



**WICEPREZES
NAJWYŻSZEJ IZBY KONTROLI**
Marian Cichosz

KON – 4101-03-01/2012
P/12/191

WYSTĄPIENIE POKONTROLNE

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli

P/11/191 – Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji oraz innych danych, o których mowa w art. 180c i 180d ustawy Prawo telekomunikacyjne.

Jednostka
przeprowadzająca
kontrolę

Najwyższa Izba Kontroli, Departament Obrony Narodowej

Kontrolerzy

1. Andrzej Pankowski, główny specjalista k.p., upoważnienie do kontroli nr 82411 z dnia 05.09.2012 r.

(Dowód: akta kontroli str. 1-2)

2. Lucjan Belza, doradca ekonomiczny, upoważnienie do kontroli nr 82421 z dnia 1.10.2012 r.

(Dowód: akta kontroli str. 3-4)

Jednostka
kontrolowana

Służba Kontrwywiadu Wojskowego, ul. Oczki 1, 00-909 Warszawa

Kierownik jednostki
kontrolowanej

gen. bryg. Janusz Nosek, powołany z dniem 20 maja 2008 r. na stanowisko Szefa Służby Kontrwywiadu Wojskowego

(Dowód: akta kontroli str. 9,45)

II. Ocena kontrolowanej działalności

Ocena ogólna

Najwyższa Izba Kontroli ocenia pozytywnie¹ działalność kontrolowanej jednostki w zbadanym zakresie.

Uzasadnienie
oceny ogólnej

Tryb pozyskiwania i wykorzystywania danych telekomunikacyjnych oraz zapewnienie bezpieczeństwa i poufności danych eliminuje ryzyko wykorzystywania ich do innych celów, niż operacyjne.

Szef SKW w ramach posiadanych kompetencji prawidłowo uregulował i doprecyzował aktami wewnętrznymi zasady uzyskiwania i przetwarzania w SKW danych od operatorów telekomunikacyjnych. Prawidłowo dokonano w kontrolowanym okresie zabezpieczenia pozyskanych danych przed nieuprawnionym dostępem do nich lub przed ich utratą lub zniszczeniem. Zapewniono także

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.

poufność przekazywania danych pomiędzy uprawnionymi jednostkami organizacyjnymi SKW.

Powyższa ocena została wydana w oparciu o badanie strony organizacyjno-formalnej uzyskiwania przez SKW danych telekomunikacyjnych.

III. Opis ustalonego stanu faktycznego

1. Ocena zgodności z przepisami wyższego rzędu wewnętrznych uregulowań prawnych oraz struktur organizacyjnych, ustanowionych w obszarach uzyskiwania, przetwarzania wykorzystania i niszczenia danych telekomunikacyjnych

Opis stanu
faktycznego

Służba Kontrwywiadu Wojskowego, na podstawie art. 32 ust. 1 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego (Dz. U. Nr 104, poz. 709), może żądać udostępnienia danych telekomunikacyjnych, o których mowa w art. 180c oraz 180d ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 ze zm.), zwanych dalej danymi telekomunikacyjnymi oraz danych identyfikujących podmiot korzystający z usług pocztowych i dotyczących faktu, okoliczności świadczenia usług pocztowych lub korzystania z tych usług, bez potrzeby uzyskania zgody Sądu, przewidzianej w art. 31 ust. 1 ustawy o SKW i SWW.

Udostępnienie SKW danych telekomunikacyjnych może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli wykorzystywanie sieci i system teleinformatyczny zapewniają możliwość ustalenia osoby uzyskującej te dane, ich rodzaju oraz czasu, w którym zostały uzyskane oraz zabezpieczenie techniczne i organizacyjne uniemożliwiają osobie nieuprawnionej dostęp do tych danych (art. 32 ust. 6 ustawy o SKW i SWW).

Szef SKW na podstawie art. 20 ust. 2 ustawy o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego upoważnił dyrektora Biura Techniki i Obserwacji (BTiO) oraz jego zastępców do występowania w jego imieniu o dane ujęte w art. 180c i 180d ustawy Prawo telekomunikacyjne. W badanym okresie, tj. 2011-2012 (do początku września) w ewidencji papierowej BTiO wystąpiło 4.283 pozycji dotyczących zapytań o ustalenia telekomunikacyjne, kierowane do czterech głównych operatorów: PLUS (za pomocą systemu PISMAK), ORANGE (za pomocą systemu POEZJA II), T-MOBILE (za pomocą systemu FINEZJA) i PLAY (za pomocą systemu RUDA), zlecone przez jednostki organizacyjne SKW realizujące procedury

operacyjne oraz inne uprawnione ustawowo podmioty - Służbę Wywiadu Wojskowego (SWW) i Żandarmerię Wojskową (ŻW).

Ponadto Szef SKW do korzystania z elektronicznych baz danych operatorów telekomunikacyjnych upoważnił imiennie osoby z dziewięciu jednostek organizacyjnych SKW realizujących czynności operacyjno-rozpoznawcze, na podstawie regulaminów organizacyjnych i instrukcji o czynnościach operacyjnych takich jak: Zarząd Operacyjny (ZO), Zarząd Ochrony Interesów Ekonomicznych Sił Zbrojnych (ZOIESZ), Biuro Pełnomocnika Ochrony i Bezpieczeństwa Wewnętrznego (BPOiBW), Biuro Radiokontrwywiadu, Inspektorat SKW w Warszawie, Inspektorat SKW w Gdyni, Inspektorat SKW w Poznaniu, Inspektorat SKW w Lublinie, Inspektorat SKW w Krakowie. Jednostki te upoważnione są do korzystania, za pomocą indywidualnych kart dostępu, z baz danych 5 operatorów telekomunikacyjnych (systemy FINEZJA, POEZJA II, PISMAK, RUDA, SONAR i BEZPIECZNA POCZTA TP). Realizowanie ww. uprawnienia wprowadzano w SKW na przełomie grudnia 2009 r. i stycznia 2010 r.

[Dowód: akta kontroli, str. 47-48]

Udostępnianie danych telekomunikacyjnych funkcjonariuszowi SKW, posiadającemu pisemne upoważnienie Szefa SKW, odbywa się na podstawie porozumień zawartych pomiędzy Szefem SKW a operatorem na podstawie art. 32 ust. 5 ustawy o SKW i SWW:

a) P4 (PLAY) – umowa nr 6/11 z dnia 25 lipca 2011 r. podpisana przez Szefa SKW i Porozumienie techniczne nr 5/11 z dnia 14 września 2011 r. podpisane przez dyrektora BTiO SKW z upoważnienia Szefa SKW,

b) POLKOMTEL (PLUS) – porozumienie nr 4/09 z dnia 9 kwietnia 2009 r. podpisane przez Szefa SKW z upoważnienia Ministra Obrony Narodowej i Porozumienie techniczne nr 4/11 z dnia 4 sierpnia 2011 r. podpisane przez dyrektora BTiO SKW z upoważnienia Szefa SKW,

c) PTC (T-MOBILE) – Porozumienie techniczne nr 3/11 z dnia 19 maja 2011 r. podpisane przez dyrektora BTiO SKW z upoważnienia Szefa SKW,

d) TP SA (ORANGE) – Porozumienie nr 5/09 z dnia 14 kwietnia 2009 r. podpisane przez Szefa SKW, z upoważnienia Ministra Obrony Narodowej.

W przypadku osób z podległych jednostek organizacyjnych realizujących ustalenia telekomunikacyjne, dyrektor BTiO, z upoważnienia Szefa SKW, przysyłał do operatorów imienne listy osób upoważnionych do realizacji ustaleń telekomunikacyjnych u 4 operatorów telefonii komórkowej oraz TPSA: Polkomtel

S.A. (PISMAK), ORANGE (POEZJA II), PTC Sp. z o.o. (FINEZJA), P4 Sp. z o.o. (RUDA) oraz TPSA (SONAR i BEZPIECZNA POCZTA TP). Cofnięcie osobie upoważnionego certyfikatu dostępu drogą elektroniczną do danych operatora następuje ze względu na zmianę zakresu obowiązków lub zmianę stanowiska upoważnionego. Wysyłanie zapytań do operatorów zarówno pisemnych, jak i drogą elektroniczną, odbywa się na wniosek żołnierza lub funkcjonariusza, podlegający weryfikacji i zatwierdzeniu przez kierownika jednostki organizacyjnej (kontrola zarządcza). Dodatkowo BTiO posiada rolę nadzorczą dla systemów FINEZJA i RUDA dla wszystkich osób upoważnionych do wysyłania zapytań drogą elektroniczną poprzez dostęp do bazy danych upoważnionego użytkownika, a operator systemu POEZJA przesyła w formie elektronicznej wszystkie zapytania w okresach kwartalnych. Uzasadnieniem dla wprowadzenia dostępu do ustaleń telekomunikacyjnych 4 głównych operatorów telefonii komórkowej i TP SA była możliwość zdalnego dostępu do baz danych tych operatorów, co mogło mieć wpływ na przyspieszenie realizacji zadań operacyjnych. Ponadto od 2009 r. istnieje w Polsce możliwość przeniesienia numerów z sieci jednego do innego operatora (migracja numerów), co wydłużyło procedurę ustalenia abonenta. Według danych Urzędu Komunikacji Elektronicznej, w 2011 r. zostało przeniesionych ponad 1 mln numerów. Większość z nich (71%) były to numery przeniesione do sieci PLAY (RUDA) – („Raport o stanie rynku telekomunikacyjnego w Polsce w 2011 r.”, Warszawa, czerwiec 2012 r.).

Procedury bezpieczeństwa danych telekomunikacyjnych związanych z realizacją wniosków o ustalenia telekomunikacyjne, w tym opracowywania danych pochodzących od operatorów telekomunikacyjnych określone zostały w „Szczególnych Wymaganiach Bezpieczeństwa dla Systemu Teleinformatycznego „PUCHACZ” (BTO-Z-4209/12), zatwierdzonych 26 czerwca 2012 r. przez Szefa Służby Kontrwywiadu Wojskowego. Dokument ten stanowił Szczególne Wymagania Bezpieczeństwa (SWB) dla systemu teleinformatycznego przetwarzającego informacje niejawne w Wydziale I Biura Techniki i Informacji i służy do wytwarzania, przetwarzania oraz przechowywania informacji niejawnych do klauzuli „Ścisłe Tajne”. Ponadto Szef Kontrwywiadu Wojskowego wprowadził 26 czerwca 2012 r. Procedury Bezpiecznej Eksploatacji dla Systemu Teleinformatycznego „PUCHACZ” do przetwarzania informacji niejawnych dla klauzuli „Ścisłe Tajne” włącznie (BTO-Z-4210/12). W SKW opracowano też „Analizę ryzyka systemu” „PUCHACZ” (BTO-Z-

4211/12), aktualizowaną na dzień 15 maja 2012 r., co omówiono w dalszej treści wystąpienia.

Dane telekomunikacyjne uzyskane z jawnych baz operatorów są eksportowane, przy wykorzystaniu dedykowanych (indywidualnych) nośników informacji do systemu „Puchacz”, gdzie są przetwarzane i kojarzone z przesłanymi zapytaniem pionów operacyjnych. Na podstawie ww. dokumentów stwierdzono minimalizowanie ryzyka w zakresie:

a) Bezpieczeństwa danych telekomunikacyjnych

W systemie informatycznym na serwerze utworzony został katalog, w którym gromadzone są dzienniki zdarzeń, które zawierają między innymi takie informacje, jak np. zmiany w systemie plików czy też uruchomione procesy przez użytkownika, co pozwala w każdej chwili jednoznacznie zidentyfikować użytkownika końcowego przetwarzającego dane.

Podstawowym zabezpieczeniem danych telekomunikacyjnych jest wykonywana każdego dnia kopia różnicowa przechowywanych danych.

Kompleks pomieszczeń, w którym zlokalizowany jest system do przetwarzania danych telekomunikacyjnych, znajduje się w I strefie bezpieczeństwa, do której dostęp mają jedynie upoważnieni pracownicy Wydziału I BTiO, którzy są jednocześnie uprawnieni do pobierania kluczy oraz aktywowania/deaktywowania systemu alarmowego.

W przypadku, gdy użytkownik systemu posiada potrzebę oddalenia się od stanowiska, musi usunąć nośniki zewnętrzne i wylogować się z systemu. W przypadku dłuższej bezczynności po 15 minutach następuje samoczynne wylogowanie użytkownika, a dalsza praca jest możliwa dopiero po ponownym uwierzytelnieniu.

Logowanie do systemu następuje po wprowadzeniu nazwy użytkownika i hasła. Indywidualnie nadane hasło ważne jest przez 90 dni. Jeśli użytkownik przed upływem tego terminu nie zmieni hasła, jego konto zostanie zablokowane. Konto jest blokowane również po trzykrotnym błędnym wprowadzeniu hasła.

Użytkowników obowiązuje kategoriyczny zakaz udostępniania hasła innym osobom. W razie jakichkolwiek problemów z logowaniem użytkownik natychmiast powiadamia administratora systemu.

Po zalogowaniu się, użytkownik ma możliwość uruchomienia tylko tej części oprogramowania systemu, do której przydzielono mu uprawnienia. Może on wykonywać tylko te czynności, które wynikają z jego zakresu obowiązków, nie ma

dostępu do usług i funkcji systemu, do których nie został uprawniony przez administratora.

W przypadku, gdy zachodzi potrzeba eksportowania danych niejawnych z systemu na nośniki CD/DVD, wówczas operator tworzy obraz ISO, a administrator dokonuje nagrania na płytę. Operator konta dokonujący eksportu zobowiązany jest zarejestrować nośnik w punkcie kontroli. Pozostały eksport możliwy jest w postaci wydruków. Dane wyeksportowane z systemu w postaci papierowej lub elektronicznej podlegają rejestracji w punkcie kontroli BTiO, zgodnie z obowiązującym zarządzeniem Nr 35/11 Szefa SKW z dnia 13 maja 2011 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych (niepublikowane), wydanym na podstawie art. 47 ust. 3 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228).

Każdy użytkownik przetwarzający dane telekomunikacyjne posiada pamięć USB zarejestrowaną w punkcie kontroli BTiO i tylko tę pamięć może wykorzystywać w systemie.

Wydruki próbne, błędne i brudnopisy niszczone są niezwłocznie w niszczarce w pomieszczeniu systemu. Dokumenty nie podpisane przez upoważnionych przełożonych niszczone są w ich pomieszczeniach w sposób uniemożliwiający odczytanie ich treści.

Osoby nieuprawnione mogą przebywać w miejscu lokalizacji systemu jedynie w towarzystwie osoby uprawnionej. Dostęp osoby nieuprawnionej do zasobów danych telekomunikacyjnych jest niemożliwy.

Pierwszy pracownik wchodzący do kompleksu pomieszczeń danego dnia, po wcześniejszym pobraniu kluczy od depozytora oraz dezaktywowaniu systemu alarmowego, zobowiązany jest do sprawdzenia czy pomieszczenia, w których znajduje się system oraz urządzenia, nie posiadają oznak włamania lub innego niepożądanego działania. Po zakończeniu pracy, ostatni wychodzący z kompleksu pomieszczeń uprawniony pracownik dokonuje sprawdzenia zabezpieczeń pomieszczeń i urządzeń, zamyka pomieszczenia, aktywuje system alarmowy i deponuje klucze w depozytorze.

W przypadku stwierdzenia przez użytkowników jakichkolwiek zmian dotyczących budowy lub konfiguracji systemu (np. programy, kable), niezwłocznie informują oni o takim fakcie administratora.

Pomieszczenia, w których zlokalizowany jest system do przetwarzania danych telekomunikacyjnych, znajdują się w I strefie bezpieczeństwa, a okna w tych pomieszczeniach zabezpieczone są folią matową, uniemożliwiającą podgląd.

b) Poufności danych telekomunikacyjnych

Dostęp do danych telekomunikacyjnych posiadają jedynie osoby uprawnione na podstawie haseł dostępowych do indywidualnych kont użytkowników systemu lub kart mikroprocesorowych zabezpieczonych kodem PIN. Osoby nieuprawnione do korzystania z systemu mogą przebywać w jego lokalizacji jedynie w towarzystwie osoby uprawnionej. Systemy do realizacji ustaleń telekomunikacyjnych są zlokalizowane w I strefie bezpieczeństwa, w której realizowana jest szczegółowo kontrola dostępu oraz zainstalowane są systemy przeciw włamaniom i napadom, monitoring, procedury wejść i wyjść oraz sygnalizacji pożarowej.

Wszystkie osoby realizujące ustalenia telekomunikacyjne posiadają aktualne poświadczenie bezpieczeństwa osobowego do klauzuli "Ścisłe Tajne". Wszystkie nośniki elektroniczne wytworzone w systemie podlegają rejestracji w punkcie kontroli bądź Sekretariacie BTiO SKW.

Nadzór nad niekontrolowanym wynoszeniem elektronicznych nośników pamięci prowadzi służba ochrony SKW, wykorzystując umieszczony przy wszystkich wejściach do budynków sprzęt elektroniczny wykrywający te nośniki.

Naprawy doraźne i konserwacja sprzętu jest realizowana przez administratorów systemu, wyłonionych z komórki realizującej ustalenia telekomunikacyjne. W przypadku poważnej awarii urządzenia są pozbawiane nośników pamięci i za zgodą Pełnomocnika Ochrony SKW oddawane do serwisu.

Umieszczenie podsłuchu uniemożliwione jest poprzez zasady poruszania się w strefach bezpieczeństwa: kontrola dostępu do pomieszczeń, sygnalizacja włamania (nieautoryzowane naruszenie strefy jak drzwi, okna), monitoring.

Stanowiska komputerowe, na których przetwarzane są informacje niejawne oraz dane telekomunikacyjne (terminale bezdyskowe), serwer (umieszczony w kabinie ekranującej) oraz drukarka tworzą system posiadający akredytację bezpieczeństwa teleinformatycznego do klauzuli "Ścisłe Tajne".

c) Integralności danych telekomunikacyjnych

Użytkownikami systemu do przetwarzania danych telekomunikacyjnych są tylko upoważnieni przez Dyrektora BTiO SKW, pracownicy Wydziału I, posiadający poświadczenie bezpieczeństwa do klauzuli „Ścisłe Tajne” oraz zaświadczenie o

przeszkoleniu w zakresie ochrony informacji niejawnych. Dostęp do systemu odbywa się na podstawie indywidualnego konta, zabezpieczonego hasłem, jednoznacznie identyfikującego danego użytkownika.

W systemie informatycznym, w którym przetwarzane są dane telekomunikacyjne, stosowane są mechanizmy uniemożliwiające naruszenie integralności tych danych. Podstawowym zabezpieczeniem danych telekomunikacyjnych jest wykonywana każdego dnia kopia różnicowa.

Przy pomocy programu antywirusowego, jeden raz dziennie, skanowany jest cały system, natomiast skanowanie pamięci USB automatycznie odbywa się podczas jego montowania oraz przy kopiowaniu plików. Baza sygnatur wirusów w systemie uaktalniana jest poprzez kopiowanie ich z repozytorium umieszczonego na stronie producenta. Bazy przenoszone są do systemu na nośnikach zewnętrznych i kopiowane przez administratora, zalogowanego lokalnie do serwera.

W przypadku awarii sprzętowej systemu, administrator usuwa awarię lub też dokonuje wymiany uszkodzonego urządzenia (zgodnie z obowiązującymi zarządzeniami Szefa SKW). W przypadku gdy administrator nie jest w stanie samodzielnie usunąć usterki, sprzęt przekazywany jest do serwisu bez nośników danych.

System do przetwarzania danych teleinformatycznych zlokalizowany jest w strefie bezpieczeństwa, w której znajduje się między innymi system sygnalizacji pożarowej, monitorowany przez Oficera Dyżurnego SKW. W przypadku zauważenia pożaru lub innego czynnika mogącego zagrozić życiu ludzkiemu i bezpieczeństwu przetwarzanych informacji niejawnych, każdy użytkownik ma obowiązek poinformować pozostałych i natychmiast zakończyć pracę w systemie (wylogować się lub wyłączyć stację terminalową).

W przypadku wystąpienia zagrożenia zewnętrznego (np. atak terrorystyczny, klęska żywiołowa) każdy użytkownik ma obowiązek natychmiastowego zakończenia pracy w systemie (wylogowania), a w przypadku napadu - uruchomienia przycisku „antynapadowego”.

W przypadku zagrożenia zniszczeniem urządzeń serwerowych, administrator zabezpiecza nośniki danych poprzez ich wyjęcie i wyniesienie poza pomieszczenia znajdującego się systemu. Administrator odpowiada wówczas za zabezpieczenie wszystkich materiałów niejawnych wyniesionych z pomieszczeń systemu. O zdarzeniu informuje Dyrektora BTiO SKW.

d) Rozliczalności danych telekomunikacyjnych w systemie informatycznym

Dostęp użytkownika do systemu informatycznego odbywa się na podstawie indywidualnego konta, zabezpieczonego hasłem. Do zakładania konta uprawniony jest jedynie administrator. Konto użytkownika może zostać zablokowane przez administratora w przypadku stwierdzenia nieupoważnionych działań prowadzonych przy użyciu danego konta, a automatycznie w przypadku wygaśnięcia terminu ważności poświadczenia bezpieczeństwa lub na polecenie Dyrektora BTiO SKW.

System informatyczny do przetwarzania danych telekomunikacyjnych zapewnia rozliczalność działań wszystkich użytkowników poprzez gromadzenie dzienników zdarzeń, co gwarantuje rozliczalność danych telekomunikacyjnych. Dzienniki zdarzeń gromadzone są w specjalnie do tego celu przeznaczonym katalogu. W katalogu tym gromadzone są takie zdarzenia jak: logowanie/wylogowanie użytkownika, usuwanie konta użytkownika, dodawanie użytkownika (konta), logowanie/wylogowanie do bazy danych ustaleń telekomunikacyjnych, dodawanie i kopiowanie rekordów w bazie danych ustaleń telekomunikacyjnych, zapis oraz usuwanie danych z pamięci USB, podłączenie/odłączenie pamięci USB, drukowanie dokumentów, uruchomione procesy przez użytkownika, zmiany w systemie plików.

W jednostce kontrolowanej opracowano „Analizę ryzyka systemu PUCHACZ” (sygn. BTO-Z-4211/12) z dnia 15 maja 2012 r. Nie rzadziej niż co 6 miesięcy ponownemu przeprowadzeniu podlega proces analizy ryzyka systemu. System opracowany został w BTiO i przeznaczony jest do wytwarzania, przetwarzania i przechowywania informacji niejawnych związanych z bieżącą działalnością Wydziału I BTiO. Oznaczało to realizację wniosków o ustalenia telekomunikacyjne, w szczególności danych pochodzących od operatorów telekomunikacyjnych. Dane wejściowe i wyjściowe w ramach ustaleń telekomunikacyjnych wprowadzane za pomocą pamięci są danymi jawnymi. Gotowe opracowania identyfikacji abonentów nie są kopiowane na nośniki USB. Jako gotowe opracowania identyfikacji podlegają tylko wydrukowi. Analizę ryzyka przeprowadzono w trzech obszarach: a) identyfikacja zasobów systemu, wymagania ochrony; b) identyfikacja zagrożeń systemu; c) identyfikacja podatności) w oparciu o metrykę wagi w skali od 1 (poziom minimalny) do 8 (poziom bardzo wysoki). Przyjętą identyfikację i szacowanie ryzyka oparto na wyliczeniu stopnia zagrożenia i podatności. Minimalizacja oszacowanego ryzyka została wprowadzona w Szczególnych Wymaganiach Bezpieczeństwa (SWB) dla systemu

teleinformatycznego przetwarzającego informacje niejawne do klauzuli „Ścisłe Tajne”. Poufność zasobów informacyjnych sklasyfikowano na poziomie wysokim.

Jednostka kontrolowana posiada urządzenia zabezpieczające przed utratą danych spowodowane awarią zasilania. Wszystkie urządzenia i komputery oraz systemy teleinformatyczne podłączone są poprzez awaryjne sieci zasilania UPS. Ponadto w centrali SKW zainstalowane są niezależne generatory, uruchamiane po ok. 20 minutach pracy urządzeń UPS.

Oceną zgromadzonych danych zajmuje się jednostka wnioskująca o ich pozyskanie. W wyjaśnieniu Szef SKW podał, że „(...) *nie ma przepisów, które nakazują niezwłoczne komisyjne i protokolarne zniszczenie danych telekomunikacyjnych w sytuacji, gdy nie zawierają informacji mających znaczenie dla postępowania karnego (SKW nie jest służbą państwową, uprawnioną do prowadzenia czynności procesowych, prowadzi jedynie czynności operacyjno – rozpoznawcze). Z uwagi na specyfikę zainteresowań SKW zniszczenie tego typu danych mogłoby spowodować ograniczenie możliwości operacyjnych wobec prowadzonych rozpracowań. Ponadto materiały te nie podlegają komisyjnemu zniszczeniu, gdyż nie zostały pozyskane w wyniku stosowania kontroli operacyjnej, a tym samym nie stosuje się wobec nich zapisu art. 31 ust. 15 ustawy o SKW i SWW. Informacje uzyskiwane od operatorów są włączone do procedur operacyjnych i po ich zakończeniu składane i przechowywane w Biurze Ewidencji Archiwum SKW wraz ze wszystkimi materiałami zgromadzonymi w prowadzonej procedurze.*”

[Dowód: akta kontroli, str. 69-70]

Na podstawie art. 37 ust. 1 ustawy o Najwyższej Izbie Kontroli, w BTiO sporządzono, na podstawie elektronicznej bazy danych, zestawienie ilości danych telekomunikacyjnych (abonenci) i historię połączeń (lokalizacja) w 2011 r. i I połowie 2012 r. W 2011 r. ustalenia wykonane przez BTiO dotyczyły 42.386 danych użytkowników, a w I połowie 2012 r. – 16.978 danych. Z zapytaniem o historię połączeń (lokalizacja) w 2011 r. wystąpiono w 1.570 wnioskach (3,7%), a w I połowie 2012 r. w 784 wnioskach (4,6%). Pozostałe zapytania dotyczyły ustalenia abonenta.

[Dowód: akta kontroli, str. 79]

Realizowane przez pozostałe jednostki organizacyjne SKW w ograniczonym zakresie, w odniesieniu jedynie do 4 operatorów telefonii komórkowej i TPSA, pozyskane dane telekomunikacyjne drogą elektroniczną poprzez karty dostępu,

dotyczyły w 2011 r. – 34.122 numerów użytkowników, a w I połowie 2012 r. – 19.560 użytkowników.

Na ogólną liczbę 76.508 ustaleń telekomunikacyjnych w 2011 r. i 36.538 w I połowie 2012 r. zrealizowanych przez wszystkie jednostki organizacyjne SKW, ustalenie abonenta przez SKW dotyczyło odpowiednio 73.009 i 34.605 abonentów oraz 3.499 (4,6%) i 1.933 (5,3%) ustaleń historii połączeń (bilingi).

[Dowód: akta kontroli, str. 79]

W jednostce kontrolowanej funkcjonuje ewidencja umożliwiająca odnotowanie, kto, kiedy i w jakim celu oraz jakie dane uzyskiwał w formie ewidencji elektronicznej, znajdującej się na twardych dyskach komputerów, na których przygotowuje się i szyfruje zapytania oraz ewidencję wysłanych zapytań (potwierdzenia), otrzymanych z sieci informatycznej operatorów telekomunikacyjnych. Ponadto prowadzona jest w BTiO ewidencja papierowa zapytań jawnych i niejawnych w formie wydruku treści zapytań do operatorów telekomunikacyjnych, wysłanych drogą elektroniczną. Ewidencja niejawna zapytań prowadzona jest w formie papierowej wyłącznie poprzez BTiO (przechowywany jest drugi egzemplarz zapytania wysłany do operatorów telekomunikacyjnych).

Na podstawie porównania próby losowo dobranej z ewidencji zapytań, otrzymanych od operatora PLAY w liczbie 12 zapisów (maj 2011 r.- 30.06.2012 r.) z ewidencją prowadzoną w jednostce kontrolowanej, stwierdzono że występują one w rejestrach elektronicznych i papierowych prowadzonych w kontrolowanej jednostce. Ponadto realizowana jest kontrola zarządcza przez Biuro Techniki i Obserwacji poprzez dostęp do bazy danych upoważnionego użytkownika, realizującego uprawnienia ustaleń telekomunikacyjnych u ww. operatora.

[Dowód: akta kontroli, str. 97]

Na podstawie próby uzyskanej z danych przekazanych przez operatorów (Sferia, Orange, Multimedia) dokonano porównania ewidencji zawierających żądania udostępnienia danych, porównując je z ewidencją prowadzoną w jednostce kontrolowanej. Na 4 zapisy operatora SFERIA, w 3 przypadkach dotyczyło to ustalenia danych abonenta, a w jednym (BTiO/Z-1705/2011 z dnia 02.06.2011 r.) wykazu połączeń abonenta (biling). W przypadku operatora ORANGE (pismo nr DK.Wych./BTO 361/2011 z dn. 13.06.2011 r.) pismo dotyczyło akredytacji systemu za pomocą interfejsu w rozumieniu art. 179 ust. 4a ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne, tj. zapewnienia warunków technicznych i

organizacyjnych dostępu i utrwalania (kontrola operacyjna). We wszystkich ww. zapytaniach wystąpiła osoba uprawniona z upoważnienia Szefa SKW.

[Dowód: akta kontroli, str. 28-32]

Z ewidencji zapytań prowadzonej w formie papierowej przez BTiO SKW, badaniem objęto losowo dobrane 150 zapytań kierowanych w 2011 r. i w 2012 r. (do września 2012 r.) do 4 największych operatorów, tj. ERA /T-MOBILE (897), PLUS (1.184), ORANGE (961), PLAY (831) oraz zapytań w rejestrze niejawnym (410). Łącznie ewidencja w formie papierowej zawierała 4.283 zapytań do ww. operatorów, z tego w 2011 r. - 2.418 zapytań i w 2012 r. - 1.865 zapytań. Z ogółem 4.283 zapytań, 3.843 kierowane były za pismem jawnym i 440 za pismem niejawnym.

[Dowód: akta kontroli, str. 14-26]

Ponadto badaniem do kontroli objęto dobór celowy 12 zapisów w oparciu o zestawienie sporządzone na podstawie informacji uzyskanych od operatorów. Łącznie badaniem objęto 162 zapisy z rejestru zapytań według dwóch cech: czy z zapytaniem wystąpiła upoważniona osoba oraz czy informacja została uzyskana na żądanie właściwej komórki organizacyjnej.

Odstąpiono od ustalenia, czy zapytanie dotyczące numeru telefonu, kierowano do jednego czy też do kilku operatorów, ze względu na wysoką pracochłonność procesu ustalenia (sprawdzanie w 4.283 pozycjach kolejnych numerów telefonu). W ewidencji zapytań nie prowadzi się rejestru, czy o dany numer występowano do jednego czy też do wielu operatorów.

[Dowód: akta kontroli, str. 27]

Na podstawie wybranej przez kontrolera próbie 150 zapytań dobranych losowo i 12 zapytań z próby celowej, wskazanej na podstawie danych uzyskanych od operatora, stwierdzono we wszystkich pozycjach, że z zapytaniem wystąpiła osoba do tego uprawniona oraz informacja została uzyskana na żądanie właściwej jednostki organizacyjnej lub podmiotu ustawowo uprawnionego (SWW).

[Dowód: akta kontroli, str. 51-63]

Z danych uzyskanych od operatora (TPSA) wynikało, iż w trzech przypadkach zapytania kierowane były za okres wykraczający poza retencję 24 miesięcy.

[Dowód: akta kontroli, str. 33-35]

Dyrektor Biura Techniki i Obserwacji SKW, odnosząc się do przedstawionych danych wyjaśnił, że: „Pozycja 1 z dn. 24.08.2011 r. pismo BTO-0-811/11. Treść zapytania: proszę o udostępnienie historii połączeń wykonanych z kart

telefonicznych o numerach (xxx). Wyjaśnienie: W zapytaniu nie został określony termin, gdyż nie można założyć, kiedy były realizowane połączenia z kart telefonicznych. Zapytanie nie dotyczyło określonego abonenta. Pozycja 2 z dnia 16.02.2012 r. Zapytanie 1056_12. Treść zapytania: proszę o przesłanie wykazu połączeń z n/wym. numeru za maksymalny okres retencji danych: (xxx). Wyjaśnienie: Wskazano okres retencji danych nieprzekraczający 24 miesiące. Pozycja 3 z dnia 15.11.2011 r.: pismo BTO-030277/11. Treść zapytania: proszę o udostępnienie historii połączeń inicjowanych z terenu całej Polski oraz przychodzących od abonentów o numerach: (xxx). Wyjaśnienie: Zapytanie dotyczyło niepełnych dwóch lat (bez siedmiu dni). Dokument w formie papierowej TPSA mogła otrzymać po 07.10.2011 r., co spowodowało, że został przekroczony okres retencji danych – 24 miesiące wstecz."

[Dowód: akta kontroli, str. 42-43]

W BTiO przeprowadzony został audyt przez Zarząd Bezpieczeństwa Informacji Niejawnych (ZBIN) z zakresu bezpieczeństwa teleinformatycznego. W wyniku audytu BTiO otrzymało Świadectwo Bezpieczeństwa Teleinformatycznego. Na podstawie zalecenia ZBIN SKW (DK Wch./BTO-1022/2012) po przeprowadzonym audycie dwie osoby spośród sześciu odbyły szkolenia specjalistyczne administratorów systemu (posiadały nieaktualne zaświadczenie o odbytym szkoleniu). Osoby te otrzymały stosowne zaświadczenie.

Ustalone
nieprawidłowości

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

Ocena częściowa

Najwyższa Izba Kontroli ocenia pozytywnie działalność kontrolowanej jednostki w zbadanym zakresie.

2. Ocena prawidłowości i sposobu wykorzystywania przez uprawnione służby i organy państwa przyznanych im uprawnień, w szczególności przestrzeganie obowiązujących zasad, przepisów ustawowych oraz procedur wewnętrznych w zakresie żądania, uzyskiwania, przetwarzania, wykorzystania i niszczenia danych telekomunikacyjnych

2.1. Sprawność i szybkość pozyskiwania informacji

Opis stanu faktycznego

W wyjaśnieniu Szef SKW podał, że nie było przypadków kwestionowania przez operatorów telekomunikacyjnych uprawnień ustawowych SKW i odmowy udostępniania danych telekomunikacyjnych. W jednostce kontrolowanej nie wystąpiły przypadki przekazywania danych telekomunikacyjnych ze znaczną zwłoką.

W SKW wprowadzono zmianę w zakresie pozyskiwania danych telekomunikacyjnych od 4 głównych operatorów (ERA/T-MOBILE, PLAY, PLUS, ORANGE) oraz TPSA decyzją Szefa SKW z dnia 4 marca 2009 r., upoważniając jednostki organizacyjne prowadzące pracę operacyjną do uzyskiwania danych telekomunikacyjnych drogą elektroniczną za pomocą kart dostępu.

Wprowadzone zmiany organizacyjne, w ocenie Zastępcy Szefa SKW, znacznie skróciły czas ustaleń telekomunikacyjnych realizowanych przez właściwe jednostki organizacyjne. Dystrybucją uprawnień (kart dostępu) zajmuje się Biuro Techniki i Obserwacji SKW jako jednostka nadzorująca.

[Dowód: akta kontroli, str. 64-65]

Ustalone nieprawidłowości

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

2.2. Zapewnienie warunków technicznych i organizacyjnych dostępu do danych telekomunikacyjnych przez uprawnione podmioty

Opis stanu faktycznego

Służba Kontrwywiadu Wojskowego, na podstawie art. 179 ust. 2 i 3 ustawy - Prawo telekomunikacyjne, w celu realizacji zadań określonych w art. 5 ustawy o SKW i SWW, wykonuje czynności operacyjno-rozpoznawcze, w szczególności utrwalania rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych. Dla realizacji tych czynności SKW podpisała umowy z operatorami telekomunikacyjnymi: ORANGE (2009 r.), T-MOBILE (2011 r.), PLUS

(2009 r.) i PLAY (2011 r.), w których opisano warunki dostępu do przekazów telekomunikacyjnych za pomocą interfejsów, określając jako punkt styku miejsce wskazane przez SKW. Inni operatorzy zapewnili jednostce dostęp do posiadanych przez przedsiębiorcę danych związanych z przekazem telekomunikacyjnym (zapewnienie warunków technicznych i organizacyjnych „dostępu i utrwalania”) na zasadach określonych w art. 179 ust. 3 ustawy - Prawo telekomunikacyjne.

[Dowód: akta kontroli: str. 80]

Ustalone
nieprawidłowości

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

2.3. Realizacja ustawowych uprawnień w zakresie pozyskiwania danych telekomunikacyjnych

Opis stanu
faktycznego

Służba Kontrwywiadu Wojskowego pozyskuje dane telekomunikacyjne w celu realizacji zadań określonych w art. 5 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego.

Legalność pozyskiwania danych telekomunikacyjnych ustalono na podstawie próby 12 pozycji próby celowej oraz 150 pozycji dobranych losowo przez kontrolera NIK. Zbadano według cech, czy informacja została uzyskana na żądanie właściwej komórki lub jednostki organizacyjnej (jednostki prowadzącej pracę operacyjną). Na 12 zapytań, z 8 wystąpiło BTiO, z 2 - Inspektoraty (Kraków i Warszawa) oraz Zarząd Operacyjny i Zarząd Ochrony Ekonomicznych Interesów Sił Zbrojnych SKW. W zbadanych 150 zapytaniach, we wszystkich przypadkach wystąpiła właściwa jednostka organizacyjna lub podmiot uprawniony ustawowo.

[Dowód: akta kontroli, str. 51-53]

Art. 32 ust. 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, brzmi: „*Obowiązek uzyskania zgody sądu, o której mowa w art. 31 ust. 1, nie dotyczy informacji niezbędnych do realizacji przez SKW zadań określonych w art. 5, w postaci danych:*

- 1) *o których mowa w art. 180c oraz 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.), zwanych dalej "danymi telekomunikacyjnymi";*
- 2) *identyfikujących podmiot korzystający z usług pocztowych oraz dotyczących faktu, okoliczności świadczenia usług pocztowych lub korzystania z tych usług."*

Na pytanie, w ilu sprawach uzyskane dane telekomunikacyjne miały wpływ na rozstrzygnięcie sprawy, dyrektor BTiO SKW podał, że:

„BTiO otrzymuje zlecenia w ww. zakresie od właściwych komórek organizacyjnych prowadzących pracę operacyjną celem dokonania ustalenia abonenta lub wystąpienia o bilingi. BTiO nie ma i nie może mieć wiedzy na temat wpływu przekazanych danych telekomunikacyjnych na rozstrzygnięcie sprawy. Powyższe ustalenia wymagałyby wglądu przez kontrolującego w prowadzone sprawy operacyjne lub inne procedury prowadzone we właściwych komórkach organizacyjnych.” W SKW prowadzone sprawy operacyjne i procedury operacyjne opatrzone są klauzulą „Ściśle Tajne”.

Dane uzyskiwane od operatorów telekomunikacyjnych nie były przekazywane innym uprawnionym do tego podmiotom.

[Dowód: akta kontroli, str. 80]

W wyjaśnieniu dyrektor Biura Pełnomocnika Ochrony i Bezpieczeństwa Wewnętrznego SKW podał, że do Szefa SKW nie wpłynęły skargi w rozumieniu Kodeksu postępowania administracyjnego, od osób publicznych lub instytucji, dotyczące zleceń realizowanych przez właściwe rzeczowo komórki organizacyjne SKW w zakresie ustalenia abonentów lub historii połączeń.

[Dowód: akta kontroli, str. 49]

Ustalone
nieprawidłowości

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

Ocena częściowa

Najwyższa Izba Kontroli ocenia pozytywnie działalność w badanym obszarze.

IV. Uwagi

Analiza procedur pozyskiwania i przetwarzania danych telekomunikacyjnych, jak również treść złożonych podczas kontroli wyjaśnień wskazuje, w ocenie NIK, na potrzebę nowelizacji ustawy - Prawo telekomunikacyjne, aby jednostki realizujące procedury operacyjne mogły uzyskać wpływ na szybkość ustaleń abonenta oraz zmniejszyć liczbę ustaleń telekomunikacyjnych, wynikającą z braku dostępnej bazy danych abonenta. Ponadto czas ustaleń telekomunikacyjnych uległ wydłużeniu na skutek nowych uwarunkowań prawnych funkcjonujących od 2009 r., które pozwalają

na migrację abonenta do kolejnego operatora telefonii komórkowej, bez konieczności zaangażowania użytkownika usług. Brak bazy danych, pozwalającej w jednym zapytaniu na ustalenie abonenta końcowego, zwielokrotnia liczbę zapytań o jeden numer użytkownika telefonu i wydłuża proces ustaleń telekomunikacyjnych. Kwestia ta może mieć istotne znaczenie w świetle przygotowywanej propozycji skrócenia retencji danych.

**Prawo zgłoszenia
zastrzeżeń**

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 uwagi 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.

Karłowice, dnia *18.01.2013r.*

Wiceprezes
Najwyższej Izby Kontroli
Marian Cichosz


podpis