezpieczeństwa lub integralności sieci lub usług, które miało istotny wpływ na funkcjonowanie sieci lub usług, o podjętych działaniach zapobiegawczych i środkach naprawczych oraz o podjętych przez przedsiębiorcę działaniach mających na celu zapewnienie bezpieczeństwa i integralności sieci i usług. Prezes UKE, w przypadku gdy uzna charakter naruszenia za istotny, informuje o jego wystąpieniu organy regulacyjne innych państw członkowskich UE i ENISA oraz (jeżeli uzna, że leży to w interesie publicznym) publikuje informacje o zdarzeniu na stronie internetowej UKE lub nakłada na przedsiębiorcę telekomunikacyjnego, w drodze decyzji, obowiązek jej podania do publicznej wiadomości (art. 175b ust. 1 i 2 ww. ustawy).

W okresie od dnia wejścia w życie ww. przepisów (22 marca 2013 r.) do dnia 30 czerwca 2014 r. przedsiębiorcy telekomunikacyjni poinformowali Prezesa UKE o 474 naruszeniach bezpieczeństwa lub integralności sieci i usług (z tego 295 zgłoszeń w 2013 r. i 179 w pierwszym półroczu 2014 r.). Praktycznie wszystkie zgłoszenia – 459 (96,8%) zostały przekazane przez firmę ORANGE[13], co wynikało z faktu, że podmiot ten obsługuje połączenia na numery alarmowe, których niedostępność podlega obligatoryjnemu zgłaszaniu, niezależnie od liczby użytkowników, których to zdarzenie dotyczy[14]. Najczęstszymi przyczynami naruszeń zgłaszanych do UKE były awarie techniczne sprzętu lub oprogramowania oraz zdarzenia losowe niezwiązane z działalnością intencjonalną (81%). Zdecydowana większość zdarzeń (około 97%) dotyczyła niedostępności usług telefonii stacjonarnej.

W przypadku 4 naruszeń bezpieczeństwa zgłoszonych przez przedsiębiorców telekomunikacyjnych[15], Prezes UKE, działając na podstawie art. 175b ust. 1 Prawa telekomunikacyjnego zastosowała procedurę informowania państw członkowskich UE i ENISA[16]. W okresie objętym kontrolą, Prezes UKE nie korzystał natomiast z uprawnień określonych w art. 175b ust. 2 ww. ustawy, dotyczących publikowania informacji o naruszeniach bezpieczeństwa na stronie internetowej UKE lub nakładania obowiązku publikowania tych informacji na przedsiębiorców telekomunikacyjnych. Jak wyjaśniła Prezes UKE, charakter naruszeń zgłoszonych przez przedsiębiorców nie wskazywał, że obowiązek publikacji informacji leży w interesie publicznym. Dotyczyły one w zdecydowanej większości awarii technicznych, spowodowanych zdarzeniami o charakterze losowym, pozostających bez wpływu na bezpieczeństwo sieci i usług.

(dowód: akta kontroli str. 8-9, 12-13, 55-75, 305, 367)

---

[13] Pozostałe zgłoszenia zostały przekazane przez: Polkomtel – 3, T-Mobile – 2, Netia – 1, Multimedia Polska – 5, Moberia – 1, P4 – 1, ZU Pawluk – 1, MSM Toruń – 1.

[14] Zgodnie z wzorem zgłoszenia określonym w rozporządzeniu Ministra Administracji i Cyfryzacji z dnia 19 marca 2013 r. w sprawie wzoru formularza do przekazywania informacji o naruszeniu bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych, które miało istotny wpływ na funkcjonowanie sieci lub usług (Dz. U. z 2013 r., poz. 386). Wzór zgłoszenia określony w ww. rozporządzeniu został uzupełniony poprzez opracowanie przez UKE dodatkowego formularza (zamieszczonego na stronie internetowej UKE) zawierającego informacje dotyczące przyczyn naruszenia, wśród których wymieniono m.in. cyberatak na infrastrukturę lub usługi.

[15] Przyczyną naruszeń były awarie sprzętu i oprogramowania oraz przerwy w zasilaniu energetycznym sprzętu.

[16] W UKE przyjęto w ww. zakresie kryteria informowania o naruszeniach, zawarte w wytycznych ENISA Technical guidance on the incident reporting in Article 13a (Version 2.0, January 2013).

Z łącznej liczby 474 informacji o naruszeniach bezpieczeństwa lub integralności sieci i usług otrzymanych przez UKE, tylko 5 zgłoszeń dotyczyło incydentów bezpieczeństwa związanych z cyberprzestrzenią (z tego 1 zgłoszenie z 2013 r.[17] oraz 4 zgłoszenia z pierwszej połowy 2014 r.[18]).

(dowód: akta kontroli str. 80-91, 172-175, 367-377, 438-475)

Odnośnie działań podejmowanych przez UKE w celu pozyskiwania informacji na temat naruszeń bezpieczeństwa lub integralności sieci i usług związanych z incydentami występującymi w cyberprzestrzeni, Prezes UKE wskazała, że w obecnym brzmieniu art. 175a ust. 1 Prawa telekomunikacyjnego daje przedsiębiorcom telekomunikacyjnym pełną swobodę w zakresie oceny istotności incydentów i zasadności ich zgłaszania do UKE. Podała również, że ustawodawca nie pozostawił kompetencji Prezesowi UKE do władczego wkraczania w ocenę zgłoszeń sporządzanych przez przedsiębiorcę, a tym samym oceny ich rzetelności, co wynika z braku szczegółowych norm prawnych, w tym zakresie.

(dowód: akta kontroli str. 91)

W dniu 11 kwietnia 2014 r., w ramach realizacji obowiązku określonego w art. 175b ust. 4 Prawa Telekomunikacyjnego, przekazany został Ministrowi Administracji i Cyfryzacji *Raport Prezesa Urzędu Komunikacji Elektronicznej o zgłoszonych w 2013 r. zagrożeniach i podjętych przez przedsiębiorców telekomunikacyjnych działaniach zapobiegawczych i środkach naprawczych w zakresie bezpieczeństwa lub integralności sieci lub informacji.* W konkluzjach do Raportu wskazano m.in., iż w ocenie UKE, ustalona w Prawie telekomunikacyjnym zasada, że ocena istotności naruszenia bezpieczeństwa lub integralności sieci lub usług należy do przedsiębiorców, skutkuje fakultatywnością zgłoszeń i powoduje różnorodność kryteriów oceny zdarzeń stosowanych przed przedsiębiorców. Zgodnie z oceną UKE wyrażoną w ww. Raporcie *(...) zmiany wymaga art. 175a ust. 1 ustawy Prawo telekomunikacyjne poprzez nałożenie na przedsiębiorców telekomunikacyjnych bezwzględnego obowiązku informowania o naruszeniach według określonego kryterium (progów zgłoszeń). Ocena istotności naruszenia powinna być tylko w części oceną własną przedsiębiorcy. Po spełnieniu progów zgłoszeń obowiązek informowania o nich powinien być bezwzględny. Ponadto w wyniku braku jednorodnej metodologii szacowania przez przedsiębiorców liczby użytkowników, na których wpływ mają poszczególne naruszenia, za celowe uważa się również w UKE rozpoczęcie prac nad wypracowaniem jednej, wspólnej dla wszystkich przedsiębiorców metody szacowania liczby użytkowników dotkniętych naruszeniem.*

W maju 2014 r. z inicjatywy MAiC, jako organu posiadającego inicjatywę legislacyjną, odbyło się spotkanie z udziałem pracowników Departamentu Spraw Obronnych UKE, na którym omówiono prawne i praktyczne aspekty realizacji obowiązków informacyjnych, określonych w art. 175a i 175b Prawa telekomunikacyjnego.

(dowód: akta kontroli str. 79-91,305-306, 808)

Ustalone nieprawidłowości

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

Uwagi dotyczące badanej działalności

NIK zwraca uwagę, iż w związku ze wzrostem zagrożeń związanych z incydentami i działalnością przestępczą w cyberprzestrzeni, w celu wdrożenia skutecznych mechanizmów zapobiegania i ograniczania ich wpływu, istotne jest zbudowanie systemu pozyskiwania wiedzy o takich zdarzeniach, mających wpływ na

[17] Zgłoszenie dotyczyło ataku *SYN Flood* (którego celem jest głównie zablokowanie usług serwera), trwającego 17 minut i dotyczącego 2 338 użytkowników.

[18] Zgłoszenia zostały dokonane w lutym 2014 r. przez czterech przedsiębiorców telekomunikacyjnych i dotyczyły ataków na urządzenia dostępowe (router) użytkowników końcowych sieci Internet. Skutkami incydentów była niedostępność lub niepełna dostępność sieci lub usług trwająca od 1,3 godz. do 23,15 godz. dotycząca łącznej liczby 441,5 tys. abonentów.

bezpieczeństwo sieci i usług. Zdaniem NIK, zasadne jest więc wdrożenie aktywnej współpracy między UKE i MAiC w celu opracowania propozycji stosownych zmian legislacyjnych (obejmujących w szczególności przepisy Działu VIIa Prawa Telekomunikacyjnego), które pozwolą określić precyzyjne kryteria i obowiązki w zakresie informowania o tego rodzaju incydentach.
W ocenie NIK, ustanowienie jednoznacznych obowiązków w zakresie informowania o incydentach, zapewni również możliwość rzetelnej realizacji pozostałych obowiązków UKE, w obszarze ochrony cyberprzestrzeni, wymienionych w art. 175e. ust. 1. Prawa telekomunikacyjnego (opisano szczegółowo w pkt III.3.3.2 wystąpienia).

3.2 Realizacja obowiązku wymienionego w art. 175e ust. 1 Prawa telekomunikacyjnego w kontekście zagrożeń związanych z cyberprzestrzenią.

Zgodnie z art. 175e ust. 1 pkt 1-3 Prawa telekomunikacyjnego, Prezes UKE publikuje na stronie internetowej UKE aktualne informacje o: potencjalnych zagrożeniach związanych z korzystaniem przez abonentów z usług telekomunikacyjnych, rekomendowanych środkach ostrożności i najbardziej popularnych sposobach zabezpieczania telekomunikacyjnych urządzeń końcowych przed oprogramowaniem złośliwym lub szpiegującym, przykładowych konsekwencjach braku lub nieodpowiedniego zabezpieczenia telekomunikacyjnych urządzeń końcowych.

Opis stanu faktycznego

W okresie od dnia wyjścia w życie ww. przepisu, tj. od 22 marca 2013 r. do 25 lipca 2014 r. na stronach internetowych UKE opublikowano jeden poradnik zawierający m.in. informacje na temat zagrożeń związanych z korzystaniem przez abonentów z Internetu oraz podstawowych, rekomendowanych środków ostrożności - pt. *Bądź świadomy zagrożeń w sieci*[19]. Ww. poradnik został opracowany we wrześniu 2013 r. i od momentu publikacji nie podlegał aktualizacjom. Ustalono również, że nie został on zamieszczony na głównej stronie internetowej UKE, a dotarcie do niego było utrudnione, ponieważ wymagało otwierania kolejnych zakładek na stronach internetowych Urzędu.

Prezes UKE wyjaśniła, iż w związku z faktem, że UKE nie otrzymuje w praktyce informacji od przedsiębiorców telekomunikacyjnych na temat incydentów bezpieczeństwa związanych z cyberprzestrzenią, ww. poradnik został opracowany m.in. w oparciu o dane uzyskiwane w drodze korespondencji wymienianej przy różnych okazjach z abonentami i przedsiębiorcami, informacje z Infolinii Centrum Informacji Konsumenckiej oraz monitoring mediów prowadzony przez pracowników Urzędu.
Wyjaśniła, że nie aktualizowano poradnika, ponieważ nie stwierdzono takiej potrzeby.
Prezes UKE wskazała również, że ze względu na konieczność publikowania dużej liczby obligatoryjnych i istotnych dla rynku telekomunikacyjnego i pocztowego komunikatów, nie ma możliwości publikowania wszystkich informacji na głównej stronie internetowej Urzędu.

(dowód: akta kontroli str. 92-156, 562-563, 807-808)

Ustalone nieprawidłowości

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

Uwagi dotyczące badanej działalności

NIK zwraca uwagę, iż w obowiązującym obecnie porządku prawnym, UKE jest jedynym organem państwowym, docierającym bezpośrednio do konsumentów z informacjami na temat zagrożeń związanych z korzystaniem z Internetu, ich potencjalnych skutków i środków ochrony (w przeciwieństwie np. do publikacji zespołów CERT[20], które docierają raczej do osób zawodowo zajmujących się

[19] Pozostałe opracowania sporządzone prze UKE w związku z realizacją obowiązków wynikających z art. 175e ust. 1 Prawa telekomunikacyjnego nie odnosiły się do bezpiecznego korzystania z Internetu i dotyczyły wyłącznie usług telefonii komórkowej i stacjonarnej, tj.: *Poradnik dla użytkowników usług telekomunikacyjnych* z 25 czerwca 2014 r., materiał pt. *UKE ostrzega - jak rozpoznać kosztownego sms-a* z października 2013 r., materiał pt. *UKE ostrzega - oddzwaniaj z głową* z października 2013 r.

[20] Computer emergency response team – Zespół reagowania na incydenty komputerowe.

bezpieczeństwem IT). Powyższe, zdaniem NIK, uzasadnia potrzebę bardziej aktywnych działań UKE w zakresie dostarczania użytkownikom Internetu aktualnych i łatwo dostępnych informacji wymienionych w art. 175e ust. 1 Prawa telekomunikacyjnego. Należy przy tym podkreślić, że warunkiem rzetelnej realizacji ww. zadania, jest dysponowanie przez UKE wiedzą na temat incydentów występujących w cyberprzestrzeni, pochodzącą z informacji przekazywanych przez przedsiębiorców telekomunikacyjnych (opisano szczegółowo w pkt III.3.3.1 wystąpienia).

3.3 Plany przedsiębiorców telekomunikacyjnych w sytuacjach szczególnych zagrożeń.

Na podstawie art. 176a ust. 1 i 2 Prawa telekomunikacyjnego, przedsiębiorcy telekomunikacyjni, w celu zapewnienia ciągłości świadczenia usług telekomunikacyjnych lub dostarczania sieci telekomunikacyjnej, są zobowiązani uwzględniać możliwość wystąpienia: sytuacji kryzysowych, stanów nadzwyczajnych, bezpośrednich zagrożeń dla infrastruktury przedsiębiorcy oraz posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń.

W wyniku badania 9 planów sporządzonych i przekazanych do UKE przez największych przedsiębiorców telekomunikacyjnych[21] ustalono, że w ww. dokumentach w ogóle nie wskazywano zagrożeń związanych ze zdarzeniami występującymi w cyberprzestrzeni (4 plany) lub wskazywano takie zagrożenia, ale nie zawarto adekwatnych do nich zabezpieczeń infrastruktury telekomunikacyjnej, procedur reagowania oraz struktur organizacyjnych przedsiębiorcy obowiązujących w przypadku wystąpienia zagrożeń związanych ze zdarzeniami występującymi w cyberprzestrzeni (4 plany)[22]. Ponadto, jeden z przedsiębiorców wskazał, że ataki cybernetyczne nie stanowią zagrożenia dla jego infrastruktury, ponieważ jego zdaniem została ona fizycznie odseparowana od innych sieci i Internetu. Analizy zagrożeń sporządzane przez przedsiębiorców telekomunikacyjnych odnosiły się do konwencjonalnych niebezpieczeństw pochodzenia naturalnego (powodzie, pożary, śnieżyce, silne wiatry), katastrof technologicznych (skażenia przemysłowe i promieniotwórcze), katastrof komunikacyjnych (drogowe, budowlane), napadów, włamań oraz aktów terroru z wykorzystaniem przemocy fizycznej. Adekwatnie do tych zagrożeń w planach opisywano tradycyjne, fizyczne zabezpieczenia infrastruktury telekomunikacyjnej oraz standardowe procedury reagowania nie odnoszące się bezpośrednio do bezpieczeństwa teleinformatycznego.

Z udzielonych przez przedsiębiorców telekomunikacyjnych wyjaśnień wynika, że zagrożenie tzw. cyberatakiem dla własnej infrastruktury telekomunikacyjnej postrzegane jest przez nich głównie w aspekcie technicznym. Stąd niezależnie, czy nieprawidłowe działanie sieci teleinformatycznych wynika ze zdarzeń w cyberprzestrzeni, czy też np. z awarii technicznej, wypadku lub aktu wandalizmu, wykorzystane zostaną te same struktury organizacyjne przedsiębiorstwa, środki techniczne i procedury reagowania[23].

(dowód: akta kontroli str.495-524, 693-694, 699, 810, 846-854)

W wyniku analizy dokumentacji dotyczącej procesu uzgadniania objętych badaniem planów ogólnych stwierdzono również, że Szef Agencji Bezpieczeństwa

---

[21] Badaniem objęto wszystkie plany ogólne sporządzone przez największych ogólnopolskich przedsiębiorców telekomunikacyjnych, wymienionych 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 ze zm.).

[22] Tj. elementów wymienionych w § 5 pkt 11 i 12 Rozporządzenie Rady Ministrów z dnia 4 stycznia 2010 r. w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń (Dz. U. z 2010 r. Nr 15, poz. 77.).

[23] NIK nie przeprowadzała u poszczególnych przedsiębiorców telekomunikacyjnych kontroli w zakresie realizacji zadań związanych z ochroną cyberprzestrzeni. Wyjaśnienia dotyczące planów działania w sytuacjach szczególnych zagrożeń zostały uzyskane w trybie art. 29 ust. 1 pkt 2 lit. f ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2012 r., poz. 82 ze zm.)

Wewnętrznego i Minister Spraw Wewnętrznych, którzy powinni przekazywać przedsiębiorcom telekomunikacyjnym informacje służące identyfikacji ryzyk dla ich działalności[24], nie wskazywali im żadnych zagrożeń związanych ze zdarzeniami występującymi w cyberprzestrzeni. Na potrzeby sporządzenia planów ogólnych, Ministerstwo Spraw Wewnętrznych przekazywało przedsiębiorcom coroczną *Ocenę zagrożenia bezpieczeństwa powszechnego w Polsce*, sporządzaną przez Biuro Rozpoznawania Zagrożeń Komendy Głównej Straży Pożarnej, odnoszącą się wyłącznie do zagrożeń konwencjonalnych (powodzie, trzęsienia ziemi, itd.).

Minister Spraw Wewnętrznych wyjaśnił, że obowiązujące przepisy (...) nie nakładają *wprost na organ obowiązku przekazywania przedsiębiorcom telekomunikacyjnym informacji na temat zagrożeń związanych ze zdarzeniami występującymi w cyberprzestrzeni.*

Szef Agencji Bezpieczeństwa Wewnętrznego wskazał, że w jego opinii brak jest unormowań prawnych dotyczących przekazywania przez ABW przedsiębiorcom telekomunikacyjnym informacji dotyczących zagrożeń występujących w cyberprzestrzeni na potrzeby sporządzenia planów działania w sytuacjach szczególnych zagrożeń.

(dowód: akta kontroli str. 693-694, 699)

Odnośnie działań podejmowanych przez UKE w celu uwzględniania przez przedsiębiorców telekomunikacyjnych w planach działania, zagrożeń związanych z cyberprzestrzenią, Prezes UKE wskazała, że na podstawie obowiązujących przepisów nie posiada uprawnień w ww. zakresie.

(dowód: akta kontroli str.809-910)

Ustalone nieprawidłowości

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

Uwagi dotyczące badanej działalności

NIK zwraca uwagę, że opracowywane przez przedsiębiorców telekomunikacyjnych plany ogólne działań w sytuacjach szczególnych zagrożeń w przeważającym stopniu odnoszą się do konwencjonalnych niebezpieczeństw i nie odzwierciedlają dynamicznie postępującej zmiany charakteru zagrożeń, związanej z rozwojem nowoczesnych technologii IT. Plany te mają bardzo ograniczone zastosowanie w kontekście analizy ryzyka i opracowanych na jej podstawie procedur reagowania kryzysowego związanych ze zdarzeniami występującymi w cyberprzestrzeni. Zasadne jest więc przeprowadzenie pogłębionej analizy dot. sposobu ich tworzenia (w szczególności definiowania zagrożeń) oraz zawartości tych dokumentów, tak aby zapewnić możliwość ich realnego wykorzystania, w tym w sytuacjach zagrożeń związanych z cyberprzestrzenią.

Ocena cząstkowa

Kontrola wykazała, że UKE realizował, wynikające z Prawa telekomunikacyjnego, zadania dotyczące zbierania i analizowania informacji o naruszeniach bezpieczeństwa lub integralności sieci lub usług, informowania konsumentów o zagrożeniach oraz uzgadniania planów przedsiębiorców telekomunikacyjnych w sytuacjach szczególnych zagrożeń. W działalności kontrolowanej jednostki stwierdzono natomiast problemy o charakterze systemowym wskazujące na brak możliwości praktycznego wykorzystania przepisów ww. ustawy w ramach realizacji zadań związanych z ochroną cyberprzestrzeni RP. Ustalono bowiem, iż nie wprowadzono precyzyjnych regulacji prawnych nakładających na przedsiębiorców obowiązek przekazywania Prezesowi UKE informacji na temat naruszeń bezpieczeństwa związanych z incydentami występującymi w cyberprzestrzeni,

[24] Przedmiotowy obowiązek wynika z § 4 ust. 3 Rozporządzenia Rady Ministrów w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń.

co m.in. wpływa negatywnie na możliwość realizacji obowiązków UKE dotyczących informowania o tego typu zdarzeniach i zagrożeniach konsumentów. Stwierdzono także, że w związku z wadliwym systemem identyfikacji zagrożeń, opracowywane przez przedsiębiorców telekomunikacyjnych plany działań, nie zawierają praktycznych schematów działania adekwatnych do zdarzeń występujących w cyberprzestrzeni.

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, wnosi o:

1. Podjęcie, w uzgodnieniu z Ministrem Administracji i Cyfryzacji, działań mających na celu zdefiniowanie roli i zadań UKE w ramach budowanego systemu ochrony cyberprzestrzeni RP oraz realizację obowiązków wymienionych w pkt 5. i 6. *Polityki.*
2. Podjęcie, we współpracy z Ministrem Administracji i Cyfryzacji, działań mających na celu opracowanie projektu zmian legislacyjnych, pozwalających na praktyczne wykorzystanie przepisów Prawa telekomunikacyjnego w ramach realizacji zadań związanych z ochroną cyberprzestrzeni RP, w szczególności w zakresie uzyskiwania informacji o incydentach oraz tworzenia przez przedsiębiorców telekomunikacyjnych planów działania w sytuacjach kryzysowych związanych ze zdarzeniami występującymi w cyberprzestrzeni.
3. Przeprowadzenie analizy w zakresie możliwości zintensyfikowania działań informacyjnych UKE skierowanych do konsumentów w obszarze zagrożeń związanych z korzystaniem z Internetu oraz rekomendowanych środków ochronnych.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

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

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

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK proszę o poinformowanie Najwyższej Izby Kontroli, w terminie 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 24.09. 2014 r.

Wiceprezes
Najwyższej Izby Kontroli
Wojciech Kutyła

podpis