BEZPIECZEŃSTWO AKTYWÓW MINISTERSTWA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI W INFRASTRUKTURZE KRYTYCZNEJ PAŃSTWA

Andrzej Machnacz

ANALIZA ZAGROŻEŃ
Obszar MSWiA

WYMAGANIA FIZYCZNE I ŚRODOWISKOWE
Obszar MSWiA

WYMAGANIA TECHNOLOGICZNE
Obszar MSWiA

WYMAGANIA PROCEDURALNE
Obszar MSWiA

POTRZEBY PRZECIWDZIAŁAŃ
Fizyczne i środowiskowe

Wybawi się od niebezpieczeństwa jedynie ten,
kto czuwa także wtedy, gdy czuje się bezpieczny.

Publiusz Siro

W artykule opisano aktywa teleinformatyczne MSWiA istotne z punktu widzenia infrastruktury krytycznej państwa, na tyle ważne dla jego funkcjonowania, że ich utrata lub znaczące przerwy w działaniu mogłyby spowodować poważne skutki dla bezpieczeństwa państwa i jego obywateli, a także dla skutecznego funkcjonowania organów władzy i administracji publicznej oraz instytucji i przedsiębiorstw.

Bezpieczeństwo i zdrowie obywateli, a także dobra środowiskowe i finansowe są poważnie zagrożone, jeśli państwo nie zapewnia ciągłości działania pewnej części infrastruktury, na tyle ważnej dla jego funkcjonowania, że jej utrata lub znaczące przerwy w działaniu mogłyby spowodować

poważne konsekwencje ekonomiczne lub socjalne, zagrażające bytowi społeczeństwa lub jego pokaźnej części.

Ta część infrastruktury, obejmująca materialne lub informacyjno-technologiczne urządzenia, sieci, usługi i dobra, zwana jest infrastrukturą krytyczną. Naruszenie lub zniszczenie elementów tej infrastruktury mogłoby spowodować poważne skutki dla zdrowia, bezpieczeństwa państwa i jego obywateli, ich zdrowia, a także dla skutecznego funkcjonowania organów władzy i administracji publicznej oraz instytucji i przedsiębiorstw.

Infrastruktura krytyczna jest stosunkowo złożona i funkcjonalnie zależna. Obejmuje między innymi: system zaopatrzenia w energię, surowce energetyczne, systemy wodociągowo-kanalizacyjne i dystrybucji żywności, sektor bankowo-finansowy, systemy transportowe i komunikacyjne, system produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych, a także systemy teleinformatyczne wchodzące w obszar szeroko rozumianych usług informacyjnych i telekomunikacyjnych.

W niniejszym artykule ograniczono się do omówienia kluczowych aktywów Ministerstwa Spraw Wewnętrznych i Administracji, dotyczących obszaru teleinformatyki jako jednego z newralgicznych elementów infrastruktury krytycznej państwa. Wskazano podstawowe wymagania dla stworzenia i utrzymywania bezpiecznej infrastruktury TI, rozumianej jako zachowanie poufności, integralności, dostępności informacji oraz rozliczalności zdarzeń [13], a także określono listę zagrożeń dla tych aktywów i ich podatności na te zagrożenia. Pozwoliło to na zidentyfikowanie ryzyka, jego oszacowanie i wskazanie obszarów wymagających zabezpieczenia.

ROLA SYSTEMÓW TI W INFRASTRUKTURZE KRYTYCZNEJ

Współczesna infrastruktura informatyczna połączona siecią komputerową niewątpliwie zrewolucjonizowała jakość wymiany informacji i synchronizacji pracy, zarówno administracji publicznej, jak i całego sektora prywatnego. Obecnie zakres zastosowań systemów komputerowych jest stosunkowo szeroki i obejmuje systemy baz danych [1], systemy kon-

troli lotów [2], automatykę przemysłową [3], aplikacje bankowe i giełdowe [4], medyczne systemy monitorujące [5] oraz wiele innych [6] [7]. Sektor administracji publicznej, a także dzisiejsze środowiska biznesowe coraz częściej są zależne od stałego dostępu do informacji [8]. Jednocześnie systemy informatyczne stały się magazynami wartościowych danych, a łatwość przesyłania, przechowywania i przetwarzania tych danych znacząco zwiększyły wydajność pracy sektora prywatnego oraz administracji. Rola systemów teleinformatycznych ciągle rośnie, a stały dostęp do danych i usług coraz częściej okazuje się kluczem do sukcesu w różnorodnych dziedzinach działalności, zarówno sektora publicznego, jak i prywatnego. Wszelkie przestoje w działaniu systemów, te planowane (wynikające z harmonogramów konserwacji sprzętu i oprogramowania) i te nieplanowane (wynikające z różnego rodzaju awarii sprzętu, błędów użytkowników, ataków wewnętrznych i zewnętrznych na elementy infrastruktury teleinformatycznej), mają decydujący wpływ na jakość funkcjonowania organów państwa oraz na ostateczny bilans finansowy przedsiębiorstwa. Jednogodzinny przestój systemu lub brak dostępu do jego zasobów może obniżać sprawność organów państwa odpowiedzialnych za bezpieczeństwo, a jego koszt może sięgać setek tysięcy, a nawet milionów dolarów. Szczególnie widoczne jest to w przypadku przedsiębiorstw zajmujących się handlem elektronicznym, gdy nawet krótkie przestoje mogą być dla firmy kompromitujące i przynieść niepowetowane straty.

Ze względu na dynamiczny rozwój technologii informacyjnych, w tym teleinformatycznych, a także powszechne stosowanie ich niemal w każdej dziedzinie życia, infrastruktura krytyczna w znacznym stopniu jest zależna od sprawnego działania systemów teleinformatycznych, których funkcjonowanie jest uwarunkowane choćby stałą dostawą energii elektrycznej. Z kolei dostawa energii elektrycznej jest uzależniona od innych elementów infrastruktury, takich jak np. szlaki komunikacyjne, którymi przewozi się surowce do elektrowni. Nietrudno się domyśleć, że praktycznie większość elementów infrastruktury krytycznej tworzy wzajemnie zależny system naczyń połączonych. Wdrażane i stosowane zaawansowane technologie są stosunkowo wrażliwe na awarie, których przyczyny mogą być inne niż tylko zawodność urządzeń. Mogą to być także błędy ludzi, anomalie pogodowe czy też ataki fizyczne i komputerowe, często związane z cyberprzestępczością, a nawet cyberterroryzmem.

MATERIALNE AKTYWA TELEINFORMATYKI MSWiA

Kluczowe dla sprawnego funkcjonowania organów władzy i administracji publicznej oraz bezpieczeństwa państwa i jego obywateli stają się systemy teleinformatyczne, stanowiące część infrastruktury krytycznej. Bez właściwego ich działania trudno byłoby sprawnie wykonywać zadania i gwarantować bezpieczeństwo życia i zdrowia obywateli, a także chronić wszelkie dobra środowiskowe i finansowe.

W celu zapewnienia funkcjonowania MSWiA i podległych mu organów w sposób redukujący zagrożenia bezpieczeństwa państwa i porządku publicznego, należałoby zidentyfikować przede wszystkim zbiór zasobów TI, których uszkodzenie mogłoby spowodować istotne zagrożenie bezpieczeństwa państwa i jego obywateli.

Do podstawowych aktywów MSWiA, w tym zasobów teleinformatycznych podległych służb, takich jak Policja, Straż Graniczna, Państwowa Straż Pożarna, należy zaliczyć[1]:

- systemy informacyjne użytkowane przez organy władzy i administracji publicznej – Centralną Ewidencję Pojazdów i Kierowców (CEPiK), Centralny Bank Danych Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL), Krajowy System Informacyjny Policji (KSIP), Zintegrowany System Ewidencyjny Straży Granicznej (ZSE), System Ewidencji Paszportowej (SEP), systemy informatyczne przechowujące dane daktyloskopijne i profile DNA (AFIS, DAKTYL, CODIS);
- systemy teletransmisyjne[2], umożliwiające określonym organom wymieniać informacje – rozległą sieć teletransmisyjną Policji

1) Z uwagi na publiczny charakter publikacji w artykule nie wymieniono wszystkich systemów informacyjnych, teletransmisyjnych, telekomunikacyjnych i łączności bezprzewodowej użytkowanych przez MSWiA oraz służby podległe, a także nie opisano ich specyfiki działania.

2) Przez określenie „sieć transmisji danych" należy rozumieć sieć IP, na bazie której następuje wymiana danych na podstawie protokołu TCP/IP, zaś przez określenie „sieć teletransmisyjna" należy rozumieć sieć rozległą podkładową, szkieletową; wszystkie sieci teletransmisyjne łącznie tworzą jeden system podkładowy dla sieci warstw wyższych.

POLWAN (sieć szkieletowa, międzywojewódzka), warszawską sieć szkieletową (SDH), wojewódzkie sieci teletransmisyjne Policji (w tym sieci miejskie MAN), policyjną sieć transmisji danych (PSTD), sieć transmisji danych Biura Kryminalnego KGP (UMR--WAN), sieć transmisji danych TESTA (krajowa domena), sieć transmisji danych PESEL-NET, sieć transmisji danych Straży Granicznej (TP SA);

- systemy telekomutacyjne – system telekomutacyjny łączności resortowej, w tym podsystem łączności bezprzewodowej, podsystemy utajnionej łączności telekopiowej, podsystem wideokonferencyjny oraz podsystem telegraficznej łączności szyfrowej;
- systemy łączności bezprzewodowej – resortowy podsystem łączności bezprzewodowej, konwencjonalny system sieci stacji bazowych, systemy trankingowe, systemy satelitarne, wojewódzkie sieci radioliniowe do transmisji danych oraz łącza radioliniowe w ramach innych systemów, systemy komórkowe głosowe oraz systemy transmisji danych w sieci komórkowej, urządzenia bezprzewodowego dostępu do Internetu, systemy lokalizacji i monitoringu oraz system krótkofalowy Policji.

Wymienione aktywa[3] są niezwykle istotne w kontekście możliwości realizacji zadań zarówno przez MSWiA, jak i przez podległe mu służby odpowiedzialne za bezpieczeństwo obywateli i porządek publiczny. Tym samym stanowią one część infrastruktury krytycznej w zakresie ochrony bezpieczeństwa i porządku publicznego, a także ochrony granic, przeciwpożarowej i bezpieczeństwa państwa.

Należy pamiętać również o tym, że bezpieczeństwo infrastruktury krytycznej państwa jest zależne nie tylko od niezakłóconego działania systemów teleinformatycznych, lecz także od zasobów ludzkich i kadrowych, warunkujących sprawność działania całej infrastruktury. I dlatego niezwykle istotne staje się zapewnienie, że wykonawcy oraz użytkownicy systemów TI rozumieją swoje obowiązki, a ich kwalifikacje są odpowiednie do wyznaczonych im ról. Ponadto, ważne jest także zredukowanie ryzyka kradzieży, naruszenia oraz niewłaściwego korzystania z urządzeń teleinformatycznych [11][12].

Naturalną konsekwencją rozwoju i upowszechniania się technologii informacyjnych jest powstawanie nowych zagrożeń dla funkcjonowania państwa [9].

Zagwarantowanie bezpieczeństwa infrastruktury krytycznej w obszarze teleinformatyki ma na celu zapewnienie odpowiednio wysokiego poziomu ochrony aktywów TI MSWiA, obejmujących informacje wytwarzane, przetwarzane, przesyłane i przechowywane z wykorzystaniem systemów informacyjnych, teletransmisyjnych, telekomutacyjnych i bezprzewodowych.

Podstawowym wymaganiem dla zapewnienia bezpieczeństwa teleinformatycznego infrastruktury krytycznej jest bezpieczeństwo informacji. Oznacza ono zachowanie następujących atrybutów bezpieczeństwa [13]:

- **poufności**, czyli ochronę przed ujawnieniem informacji nieuprawnionemu odbiorcy;
- **integralności**, co oznacza ochronę przed modyfikacją lub zniekształceniem informacji przez osobę nieuprawnioną;
- **dostępności**, co oznacza gwarancję uprawnionego dostępu do informacji zawsze, gdy jest to niezbędne;
- **rozliczalności**, co oznacza możliwość określenia i weryfikacji odpowiedzialności za działania, usługi i realizowane funkcje.

Informacje wytwarzane, przetwarzane, przechowywane i przesyłane z wykorzystaniem wymienionych systemów są zasobem, który charakteryzuje się najwyższym poziomem wrażliwości. Do pochodnych zasobów, które mogą być zagrożone w wyniku przełamania zabezpieczeń związanych z poufnością, integralnością, dostępnością danych przetwarzanych w wymienionych systemach oraz z rozliczalnością zdarzeń można zaliczyć:

3) W dalszej części artykułu pojęcie aktywów będzie utożsamiane z pojęciem zasobów rozumianych zgodnie z [13].

- Z1. Poczucie bezpieczeństwa obywateli.
- Z2. Autorytet państwa.
- Z3. Prestiż MSWiA.

Aktywa TI MSWiA, w tym systemy informacyjne, teletransmisyjne, telekomutacyjne i bezprzewodowe oraz informacje w nich przetwarzane są narażone na zagrożenia, które mogą zaszkodzić bezpieczeństwu państwa. Szkoda może powstać jako skutek bezpośredniego lub pośredniego ataku na przetwarzaną informację lub usługę teleinformatyczną, np. uszkodzenie, ujawnienie, modyfikacja, utrata informacji, usługi lub jej dostępności. Aby wyrządzić szkodę, wykorzystuje się podatności zasobów. Należy więc identyfikować zagrożenia oraz określić ich poziom i prawdopodobieństwo powstania. Podatność związana z zasobami teleinformatycznymi MSWiA oznacza pewną słabość fizyczną, organizacyjną, proceduralną, osobową, zarządzania, administrowania, sprzętu komputerowego, oprogramowania lub informacji. Może ona być wykorzystana przez zagrożenie, które oddziałuje na zasoby i powoduje wystąpienie zdarzenia zakłócającego lub wręcz uniemożliwiającego wykonanie zadań postawionych MSWiA i podległym mu służbom. Podatność nie powoduje szkody, ale jest warunkiem lub zbiorem warunków, które mogą umożliwić zagrożeniu oddziaływanie na zasoby. Podatności mogą pochodzić z różnych źródeł, np. wewnętrznych względem zasobu i mogą istnieć, dopóki same zasoby nie zmienią się w taki sposób, że podatność nie będzie się już do nich odnosić. Podatności oznaczają te słabości aktywów TI MSWiA, które mogą być wykorzystane i mogą prowadzić do niepożądanych skutków. Stanowią możliwości, które pozwalają zagrożeniu wyrządzić szkodę. Należy monitorować wszystkie podatności, aby zidentyfikować te, które stanowią dotychczasowe lub nowe potencjalne zagrożenie.

Zagrożenia mogą mieć pochodzenie **ludzkie zamierzone** i mogą być przypadkowe lub **rozmyślne** [14]. Do rozmyślnych można zaliczyć usiłowanie uzyskania dostępu do informacji przez osoby mające odpowiednią wiedzę i doświadczenie. W tej grupie mieszczą się również działania legalnych użytkowników, osób konserwujących sprzęt, gości, a także innych osób lub organizacji zainteresowanych informacjami dostępnymi w ramach aktywów TI MSWiA. Zagrożenia tego typu mogą być spowodowane również

przypadkowo przez każdego użytkownika, który ma dostęp do zasobów systemów teleinformatycznych MSWiA. Mogą być również **wywołane czynnikami technicznymi** lub **środowiskowymi** (naturalne). Do takich zagrożeń można zaliczyć awarie urządzeń systemów TI.

Wstępna analiza aktywów MSWiA z obszaru bezpieczeństwa i porządku publicznego, stanowiących elementy infrastruktury krytycznej, pozwala na sformułowanie następującej listy zagrożeń dla bezpieczeństwa systemów teleinformatycznych [14]:

- ZP1. Utrata poufności lub uszkodzenie danych przechowywanych w systemach informacyjnych.
- ZP2. Utrata dostępności informacji przechowywanych w systemach informacyjnych lub w wyniku uszkodzenia elektronicznych nośników informacji.
- ZP3. Utrata integralności informacji przechowywanych w systemie informacyjnym.
- ZP4. Utrata poufności i integralności informacji przesyłanych z wykorzystaniem systemów teletransmisyjnych, telekomutacyjnych i bezprzewodowych.
- ZP5. Utrata dostępności informacji przesyłanych z wykorzystaniem systemów teletransmisyjnych, telekomutacyjnych i bezprzewodowych.
- ZP6. Uniemożliwienie rozliczalności działań przeprowadzanych w systemach teleinformatycznych.

Zagrożenia ludzkie zewnętrzne (ZLZ), spowodowane celowym lub przypadkowym działaniem osób nieuprawnionych, mogą być wynikiem:

- ZLZ1. Ataku terrorystycznego na obiekty, w których są zainstalowane podstawowe urządzenia systemów teleinformatycznych; zdalnego wprowadzenia do systemu oprogramowania złośliwego; zdalnego uzyskania uprawnień; ataku impulsem elektromagnetycznym; użycia materiałów wybuchowych.
- ZLZ2. Zdalnego lub bezpośredniego skopiowania danych lub kradzieży nośników, na których dane te są przechowywane.
- ZLZ3. Podsłuchu łączy teletransmisyjnych, telekomutacyjnych i bezprzewodowych; podszycia się pod uprawnionego użytkow-

nika; skopiowania wydruków; przejmowania ulotu elektromagnetycznego.

- ZLZ4. Zablokowania linii teletransmisyjnej lub telekomutacyjnej; przeciążenia systemu informacyjnego w wyniku generowania dużej ilości wiadomości lub niedostępności usług telekomunikacyjnych z powodu zaniechania działań przez dostawcę usługi lub ze względu na awarię łączy telekomunikacyjnych.
- ZLZ5. Odcięcia zasilania podstawowych urządzeń systemów teleinformatycznych w wyniku przerwy w dostawach energii elektrycznej, spowodowanej zaniechaniem działań dostawcy lub awarią infrastruktury.
- ZLZ6. Celowego modyfikowania informacji w czasie ich przesyłania łączami teletransmisyjnymi lub telekomutacyjnymi, generowania zakłóceń w liniach przesyłowych.
- ZLZ7. Celowego wykorzystania błędów oprogramowania urządzeń zabezpieczających, np. typu zapora sieciowa.

Zagrożenia ludzkie wewnętrzne (ZLW), spowodowane celowym lub przypadkowym działaniem osób uprawnionych, mogą być wynikiem:

- ZLW1. Uszkodzenia urządzeń lub oprogramowania systemów TI na skutek działań sabotażowych lub błędów obsługi (błędy utrzymania i eksploatacji); wprowadzenia oprogramowania złośliwego; uzyskania przez uprawnionego użytkownika nieprzysługujących mu uprawnień, np. uzyskania uprawnień administratora, a także użycia oprogramowania przez nieautoryzowanych użytkowników; niewłaściwego użycia zasobów, tzn. niezgodnego z procedurami eksploatacji.
- ZLW2. Nieautoryzowanego skopiowania wszystkich lub wybranych informacji z systemów TI przez nieuprawnionego do takich działań użytkownika, lub skopiowania danych z nośników, na których są one archiwizowane; wprowadzenia oprogramowania złośliwego lub modyfikacji oprogramowania w sposób umożliwiający zdalny dostęp do informacji przechowywanych w systemach TI.
- ZLW3. Przejmowania informacji przesyłanych siecią teletransmisyjną lub telekomutacyjną; uzyskania nieuprawnionego dostępu do terminala innego użytkownika; przypadkowego wysłania niezaszyfrowanych danych.

- ZLW4. Zmodyfikowania zasobów systemów TI przez uprawnionego użytkownika; uzyskania nieprzysługujących uprawnień do wszystkich lub wybranych zasobów systemów TI.
- ZLW5. Uzyskania nierejestrowanego dostępu do zasobów systemu TI; podszycia się pod innego uprawnionego użytkownika; zniszczenia lub modyfikacji rejestrów aktywności określonych składowych systemu TI przez uprawnionego użytkownika lub nieuprawnionego dostępu do tych rejestrów.
- ZLW6. Nielegalnego instalowania oprogramowania niezwiązanego z działalnością MSWiA i funkcjami systemów TI, a także użycia narzędzi sieciowych lub innego oprogramowania w nieautoryzowany sposób.
- ZLW7. Celowego lub spowodowanego błędem obsługi unieruchomienia systemów TI lub wybranych ich składowych, np. urządzeń systemu łączności, zasilania itp.
- ZLW8. Przejmowania i następnie modyfikowania informacji przesyłanych siecią teletransmisyjną lub telekomutacyjną.

Zagrożenia wywołane czynnikami środowiskowymi mogą być wynikiem utraty dostępności informacji i usług systemów TI, spowodowanej wystąpieniem powodzi, pożaru, wyładowań atmosferycznych itp. Na przykład uderzenie pioruna w budynek, w którym znajdują się elementy systemu TI, może spowodować pożar lub awarię infrastruktury teleinformatycznej na skutek wystąpienia przepięć w sieci energetycznej. Zagrożenia spowodowane czynnikami środowiskowymi i technicznymi są związane przede wszystkim z możliwością utraty lub uszkodzenia danych dostępnych w systemach TI. Na przykład awaria komputerów, serwerów, pamięci masowych, elementów sieci komputerowej lub innych urządzeń TI wynikająca z wad sprzętu, a także awarie spowodowane błędami programistów niewykryte podczas testów mogą spowodować brak dostępu do zasobów krytycznej infrastruktury TI.

Najważniejszym zasobem niematerialnym aktywów TI MSWiA i podległych służb jest poczucie bezpieczeństwa obywateli. Nie mniej ważny jest autorytet państwa i prestiż MSWiA. Środki ochrony powinny być skierowane na ochronę zasobów krytycznych dla bezpieczeństwa obywateli i obarczonych największym ryzykiem.

Z uproszczonej analizy ryzyka[4] dla aktywów TI MSWiA stanowiących część infrastruktury krytycznej wynikają następujące priorytety ochrony atrybutów bezpieczeństwa:

- Poufność i integralność informacji przesyłanych oraz przechowywanych w systemach TI.
- Dostępność informacji i usług realizowanych przez systemy teleinformatyczne.
- Rozliczalność działań przeprowadzanych w systemach TI.

Klasyfikację przedstawiono od najwyższego (3) do najniższego (1) priorytetu.

WYMAGANIA W ZAKRESIE ZABEZPIECZENIA

W celu zapewnienia bezpieczeństwa infrastruktury krytycznej w obszarze aktywów teleinformatycznych MSWiA należy podjąć wszelkie kroki w kierunku zabezpieczenia informacji, przetwarzanych w systemach informacyjnych i przesyłanych za pośrednictwem systemów telekomunikacyjnych, przed nieautoryzowanym dostępem i zmianami.

Biorąc pod uwagę zidentyfikowane zagrożenia i przeprowadzoną wstępną analizę ryzyka, można sformułować następujące ogólne wymagania dla zapewnienia bezpieczeństwa aktywów TI MSWiA w infrastrukturze krytycznej [11]:

- Stosowanie środków ochrony fizycznej biur, pomieszczeń i urządzeń stanowiących część aktywów TI IK.
- Zapewnienie, że sprzęt TI jest rozlokowany lub chroniony w taki sposób, aby redukować ryzyka wynikające z zagrożeń i niebezpieczeństw środowiskowych oraz z nieautoryzowanego dostępu.
- Zapewnienie, że sprzęt czasowo użytkowany poza strefami obiektów MSWiA lub służb podległych jest odpowiednio chroniony z uwzględnieniem występującego w takich warunkach ryzyka.
- Zapewnienie, że obowiązki i zakresy odpowiedzialności są rozdzielone w celu ograniczenia możliwości nieuprawnionej lub nieumyślnej modyfikacji lub niewłaściwego użycia aktywów TI MSWiA.
- Określenie i regularne przeglądanie wymagań dotyczących umów

o zachowaniu poufności i nieujawnianiu informacji, z uwzględnieniem potrzeb MSWiA oraz podległych służb w zakresie ochrony informacji.

- Zapewnienie, że umowy ze stronami trzecimi, dotyczące dostępu, przetwarzania, przekazywania lub zarządzania informacjami należącymi do MSWiA i służb podległych lub środkami przetwarzania informacji, lub dodania produktów lub usług do środków przetwarzania informacji, obejmują wszystkie wymagania bezpieczeństwa.
- Zapewnienie, że role i zakresy odpowiedzialności pracowników, wykonawców oraz użytkowników reprezentujących stronę trzecią są w zakresie bezpieczeństwa określone i udokumentowane zgodnie z polityką bezpieczeństwa informacji w MSWiA i służbach podległych.
- Regularne informowanie o uaktualnieniach obowiązujących w MSWiA i służbach podległych polityk i procedur, które są związane z wykonywaną przez nich pracą.
- Wprowadzenie odpowiedzialności kierownictwa oraz procedur zapewniających szybką, skuteczną i uporządkowaną reakcję na incydenty związane z bezpieczeństwem informacji.
- Zapewnienie, że wszyscy pracownicy MSWiA i służb podległych oraz – tam gdzie jest to wskazane – wykonawcy i użytkownicy reprezentujący stronę trzecią są przeszkoleni.
- Zapewnienie, że wszyscy pracownicy, wykonawcy i użytkownicy reprezentujący stronę trzecią zwracają organizacji wszystkie posiadane aktywa w momencie zakończenia stosunku pracy, kontraktu lub umowy, a ich wszelkie uprawnienia związane z dostępem do zasobów wygasają.

---

4) Z uwagi na publiczny charakter publikacji w artykule nie przedstawiono szczegółowej analizy ryzyka poprzez wskazanie kluczowych ryzyk wynikających z podatności na zagrożenia głównych zasobów teleinformatycznych MSWiA, a także nie wskazano najbardziej prawdopodobnych i najbardziej dotkliwych w skutkach scenariuszy zagrożeń (*disaster scenario*), dla których powinien być opracowany plan zapewnienia ciągłości działania. Z tego samego powodu nie przedstawiono również analizy podatności poprzez ocenę prawdopodobieństwa wystąpienia danego zagrożenia oraz ocenę jego wpływu na dany zasób TI. Zgodnie z metodyką TRA (*Threat and Risk Analysis*) nie podano także zestawienia ilościowych ocen prawdopodobieństwa wystąpienia zagrożenia w celu uzyskania ilościowej oceny stopnia ryzyka.

- Zapewnienie, że urządzenia rozwojowe, testowe i eksploatacyjne są rozdzielone, aby zredukować ryzyko nieupoważnionego dostępu lub zmian w systemach eksploatacyjnych.
- Monitorowanie wykorzystania zasobów oraz przewidywanie przyszłej pojemności systemów TI, aby zapewnić ich właściwą wydajność.
- Zapewnienie, że procedury monitorowania użycia środków przetwarzania informacji oraz wyniki działań monitorujących są regularnie przeglądane.
- Zapewnienie, że prace rozwojowe nad oprogramowaniem, powierzone firmie zewnętrznej, są nadzorowane i monitorowane.
- Zapewnienie, że wszelkie wymagania wynikające z ustaw, zarządzeń i umów oraz podejście organizacji do ich wypełniania są wyraźnie określone, udokumentowane i aktualizowane dla każdego systemu TI.

W tabeli 1 przedstawiono propozycję wybranych zabezpieczeń, odpowiednio do atrybutów bezpieczeństwa i zidentyfikowanych zagrożeń dla bezpieczeństwa aktywów teleinformatycznych MSWiA, stanowiących część IK.

Utrzymanie bezpieczeństwa IK w aspekcie teleinformatycznym powinno również uwzględniać następujące wymagania w odniesieniu do środków zaradczych:

- Opracowanie i utrzymywanie zarządzanego procesu zapewnienia ciągłości działania w MSWiA i służbach podległych, które określają wymagania bezpieczeństwa informacji potrzebne do zapewnienia ciągłości działania.
- Wdrożenie procedur postępowania z informacjami oraz ich przechowywania w celu ochrony informacji przed nieautoryzowanym ujawnieniem lub niewłaściwym użyciem.
- Opracowanie i wdrożenie planów utrzymania lub odtworzenia działalności, zapewniających dostępność informacji na wymaganym poziomie i w wymaganym czasie po wystąpieniu przerwy lub awarii krytycznych.
- Zapewnienie, że wymagania odnoszące się do elementów bezpieczeństwa, poziomu usług oraz zarządzania wszystkimi usługami sieciowymi są określone i włączone do odpowiednich umów na do-

Tabela 1. Powiązania w infrastrukturze telekomunikacyjnej

Zapewnienie	*Atrybut bezpieczeństwa*	*Priorytet ochrony*[5]	*Zabezpieczenie (wybrane środki zaradcze)*
ZP1 ZLZ1, ZLZ2, ZLZ7, ZLW2	Poufność	3	- Stosowanie mechanizmów zabezpieczających, zwłaszcza kryptograficznych, zapewniających bezpieczeństwo informacji w długim okresie, lub pozwalających na zwiększenie ich siły. - Stosowanie środków umożliwiających automatyczną identyfikację urządzeń jako środka uwierzytelniania połączeń z określonych lokalizacji lub urządzeń. - Zapewnienie, że prawa dostępu pracowników, wykonawców, użytkowników reprezentujących stronę trzecią do informacji i środków przetwarzania informacji są odbierane w momencie zakończenia stosunku pracy, kontraktu lub umowy lub modyfikowane zgodnie z zaistniałymi zmianami zatrudnienia. - Zapewnienie, że wszystkie składniki sprzętu zawierające nośniki informacji są sprawdzane, aby przed jego zbyciem upewnić się, że wszystkie informacje wrażliwe i licencjonowane oprogramowanie zostały usunięte lub bezpiecznie nadpisane. - Zapewnienie, że sprzęt TI, informacje lub oprogramowanie nie są wynoszone z obszarów chronionych bez uprzedniego zezwolenia.

5) Wartość „1" – priorytet niski, wartość „2" – priorytet średni, wartość „3" – priorytet wysoki.

Zapewnienie	*Atrybut bezpieczeństwa*	*Priorytet ochrony*	*Zabezpieczenie (wybrane środki zaradcze)*
ZP2 ZLZ1, ZLZ4, ZLZ5, ZLW1, ZLW7	Dostępność	2	- Zapewnienie, że sprzęt TI jest prawidłowo konserwowany, aby zapewnić jego ciągłą dostępność i integralność. - Stosowanie środków ochrony fizycznej aktywów TI przed zniszczeniami powstałymi na skutek pożaru, zalania, trzęsienia ziemi, wybuchu, niepokojów społecznych i innych naturalnych lub spowodowanych przez człowieka katastrof. - Stosowanie środków zapewniających, że sprzęt TI jest chroniony przed awariami zasilania lub zakłóceniami spowodowanymi awariami systemów wspomagających. - Stosowanie środków umożliwiających automatyczną identyfikację urządzeń jako środka uwierzytelniania połączeń z określonych lokalizacji lub urządzeń. - Stosowanie mechanizmów weryfikacji uprawnień i realizacji kontroli dostępu do zmagazynowanych informacji o różnych klauzulach tajności. - Wdrożenie zabezpieczeń zapobiegających, wykrywających i usuwających kod złośliwy oraz stosowanie właściwych procedur uświadamiania użytkowników. - Zapewnienie, aby nie było możliwości wyłączenia zabezpieczeń dostępu do zasobów systemów teleinformatycznych przez jedną osobę.

Zapewnienie	*Atrybut bezpieczeństwa*	*Priorytet ochrony*	*Zabezpieczenie (wybrane środki zaradcze)*
ZP3 ZLZ7, ZLW1, ZLW3, ZLW4, ZLW5, ZLW6	Integralność	3	- Stosowanie środków zapewniających autentyczność przesyłanych informacji oraz uwierzytelnianie nadawcy i odbiorcy. - Zapewnienie, że informacje zawarte w transakcjach on-line są chronione, aby zapobiegać niekompletności transmisji, błędnemu rutingowi, nieautoryzowanym zmianom, nieautoryzowanemu ujawnieniu, nieautoryzowanemu kopiowaniu i powtórzeniu. - Zapewnienie, że integralność informacji umieszczanych w publicznie dostępnych systemach jest zagwarantowana, aby zapobiec nieuprawnionej modyfikacji poprzez stosowanie np. rozwiązań kryptograficznych. - Zapewnienie, że zegary wszystkich stosownych systemów przetwarzania informacji w organizacji lub domenie są synchronizowane z uzgodnionym, dokładnym źródłem czasu. - Wdrożenie zabezpieczeń zapobiegających, wykrywających i usuwających kod złośliwy oraz stosowanie właściwych procedur uświadamiania użytkowników.

Zapewnienie	*Atrybut bezpieczeństwa*	*Priorytet ochrony*	*Zabezpieczenie (wybrane środki zaradcze)*
ZP4 ZLZ2, ZLZ3, ZLZ6, ZLW1, ZLW2, ZLW3, ZLW6, ZLW8	Poufność i Integralność	3	- Zapewnienie poufności i integralności informacji przetwarzanych na poszczególnych stanowiskach pracy mających dostęp do systemów informacyjnych i teletransmisyjnych poprzez wdrożenie rozwiązań kryptograficznych. - Stosowanie środków umożliwiających automatyczną identyfikację urządzeń jako środka uwierzytelniania połączeń z określonych lokalizacji lub urządzeń. - Zapewnienie, że prawa dostępu pracowników, wykonawców, użytkowników reprezentujących stronę trzecią do informacji i środków przetwarzania informacji są odbierane w momencie zakończenia stosunku pracy, kontraktu lub umowy lub modyfikowane zgodnie z zaistniałymi zmianami zatrudnienia. - Stosowanie mechanizmów weryfikacji uprawnień i przeprowadzania kontroli dostępu do urządzeń przetwarzających dane o różnych klauzulach tajności. - Zapewnienie, że zegary wszystkich stosownych systemów przetwarzania informacji w organizacji lub domenie są synchronizowane z uzgodnionym, dokładnym źródłem czasu. - Zapewnienie, że sieci TI są odpowiednio zarządzane i nadzorowane, aby ochronić je przed zagrożeniami, a także, aby utrzymać bezpieczeństwo systemów i aplikacji używających sieć, z uwzględnieniem przesyłanych informacji.

Zapewnienie	*Atrybut bezpieczeństwa*	*Priorytet ochrony*	*Zabezpieczenie (wybrane środki zaradcze)*
ZP5 ZLZ1, ZLZ4, ZLZ5, ZLW1, ZLW2, ZLW3, ZLW5, ZLW7	Dostępność	2	- Stosowanie środków zapewniających, że okablowanie zasilające i telekomunikacyjne służące do przesyłania danych lub wspomagające usługi informacyjne w ramach IK jest chronione przed przejęciem lub uszkodzeniem. - Zapewnienie, aby nie było możliwości wyłączenia zabezpieczeń dostępu do zasobów systemów teleinformatycznych przez jedną osobę.

Zapewnienie	*Atrybut bezpieczeństwa*	*Priorytet ochrony*	*Zabezpieczenie (wybrane środki zaradcze)*
ZP6 ZLZ1, ZLZ3, ZLW3, ZLW4, ZLW5, ZLW6, ZLW8	Rozliczalność	1	- Zapewnienie, że wszystkie informacje i aktywa TI związane ze środkami przetwarzania informacji mają właściciela (osoba lub podmiot, który ma zatwierdzoną kierowniczą odpowiedzialność za sterowanie produkcją, rozwój, utrzymanie, korzystanie i bezpieczeństwo aktywów) w postaci wyznaczonej części organizacji MSWiA i służb podległych. - Stosowanie metod uwierzytelniania zapewniających rozliczalność działań wykonywanych w systemach informacyjnych, teletransmisyjnych, telekomutacyjnych i bezprzewodowych z możliwością wskazania w sposób niezaprzeczalny osoby i czynności. - Zapewnienie, że działania administratorów i operatorów systemów są rejestrowane, błędy są rejestrowane i analizowane oraz że są podejmowane odpowiednie działania. - Zapewnienie, że przyznawanie i odbieranie dostępu do wszystkich systemów informacyjnych i usług TI opiera się na formalnej procedurze rejestrowania i wyrejestrowywania użytkowników. - Zapewnienie rozliczalności działań użytkowników, w tym działań z uprawnieniami administratora. - Zapewnienie, że zmiany w środkach przetwarzania informacji i systemach TI są kontrolowane. - Zapewnienie, że sprzęt TI, informacje lub oprogramowanie nie są wynoszone z obszarów chronionych bez uprzedniego zezwolenia.

starczanie usług TI, niezależnie od tego, czy są realizowane własnymi środkami, czy zlecane na zewnątrz.
- Zapewnienie, że zabezpieczenia, definicje usług oraz poziomy dostaw zawarte w umowach serwisowych ze stronami trzecimi są wdrożone, wykonywane i utrzymywane przez stronę trzecią.
- Opracowanie i wdrożenie formalnych polityk wymiany informacji, procedur i zabezpieczeń w celu ochrony wymiany informacji przekazywanej za pomocą wszelkich rodzajów środków komunikacji.
- Opracowanie i wdrożenie polityki i procedury ochrony informacji związanych z połączeniami między systemami informacyjnymi.
- Określenie, udokumentowanie i wdrożenie zasad dopuszczalnego korzystania z informacji oraz aktywów TI MSWiA związanych ze środkami przetwarzania informacji.

PODSUMOWANIE

Pomijane sfery wymiany informacji między poszczególnymi służbami, a także marginalne traktowanie infrastruktury TI wykorzystywanej przez MSWiA oraz podległe służby może doprowadzić do sytuacji, w której zapewnienie bezpieczeństwa państwa i jego obywateli, a także skuteczne funkcjonowanie organów władzy i administracji publicznej będzie niemożliwe.

Płaszczyzna bezpieczeństwa narodowego w aspekcie infrastruktury krytycznej staje się coraz bardziej zależna od swobodnego przepływu informacji i od zachowania systemów bazujących na informacjach. Niezbędne zatem dla bezpieczeństwa państwa staje się wprowadzenie polityk bezpieczeństwa informacyjnego, zapewniających ochronę istniejących systemów teleinformatycznych i gwarantujących państwu oraz chronionym przez nie podmiotom posiadanie, przetrwanie i swobodę rozwoju.

W celu zagwarantowania bezpieczeństwa aktywów teleinformatycznych MSWiA oraz służb podległych, w tym obniżenia ryzyka utraty poufności, integralności i dostępności przetwarzanych danych, a także rozliczalności zachodzących zdarzeń, niezwykle ważne może się okazać wdrożenie wymienionych środków ochrony.

Literatura

[1] Barga R., Lomet D., Baby T., Agrawal S., *Persistent client-server database sessions, Advanced in database Technology-EDBT 2000, Proceedings Lecture Notes in Computer Science*, 1777: 462–477, 2000.

[2] Aleksa B. D., Carter J. P., *Boeing 777 Airplane Information Management System Operational Experience*, AIAA/IEEE Digital Avionics Systems Conference, Vol. II, pp. 3.1–21–3.1–27, 1997.

[3] Docquier N., Candel S., *Combustion control and sensors: a review, Progress in Energy and Combustion Science*, 28 (2):107–150, 2002.

[4] Delco M., and Lonescu M., *xProxy: A transparent caching and delta transfer system for web objects,* http://www.cs.pdx.edu/~delco/xproxy.ps.gz, UC Berkeley class project: CS262B/CS268, May 2000.

[5] Wan D., *Magic Medicine Cabinet: A Situated Portal for Consumer Healthcare, in Proceedings of First International Symposium on Handheld and Ubiquitous Computing (HUC '99)*, September 1999.

[6] Malamos A., Malamas E., Varvarigou T., Ahuja S., *A model for availability of quality of service in distributed multimedia systems, Multimedia Tools and Applications,* 16 (3): 207–230, Mar 2002.

[7] Malloy A., Varshney U., Snow A., *Supporting mobile commerce applications using dependable wireless networks, Mobile Networks & Applications*, 7 (3): 225–234 Jun 2002.

[8] Zasępa T., *Fenomen społeczeństwa informacyjnego,* praca zbiorowa pod redakcją ks. prof. Tadeusza Zasępy, Edycja Świętego Pawła.

[9] Kośla R., *Ochrona infrastruktury krytycznej w Polsce – aktualny stan prac*, materiał dostępny na stronie http://www.cert.pl/PDF/Kosla_p.pdf.

[10] *EAPC/PfP Workshop on Critical Infrastructure Protection & Civil Emergency Planning: Dependable Structures, Cybersecurity and Common Standards*, Zurich, Switzerland 9–11 September 2004.

[11] *PN-ISO/IEC 27001:2007 – Technika informatyczna. Techniki bezpieczeństwa. Systemy Zarządzania Bezpieczeństwem Informacji – Wymagania.*

[12] *PN-ISO/IEC 17799 Technologie informacyjne. Zasady postępowania* w zarządzaniu bezpieczeństwem informacji.

[13] *PN-I-13335-1 Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych.*

[14] *ISO/IEC TR 13335-3 Information technology – Guidelines for the management of IT Security - Part 3: Techniques for the management of IT Security.*