WYMAGANIA TECHNOLOGICZNE DLA BEZPIECZEŃSTWA KOMERCYJNYCH SYSTEMÓW TELEINFORMATYCZNYCH

Dariusz Bogusz

WYMAGANIA TECHNOLOGICZNE
Obszar publiczny

Wymagania technologiczne dla bezpieczeństwa komercyjnych systemów teleinformatycznych:

- *Co to jest komercyjny system teleinformatyczny?*
- *Architektury sieci IT. Cechy bezpieczeństwa w systemach komercyjnych. Kiedy system jest bezpieczny?*
- *Technologie stosowane do zarządzania zagrożeniami.*

WPROWADZENIE

W dziedzinie działalności społecznej wyróżniamy organizacje rządowe, stowarzyszenia non-profit i organizacje komercyjne. Organizacje rządowe (np. wojsko, policja) zaspokajają podstawowe i powszechne potrzeby społeczne. Przykładem takich potrzeb jest zapewnienie bezpieczeństwa zewnętrznego i wewnętrznego. Organizacje pozarządowe, takie jak stowarzyszenia non-profit, zaspokajają ważne potrzeby społeczne pewnych grup i środowisk, np. stowarzyszenia rozwoju regionalnego, stowarzyszenia wspierające pracę niepełnosprawnych. Głównym natomiast celem istnienia organizacji komercyjnych jest przynoszenie zysku swojemu właścicielowi.

Jest to jednak możliwe wyłącznie poprzez zaspokajanie potrzeb społecznych, za które ktoś jest skłonny zapłacić (np. potrzeba komunikacji między ludźmi w wypadku operatorów telekomunikacyjnych). Z punktu widzenia działalności bieżącej, organizacje non-profit działają w ten sam sposób jak organizacje komercyjne, jednak realizacja ich misji społecznej

ma wyższy priorytet niż przynoszenie zysku (z założenia nie przynoszą zysku, inwestując maksimum środków w realizację misji). Peter F. Drucker [1] proponuje traktować je jak organizacje komercyjne.

Podstawowym zagadnieniem ekonomicznym, z jakim spotykają się przedsiębiorstwa, jest osiągnięcie trwałej przewagi konkurencyjnej. We współczesnym świecie ekonomia opiera się głównie na przetwarzaniu informacji. Działalność bieżąca wiąże się więc z jej pozyskiwaniem, przechowywaniem i przetwarzaniem. Na potrzeby niniejszej pracy przyjmiemy, że komercyjny system teleinformatyczny to całość środków technicznych i organizacyjnych, które służą pozyskiwaniu, przechowywaniu i przetwarzaniu informacji w celu osiągnięcia zysku ekonomicznego. Wynika stąd dominująca w systemach komercyjnych zasada: nakłady niezbędne do funkcjonowania komercyjnego systemu teleinformatycznego nie mogą być większe niż korzyści odnoszone przez organizację z jego używania. Dotyczy to zarówno samej inwestycji (zakupu), jak i używania (koszty bieżące) bezpiecznego systemu IT.

ARCHITEKTURA SIECI IT

Już w XX wieku stwierdzono, że dla rozwoju systemów IT niezbędna jest standaryzacja i dekompozycja zagadnienia komunikacji pomiędzy systemami IT. Wyczerpujące omówienie istniejących architektur sieci, podobnie jak kompleksowe omówienie wszystkich technologii stosowanych do ich ochrony, wykracza poza ramy niniejszego opracowania. Tutaj przedstawimy tylko technologie i metody najbardziej popularne.

Pierwotnie zestaw referencyjnych modeli dla systemów IT opracowała międzynarodowa organizacja standaryzacyjna OSI. Zaproponowała ona model referencyjny podzielony na warstwy: fizyczną, łącza danych, sieciową, transportową, sesyjną, prezentacyjną i aplikacyjną [2]. Podział na siedem warstw ułatwia dekompozycję zagadnienia, a standaryzacja punktów styku pomiędzy warstwami pozwala abstrahować od implementacji działania poszczególnych warstw. Model ten bywa również nazywany warstwowym modelem OSI. W środowiskach przemysłowych jest uważany za dobrze standaryzowany, ale jego wdrożenie jest skomplikowane. Obecnie najczęściej jest on podstawą wysoce skalowalnych rozwiązań sieci transportowych.

Wraz z przypadającą na lata dziewięćdziesiąte XX wieku popularyzacją sieci Internet znaczenia nabrał prostszy model, oparty na stosie protokołów internetowych TCP/IP. Model TCP/IP [3], nazywany też modelem DoD, został opracowany w latach siedemdziesiątych XX wieku na zlecenie Departamentu Obrony Stanów Zjednoczonych w ramach projektu ARPA Net. Celem projektu było opracowanie odpornych na atak sieci komputerowych, przy czym poważnie brano pod uwagę również bezpieczeństwo w razie ataku jądrowego. Model TCP/IP wyróżnia cztery warstwy: łącza, sieciową, transportową i aplikacyjną. Podobnie jak w modelu OSI, standaryzacji podlegają punkty styku pomiędzy warstwami, a nie implementacja warstwy. Gdy specyfikowano ten model, zagadnienia obsługiwane przez wyższe warstwy modelu OSI nie były standaryzowane dla sieci komputerowych, a więc model TCP/IP zawiera je w warstwie aplikacyjnej.

We współczesnych rozwiązaniach sieci i aplikacji komputerowych najczęściej jest stosowany model TCP/IP. Dzięki otwartości i podatności na zmiany modelu TCP/IP, możliwe stało się standaryzowanie również zagadnień bezpieczeństwa sieciowego, np. protokołów warstwy sieciowej, jak IPsec, czy też warstwy aplikacyjnej, jak TLS.

KOMERCYJNE SYSTEMY TELEINFORMATYCZNE

Jak już wspomniano, funkcje systemów IT są związane z informacjami. Według autora, krytycznym elementem jest właśnie informacja i jej wpływ na zysk organizacji. Tak więc środki służące jej przetwarzaniu muszą być odpowiednio dobrane do cech tejże informacji. Zgodnie z tezami proponowanymi przez za Warrena Petersona i Shrinatha Tandura [12] ważne jest przy tym, aby informacja była:

- poufna co najmniej do momentu, gdy zostanie wykorzystana;
- wiarygodna dla nadawcy i adresata (treść nie może ulec przypadkowej lub celowej zmianie w określonym przedziale czasu);
- dostępna we właściwym czasie dla adresata;
- niezaprzeczalna dla nadawcy i adresata (sam fakt nadania i odebrania przez właściwe osoby, w określonym przedziale czasu nie budzi wątpliwości).

Zachowanie wymienionych warunków wiąże się z osiągnięciem bądź utrzymaniem przewagi konkurencyjnej przez przedsiębiorstwo. Mogą być one realizowane wymiennie metodami technicznymi lub organizacyjnymi. W wypadku systemów komercyjnych rachunek ekonomiczny i cele biznesowe przedsiębiorstwa wyznaczają odpowiedni dobór środków dla osiągnięcia i trwałego utrzymania przewagi konkurencyjnej (w tym zachowania bezpieczeństwa systemów IT). Z tego powodu w organizacjach komercyjnych (np. organizacji autora) stosuje się klasyfikację informacji, następnie dostosowuje sposób jej przetwarzania do takich cech tejże informacji, jak: wpływ na zysk, czas życia, adresat i odbiorca.

Zgodnie z definicją zaproponowaną przez B. Pfitzmanna i M. Waidnera [4] bezpieczny system teleinformatyczny jest definiowany jako wyidealizowane urządzenie, które poprawnie i w całości realizuje tylko i wyłącznie cele zgodne z intencjami właściciela. Jednakże instytucje komercyjne działają w zmiennych warunkach i ich systemy IT muszą spełniać swoje funkcje w bezpieczny sposób niezależnie od zmian w otoczeniu i wewnątrz organizacji. Bezpieczeństwo systemów IT jest procesem, który polega na instalacji systemów bezpieczeństwa, wzmacnianiu, monitorowaniu ich, odpowiedzi na ataki w toku i odstraszaniu napastników [5]. Skuteczność celowego ataku opiera się na niezdolności do rozpoznania zagrożenia. Nie jest możliwe zabezpieczenie się przed niebezpieczeństwem, którego nie jest się świadomym. Z faktu tego wynika konieczność monitorowania i klasyfikacji zagrożeń bezpieczeństwa. Zależnie od przyjętego modelu referencyjnego można klasyfikować zagrożenia dla każdej z warstw modelu. Nie można jednak przy tym zapominać, że najczęstszą przyczyną zagrożeń dla bezpieczeństwa IT jest czynnik ludzki [6].

Z punktu widzenia organizacji komercyjnej, podstawową miarą zagrożenia jest jego wpływ na zysk przedsiębiorstwa. Z ekonomicznego punktu widzenia, zarządzanie zagrożeniami jest więc tożsame z zarządzaniem ryzykiem. Dla organizacji komercyjnych przyjmuje się cztery metody zarządzania zagrożeniami [7]. Najbardziej oczywista wydaje się likwidacja przyczyn zagrożenia, można również ograniczyć wpływ na działanie przedsiębiorstwa, kolejną metodą jest przeniesienie skutków na inny podmiot (np. ubezpieczenie), a najmniej oczywiste, choć również często stosowane w biznesie, jest przyjęcie zagrożenia bez środków zaradczych i jedynie monitorowanie jego występowania oraz skutków. Jest to podejście stosowane w sytuacjach, gdy koszt neutralizacji zagrożenia jest większy niż poten-

cjalne szkody, jakie może ono spowodować. Należy tu podkreślić zwłaszcza aspekt statystyczny. Nawet zagrożenia mające bardzo poważny wpływ na zysk, w przypadku wystąpienia będą przyjmowane bez środków zaradczych, gdy prawdopodobieństwo ich wystąpienia jest niewielkie.

Dochodzimy tutaj do wymogu klasyfikacji zagrożeń pod względem ich potencjalnego wpływu na zysk przedsiębiorstwa oraz szacowania prawdopodobieństwa wystąpienia danego zagrożenia. Istnieje wiele definicji ryzyka. Na potrzeby tej pracy przyjmiemy prostą definicję [8], według której ekonomiczna wartość zagrożenia wyraża się wzorem:

$$EV = P * VaR$$

gdzie

EV – wartość ekonomiczna zagrożenia
P – prawdopodobieństwo wystąpienia danego zagrożenia
VaR – wartość zysku przedsiębiorstwa narażonego na powyższe zagrożenie.

Takie podejście pozwala podejmować decyzje ekonomiczne dotyczące klasyfikacji zagrożeń oraz możliwych do zastosowania środków zaradczych.

W szczególności standardy serii ISO 27000 definiują system zarządzania bezpieczeństwem informacji (ISMS). Ze względu na wielkość zagadnienia zarządzanie ryzykiem trudno poddaje się standaryzacji. I dlatego obok standardów ważną rolę odgrywają w tym wypadku dobre praktyki. W celu lepszego zrozumienia tematu w środowisku biznesowym i mając na względzie potrzeby wspólnej gospodarki, Unia Europejska przez swoją agencję ENISA prowadzi projekt mający na celu popularyzację zarządzania ryzykiem w przedsiębiorstwach [9]. Jednym z aspektów zarządzania ryzykiem jest właśnie zarządzanie bezpieczeństwem informacji. Obok potrzeby biznesowej, zarządzanie bezpieczeństwem w pewnych organizacjach komercyjnych wynika również z ustawodawstwa. Na przykład, według takich autorów, jak Yuvraj Gurung, Shyamala Sudhir, Roopa Thomas i Anuradha Krishnan, dla organizacji zarejestrowanych w USA lub notowanych na tamtejszych giełdach obowiązują [10]: *Computer Security Act* (1987), *Health Isurance Portability and Accounability Act* (HIPAA 1996), *Sabanes-Oxley Act* (2002). Na terenie Polski jest podobnie, obowiązuje np. ustawa o ochronie danych osobowych (1997).

METODY ZARZĄDZANIA ZAGROŻENIAMI

Obecnie przyjmuje się, że właściwym podejściem do zagadnienia zarządzania bezpieczeństwem systemów IT jest ochrona strefowa. Polega ona na podzieleniu całego systemu IT na strefy związane z przetwarzaniem informacji o różnych atrybutach (wartości ekonomicznej i czasie życia) i realizujące odmienne zadania. Znajduje to odzwierciedlenie w obowiązującej dla tej sieci polityce bezpieczeństwa. Należy tu zauważyć, że posiadanie polityki bezpieczeństwa jest wymogiem podstawowym, którego spełnienie umożliwia zarządzanie bezpieczeństwem w organizacji. Cztery główne składniki skutecznej strategii ochrony sieci to:

- polityki bezpieczeństwa,
- silne szyfrowanie,
- autentykacja,
- audytowanie.

Na przykładzie komercyjnego produktu HiPath Wireless [13] przedstawimy wymienione mechanizmy.

Polityki bezpieczeństwa same w sobie stanowią składnik organizacyjny. Niemniej jednak bezpieczeństwo systemu IT jest całkowicie zależne od możliwości implementacji polityk. Ze względu na czynnik ekonomiczny, poziom stosowanych zabezpieczeń sieci powinien być adekwatny do atrybutów (wartości i czasu życia) informacji. Na przykład, w sieci bezprzewodowej przyjmuje się szyfrowanie algorytmem CCMP (AES) i uwierzytelnienie zgodne ze standardem 802.1x, opisane wspólnie standardem WPA2 (802.11i), za adekwatne w sieciach bankowych. Natomiast szyfrowanie algorytmem TKIP (RC4) i uwierzytelnienie zgodne ze standardem 802.1x, opisane wspólnie standardem WPA, za adekwatne w sieci akademickiej i w zastosowaniach transmisji głosu w sieciach bezprzewodowych WiFi. Podobnie szyfrowanie algorytmem CRC-32 (RC4) i uwierzytelnienie hasłem, opisane wspólnie standardem WEP, uważa się za adekwatne dla dostępu gości do sieci bezprzewodowych WiFi w przedsiębiorstwie czy hotelu. Może również nie być szyfrowania i autentykacji w publicznych i bezpłatnych punktach dostępu. Wszystkie opisane sytuacje mogą występować też jednocześnie, np. w dużym budynku o przeznaczeniu biurowym. Możliwość implementacji kilku odpowiednich polityk z wykorzystaniem pojedynczej infrastruktury IT jest dużą korzyścią dla przedsiębiorstwa.

Szyfrowanie samo w sobie powoduje jednocześnie zwiększenie poziomu poufności informacji i zmniejszenie jej dostępności. Dobrze jest to widoczne na przykładzie modułów transmisji WiFi, w które są wyposażone komputery przedsiębiorstwa. Najbardziej obecnie zaawansowany standard 802.11i został wprowadzony w roku 2004, a więc wszystkie komputery wyprodukowane wcześniej go nie spełniają. Aby uniknąć konieczności natychmiastowej wymiany całego sprzętu przedsiębiorstwa, stosuje się najsilniejsze szyfrowanie odpowiednie do typu informacji i dzieli użytkowników zależnie od możliwości ich sprzętu.

Zagadnienie autentykacji może być przedstawione na przykładzie hotelu, gdzie urządzenia pracowników będą autentykowane zgodnie ze standardem 802.1x i przydzielane do odpowiednich zamkniętych grup, natomiast goście hotelowi będą autentykowani na podstawie hasła dostępnego poprzez recepcję hotelową lub odpowiednie strony WWW, zapewniające możliwość płatnego dostępu do sieci (bez innego mechanizmu).

Audytowanie wymaga zbierania danych o sieci. W tym wypadku jest to sieć bezprzewodowa. Punkty dostępu do sieci bezprzewodowej mogą działać jak czujniki IDS, aktywnie przeglądając wszystkie dostępne pasma i kanały radiowe. Informacja o włamaniach jest przesyłana do serwera zarządzającego, który zapewnia zaawansowane mechanizmy raportowania. Automatyczna klasyfikacja zagrożeń (własny, sąsiedzki, wrogi, itd) daje możliwość fizycznej lokalizacji lub uniemożliwienia dostępu dla obiektów wrogich. Istotna jest również możliwość zdefiniowania polityk bezpieczeństwa i automatycznego sprawdzania zgodności stanu sieci ze zdefiniowanymi politykami oraz raportowania lub podejmowania akcji zaradczych w razie niezgodności.

Różne technologie znajdują zastosowanie w różnych strefach. Według Warrena Petersona [11]:

- polityki bezpieczeństwa powinny być implementowane w każdej z warstw sieci osobno;
- bezpieczeństwo urządzeń powinno obejmować np. urządzenia trasujące (rutery), zapory ogniowe (*firewall*), konwertery adresów (NAT) i są potrzebni pośrednicy dla usług sieciowych (*proxy server*);

- niezbędne są systemy wykrywania włamań (IDS) stosowane do monitorowania ruchu w sieci i urządzeń aktywnych;
- autentykacja powinna się odbywać metodami jedno-, dwu- i trzyskładnikowymi w zależności od potrzeb;
- zabezpieczenie systemu plików powinno być stosowane od momentu autentykacji użytkownika, aby dopuścić lub uniemożliwić dostęp do informacji i zasobów;
- dostęp fizyczny do sieci oraz do poszczególnych urządzeń powinien być przemyślany (zaadresowany).

Istnieje bardzo wiele technologii używanych do zapewnienia bezpieczeństwa systemów IT. Opierając się na wynikach pracy Warrena Petersona, Shrinatha Tandura [12] oraz doświadczeniach autora, wymienimy tu najczęściej stosowane.

- Autentykacja – potwierdzenie tożsamości użytkownika, urządzenia przez system IT. Autentykacja metodami jednoskładnikowymi to np. wykorzystanie wiedzy typowe dla komercyjnych systemów IT, paranazwa użytkownika i hasło, metodami dwuskładnikowymi to paranazwa wsparta dodatkowo elementem posiadania, np. generatorem haseł jednorazowych (token), zaś autentykacja metodami trzyskładnikowymi to paranazwa użytkownika i hasło, uzupełnione jeszcze o to, kim jestem, np. element biometryczny, jak odcisk palca czy skan tęczówki oka.
- Niezaprzeczalność – metoda, dzięki której nadawca informacji potwierdza swoją tożsamość odbiorcy i potwierdza sam fakt dostarczenia informacji.
- Podpis cyfrowy – informacja jest szyfrowana za pomocą prywatnego klucza nadawcy.
- System detekcji włamań (*Inrusion Detection System* – IDS) – system wykorzystujący różne techniki w celu zdiagnozowania faktu włamania do sieci komputerowej przez obserwację działań, logi bezpieczeństwa i audyty danych.
- Zapora ogniowa (*Firewall*) – system zapewniający ochronę przejścia pomiędzy sieciami. W szczególności brama ograniczająca ruch zgodnie ze zdefiniowaną polityką bezpieczeństwa.
- DMZ – strefa zdemilitaryzowana – obszar sieci dołączony zarówno do wewnętrznej sieci firmowej, jak i do niezabezpieczonej sieci zewnętrznej.

- Kryptografia – dziedzina wiedzy zajmująca się technikami kodowania informacji, tak by były niedostępne dla osób nieupoważnionych, i rozkodowywania ich przez osoby upoważnione.
- PKI (*Public Key Infrastructure*) – infrastruktura klucza publicznego, zasoby zapewniające użytkownikom bezpieczeństwo przesyłania informacji, potwierdzenie tożsamości uczestników dzięki parom kluczy szyfrujących.
- Karta procesorowa (*Chip card*) – urządzenie w formie karty kredytowej, zawierające układ mikroprocesorowy. Zależnie od typu, pozwala na zapamiętanie hasła, klucza prywatnego PKI lub wręcz zawiera procesor kryptograficzny.
- Usługa katalogowa – repozytorium informacji o wszystkich obiektach w sieci. Poza nazwami użytkowników i urządzeń może zawierać prawa dostępu, klucze publiczne. Umożliwia scentrentralizowaną kontrolę dostępu do sieci.
- VPN (*Virtual Private Network*) – wirtualna sieć prywatna, tunel służący do przesyłu informacji, zabezpieczonej metodami kryptograficznymi, za pośrednictwem sieci publicznej.
- Biometryka – nauka badająca unikatowe cechy fizyczne ciała ludzi w celu użycia ich do potwierdzenia tożsamości.
- Audytowanie – niezależne badanie zapisów działania sieci w celu potwierdzenia zgodności z zaleceniami, politykami i procedurami operacyjnymi oraz ewentualne zalecenie ich zmiany; systematyczne przeglądanie zapisów urządzeń sieciowych w celu ustalenia utylizacji zasobów.
- Zabezpieczanie dowodów (*network forensics*) – proces określania przebiegu i skutków włamania w celu pozyskania dowodów możliwych do wykorzystania w postępowaniu sądowym.
- Polityka bezpieczeństwa – zestaw reguł, praw i praktyk określających jak organizacja zarządza, chroni i rozpowszechnia informacje poufne.
- Ochrona strefowa – proces jednoczesnego wykorzystania wielu technologii i systemów w celu ochrony systemu IT.

Zarządzanie zagrożeniami odbywa się w różnych obszarach i w różnych dziedzinach. Zgodnie z definicją Warrena Petersona [11] możemy przyjąć następującą podstawową klasyfikację:

- urządzenia końcowe: bezpieczeństwo fizyczne i bezpieczeństwo lokalnych danych (np. systemu plików);

- autentykacja urządzeń końcowych: autoryzacja użytkowników do korzystania z urządzenia, siła i komplikacja haseł, przechowywanie danych uwierzytelniających (login i hasło);
- urządzenia przesyłające: bezpieczeństwo fizyczne i kontrola ruchu;
- serwery usług: bezpieczeństwo fizyczne, bezpieczeństwo lokalnych danych (np. systemu plików), bezpieczeństwo systemu operacyjnego, autentykacja, poprawna konfiguracja i bezpieczeństwo samych usług;
- audytowanie: możliwość wprowadzenia polityk audytowania (zapisywania ważnych zdarzeń) i przeglądania zapisów co najmniej dla urządzeń transmisyjnych i serwerów usług;
- szyfrowanie: możliwość wdrożenia technik kryptograficznych w celu autentykacji, lokalnego przechowywania i przesyłania danych oraz zachowywania ustawień aplikacji.

Dodatkowo, zdaniem autora, należy tu uwzględnić medium fizyczne: bezpieczeństwo fizyczne.

PODSUMOWANIE

W niniejszym opracowaniu przedstawiono najczęściej używane architektury sieci IT, cechy bezpieczeństwa w systemach komercyjnych oraz metody zarządzania zagrożeniami. Z powyższego wynikają wymagania technologiczne stawiane systemom IT, które chcemy uznać za bezpieczne. Należy jednak zauważyć, iż nie każdy bezpieczny system zawiera wszystkie wymienione elementy. Stosowanie narzędzi bezpieczeństwa w komercyjnych systemach IT zawsze jest podporządkowane kryterium podstawowego celu przedsiębiorstwa. Jest nim przynoszenie zysku.

Literatura

[1] Drucker P. F., *The essential Drucker,* 2001, przekład polski: *Myśli przewodnie Druckera*, MT Bizness, Czarnów 2002, s. 31.

[2] *International Standard ISO/IEC 7498-1, Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model: ISO/IEC 7498-1:1994(E),* materiał dostępny na stronie http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip/.

[3] Socolofsky T., Kale C., *A TCP/IP Tutorial: IETF Request for Comments 1180*, materiał dostępny na stronie http://www.ietf.org/rfc/rfc1180.txt/.

[4] Pfitzmann B., Waidner M., *A General Framework for Formal Notions of "Secure" Systems: Hildesheimer Informatik-Berichte.*

[5] *CompTIA, Security+ Certification (Part 1): Identifying Security Threats*, materiały kursowe. Kurs dostępny na stronie http://www.comptia.org/.

[6] *Global Security Survey 2005, Raport na temat bezpieczeństwa w wiodących firmach sektora finansowego*, Deloitte Touche Tohmatsu 2005, materiał dostępny na stronie http://www.deloitte.com/dtt/cda/doc/content/pl_GlobalSecuritySurvey2005_EN.pdf/.

[7] *A Risk Management Standard: PD ISO/IEC Guide 73: AIRMIC, ALARM, IRM*, 2002, materiał dostępny na stronie http://www.the-irm.org/publications/PUstandard.html/.

[8] *Bezpieczeństwo teleinformatyczne,* Wikipedia, materiał dostępny na stronie http://pl.wikipedia.org/wiki/Bezpieczeństwo_teleinformatyczne/.

[9] *Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools ENISA*, 2006, s. 23, materiał dostępny na stronie http://www.enisa.europa.eu/rmra/downloads.html/.

[10] Gurung Y., Shyamala S., Roopa T. i Anuradha K., *Security Awareness (Second Edition)*: ISBN: 1-4246-0295-5 ELEMENT K PRESS, 2006.

[11] Peterson W., *Network Security Fundamentals:* ISBN: 0-7580-2570-X ELEMENT K PRESS, 2005.

[12] Peterson W., Tandur S., *Network Defense and Countermeasures (Second Edition)*: ISBN: 0-7580-6632-5 ELEMENT K PRESS, 2005.

[13] *Whitepaper Enterprise-grade Wireless LAN Security, Siemens AG 2005*, materiał dostępny na stronie http://www.siemens.com/index.jsp?sdc_p=dpHPo1077912fcls7mnt4u0&sdc_sid=26111901643/.