Teresa Mendyk-Krajewska, Zygmunt Mazur, Hanna Mazur

Ryzyko bezprzewodowej dostępności zasobów sieciowych w realizacji usług elektronicznych i e-biznesie

Ekonomiczne Problemy Usług nr 88, 625-633

2012

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 703 EKONOMICZNE PROBLEMY USŁUG NR 88 2012

TERESA MENDYK-KRAJEWSKA, ZYGMUNT MAZUR, HANNA MAZUR
Politechnika Wrocławska

RYZYKO BEZPRZEWODOWEJ DOSTĘPNOŚCI ZASOBÓW SIECIOWYCH W REALIZACJI USŁUG ELEKTRONICZNYCH I E-BIZNESIE

Wprowadzenie

Wygoda instalowania i użytkowania sieci bezprzewodowych spowodowała dynamiczny ich rozwój, obserwowany od ponad dziesięciu lat. Konsekwencją dużego zainteresowania realizacjami bezprzewodowymi było opracowanie i systematyczne rozwijanie różnego typu urządzeń mobilnych, umożliwiających zdalną pracę w systemie teleinformatycznym (także realizację usług) o każdej porze, z dowolnego miejsca, nawet podczas przemieszczania się.

Niestety, ogólnodostępne aplikacje wykorzystywane do realizacji e-usług i w e-biznesie często zawierają luki (wady programowe) umożliwiające przeprowadzenie ataku na system, czego skutkiem może być, na przykład, kradzież danych lub przejęcie kontroli nad urządzeniem. Bezprzewodowy dostęp do zasobów sieciowych niesie dodatkowe zagrożenia, głównie z powodu transmitowania danych w otwartej przestrzeni. Wśród szkodliwych działań dla sieci bezprzewodowych można wymienić zagłuszanie lub zakłócanie transmitowanego sygnału, instalację fałszywych punktów dostępowych umożliwiających przechwytywanie danych, przeciążanie systemu w celu blokowania dostępności usług, przełamywanie zabezpieczeń kryptograficznych czy infekowanie urządzeń mobilnych. Zagrożenie dla bezpiecznego użytkowania systemów komputerowych może być powodowane zarówno przez automatycznie propagowane szkodliwe oprogramowanie, jak i przez ludzi – nie tylko hakerów, ale też przez zatrudnionych lub byłych pracowników danej organizacji (instytucji, firmy), na której niekorzyść działają. Mimo powszechnej już świadomości realnych zagrożeń podstawowe zasady bezpieczeństwa są nierzadko nadal ignorowane, co w dużym stopniu wynika z ograniczonych moż-

liwości przeciwdziałania niekorzystnym zjawiskom (z powodu wysokich kosztów audytu bezpieczeństwa czy odpowiednio mocnego systemu zabezpieczeń) i dotyczy głównie zwykłych użytkowników oraz małych i średnich firm.

1. Rynek usług internetowych

Usługi elektroniczne i e-biznes to elementy e-gospodarki rozumianej jako realizacja procesów rynkowych z wykorzystaniem technologii informatycznych. Do tych procesów zalicza się produkcję, sprzedaż i dystrybucję produktów (z czym wiąże się przesyłanie danych pomiędzy producentami, dystrybutorami i odbiorcami produktów i usług), a także przekazywanie różnego rodzaju danych w ramach działalności administracyjnej, biznesowej itd. Dziś nie sposób wyobrazić sobie prowadzenie biznesu bez dostępu do sieci globalnej. Każda firma (instytucja, organizacja) stara się mieć własną witrynę internetową, by umieścić na niej informacje o prowadzonej działalności, udostępnić dane kontaktowe i stworzyć możliwości składania zamówień na produkty, usługi lub rezerwacje – w celu pozyskania klientów czy partnerów biznesowych, zawierania kontraktów, przesyłania dokumentów itd.

Według firmy Millward Brown SMG/KRC w połowie 2010 roku już 80% internautów korzystało z sieci w celu porównania ofert i cen towarów przed planowanym zakupem. Obserwowany dynamiczny rozwój usług elektronicznych wynika z powszechnej dostępności Internetu oraz szybkości i wygody ich realizacji.

Niestety, podczas realizacji usług elektronicznych może wystąpić wiele problemów dotyczących uczciwości i rzetelności kontrahenta, jakości i czasu świadczonych usług, płatności, bądź wykonywania dodatkowych czynności (np. związanych z serwisem). Można spotkać się z nieprawdziwymi informacjami w reklamach i fałszywymi sklepami wyłudzającymi pieniądze, kłopot może sprawiać dochodzenie roszczeń klienta na gruncie porządku prawnego innego kraju (uciążliwość, wysokie koszty). Ponadto nie zawsze można zwrócić zakup bez podania powodu.

Jednak znacznie poważniejsze problemy, zarówno przy realizacji e-usług, jak i w e-biznesie, dotyczą bezpieczeństwa, a wynika to między innymi z potrzeby zapewnienia ochrony przechowywanych i przesyłanych danych, zapewnienia dostępności danych i usług uprawnionym użytkownikom, konieczności aktualizacji regulacji prawnych oraz potrzeby zachowania anonimowości w sieci. Wyłudzanie i wyciek danych, szpiegostwo przemysłowe, zwalczanie konkurencji (np. przez tworzenie fałszywych stron internetowych) to tylko niektóre z zagrożeń, z którymi można się spotkać podczas działalności prowadzonej z wykorzystaniem Internetu.

2. Zagrożenia dla technologii bezprzewodowych

Wszelka działalność podejmowana w oparciu o sieci komputerowe (w tym realizacja e-usług i e-biznes) obarczona jest pewnym ryzykiem wynikającym z istnienia zagrożeń dla bezpiecznego użytkowania systemów i sieci komputerowych. Niestety, stopień zagrożenia rośnie wraz z rozwojem sieci i technologii informatycznych – obserwuje się coraz bardziej wyrafinowane metody ataków, a dostęp do gotowych, rozbudowanych funkcjonalnie narzędzi umożliwiających ich przeprowadzenie jest coraz łatwiejszy. Zjawisko przestępczości sieciowej obejmuje coraz większą liczbę użytkowników, a powodowane straty (wynikające z powstałych szkód, ich likwidacji, rozwiązywania problemów i straconego czasu) sięgają olbrzymich kwot. W Polsce, według raportu *Norton Cybercrime Report* firmy Symantec, szacowane straty sięgają 2,9 mld zł rocznie[1]. Zagrożenia są coraz poważniejsze. Przykładowo, w 2011 roku informowano o nowej odmianie konia trojańskiego SpyEye włamującego się na konta bankowe oraz o ataku hakerów na platformę informacyjną giełdy w Hongkongu (i nie był to pierwszy atak wymierzony w światowe giełdy). Tylko w grudniu 2011 roku Google usunął z Android Market 22 aplikacje (będące koniami trojańskimi), a w ciągu całego roku usunął ich łącznie 100[2].

Na ataki szczególnie narażone są realizacje bezprzewodowe, co wynika z dostępności sygnału propagowanego w otwartej przestrzeni i trudności związanych z jego ochroną (m.in. z powodu słabości stosowanych mechanizmów zabezpieczeń). Problem różnego rodzaju zagrożeń (wirusy, phishing, spam) dotyczy nie tylko technologii Wi-Fi sieci WLAN, ale też technologii sieci komórkowych oraz Bluetooth.

Sieci WLAN są łatwe do wykrycia i analizy. Dostępne narzędzia (jak na przykład NetStumbler, Kismet, WifiScanner, Gtkskan czy inSSIDer) umożliwiają określenie nazwy sieci SSID/ESSID (*Service Set Identifier/Extended* – SSID), zasięgu sygnału, adresów MAC (*Media Access Control*) i IP oraz stosowanych zabezpieczeń kryptograficznych (WEP[3], WPA[4], WPA2[5] lub braku ochrony), a także analizę nagłówków pakietów oraz pól wektora inicjalizującego (wykorzystywanego w procesie szyfrowania).

Celem podejmowanych ataków jest zakłócenie lub całkowita blokada pracy systemu (sieci), a także chęć uzyskania nieautoryzowanego dostępu do zasobów.

---

[1] www.norton.com/cybercrimereport, 2011.

[2] www.androidguys.com/2011/12/13/22-apps-kicked-from-android-market-over-premium-sms-toll-fraud, 13.12.2011.

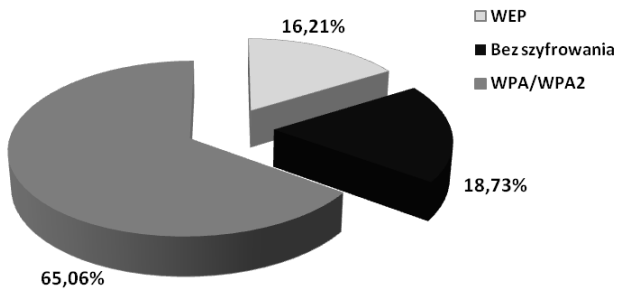
[3] *Wired Equivalent Privacy* – najsłabszy ze standardów bezpieczeństwa dla sieci WLAN; algorytm szyfrowania RC4; wykazuje szereg wad.

[4] *Wi-Fi Protected Access* – jeden ze standardów bezpieczeństwa dla sieci WLAN, wprowadza wiele zmian w stosunku do WEP (zmiany w stosowaniu RC4, stosowany protokół zarządzania kluczami TKIP, mechanizm MIC, protokół EAP).

[5] Standard mocniejszy od WPA – wykorzystuje m.in. algorytm szyfrowania AES i protokół CCMP; nie jest kompatybilny z wcześniejszymi rozwiązaniami.

Atak można przeprowadzić przy pomocy gotowych narzędzi (np. Aircrack-ng – do łamania haseł WPA), które mają służyć do audytu poziomu ochrony. Pozwalają one między innymi określić poprawność konfiguracji punktów dostępowych, występowanie nielegalnych punktów dostępu oraz istnienie innych sieci w pobliżu badanej, mogących stanowić dla niej źródło zakłóceń. Skanery bezpieczeństwa (np. Mognet, tcpdump, airfart, Wireshark) działają w oparciu o bazy zdefiniowanych zagrożeń oraz metody wykorzystujące algorytmy sztucznej inteligencji do analizy stanu systemu pod kątem nieznanych szkodliwych działań.

Z badań wynika, iż użytkownicy technologii bezprzewodowych mają świadomość istnienia zagrożeń i zabezpieczają swoje systemy coraz skuteczniej. Jesienią 2011 roku opublikowano wyniki badania poziomu ochrony 2900 sieci Wi-Fi wykrytych we Wrocławiu na trasie kilkunastu kilometrów[6]. Uzyskane rezultaty, przedstawione na rysunku 1, wskazują, że większość użytkowników (65%) stosuje stosunkowo mocne mechanizmy ochrony WPA i WPA2.



Rys. 1. Systemy zabezpieczeń stosowane w badanych sieciach Wi-Fi

Źródło: opracowanie własne na podstawie: M. Ziarek, *Bezpieczeństwo sieci WiFi w Polsce 2010/2011*, Wrocław, www.viruslist.pl/analysis.html?newsid=681.

System zabezpieczeń WEP cechuje szereg wad, takich jak: słaby kryptograficznie klucz szyfrujący i brak zdefiniowanego sposobu zarządzania kluczami (poziom zaufania do klucza spada wraz ze wzrostem liczby użytkowników i z czasem jego używania), stosowanie mechanizmu CRC-32[7] do zabezpieczenia przed modyfikacją, opcjonalna autoryzacja użytkowników oraz brak mechanizmu kontroli ramek transmisyjnych (możliwość wprowadzania strumienia danych dla przyspiesze-

[6] Tzw. *wardriving* polegający na wykrywaniu sieci i zbieraniu o nich informacji podczas przemieszczania się samochodem.

[7] *Cyclic Redundancy Check* – cykliczna kontrola nadmiarowa – mechanizm wykorzystywany do wykrywania błędów i modyfikacji w przechowywanych i przesyłanych danych (tu 32--bitowa sekwencja nadmiarowa); słaby kryptograficznie z powodu zależności liniowych.

nia procesu łamania klucza). System WEP nie zapewnia więc dostatecznej ochrony, mechanizmy WPA też nie są pozbawione wad (m.in. możliwy jest atak na protokół TKIP[8] i ominięcie procesu uwierzytelniania), jednak najbardziej niepokojący jest fakt, że prawie 19% sieci nadal pozostaje otwarte. Niestety, w uznawanym dotąd za najsilniejszy systemie zabezpieczeń WPA2 w połowie 2010 roku wykryto lukę pozwalającą osobom mającym już dostęp do sieci na szereg niepożądanych działań, między innymi na przeprowadzenie ataku Man-in-the-Middle, przechwytywanie ruchu i na przejęcie uwierzytelnionego urządzenia. Słabością WPA2 jest brak odporności klucza grupowego GTK (*Group Temporal Key*) na fałszowanie danych i podszywanie się pod adresy sieciowe.

Jedną z przyczyn trudności w skutecznym zabezpieczaniu sieci bezprzewodowych jest brak ich kompatybilności z powodu różnorodności sprzętu i dostępnych standardów bezpieczeństwa. Wobec skali zjawiska zagrożeń wysoki poziom ochrony systemów teleinformatycznych staje się zadaniem priorytetowym.

3. Zagrożenia dla urządzeń mobilnych a usługi elektroniczne i e-biznes

Wraz z rozwojem technologii bezprzewodowych nastąpił szybki rozwój urządzeń mobilnych (smartfonów[9], smartbooków[10]), wobec czego także one stały się przedmiotem zainteresowania przestępców sieciowych i w ostatnim okresie coraz więcej zagrożeń kierowanych jest właśnie na nie.

Urządzenia mobilne z dostępem do Internetu są coraz bardziej rozbudowane funkcjonalnie, a przy tym ich ceny szybko spadają, zatem ich używanie staje się powszechne (w trzecim kwartale 2011 roku sprzedano 440,5 mln urządzeń mobilnych oraz 115 mln smartfonów)[11]. Są one wykorzystywane do realizacji usług elektronicznych (usług bankowych czy e-zakupów) oraz do prowadzenia zadań biznesowych. Umożliwiają menedżerom i pracownikom przedsiębiorstw stały kontakt oraz dostęp do firmowych zasobów, zatem są chętnie przez nich używane (np. podczas podróży służbowych). Ważne i poufne dane, które są przechowywane niemal na każdym takim urządzeniu, mogą być źródłem wysokich zysków, stąd coraz większe zainteresowanie przestępców możliwością ich uzyskania. Celem ataku może być chęć przejęcia poufnych danych, zapisanych numerów telefonów czy treści wiadomości lub prowadzonych rozmów.

---

[8] *Temporal Key Integrity Protocol* – protokół do zarządzania kluczami; zapewnia dynamiczną wymianę kluczy.

[9] Urządzenia stanowiące połączenie telefonu i komputera.

[10] Oparte na podobnej architekturze co telefony komórkowe; wyposażone w pełną klawiaturę, duży ekran i baterie o długiej żywotności; łączą zalety netbooków i smartfonów.

[11] K. Bąkowski, *Rośnie sprzedaż smartfonów, Android niezaprzeczalnym liderem*, 16.11.2011.

Eksperci przewidują, że za kilka lat połączenia z siecią globalną będą realizowane głównie przy pomocy smartfonów, z powodu szybkiego rozwoju technologii urządzeń mobilnych. Z najnowszych badań firmy Ericsson Consumer Lab wynika, że w Polsce użytkownicy mobilnego dostępu do Internetu stanowią aż 55% wszystkich internautów (dla porównania w Wielkiej Brytanii jest ich 43%, w USA – 31%)[12]. Jest to ponad dwukrotny wzrost użytkowników bezprzewodowego dostępu w ciągu ostatnich dwóch lat. Zdecydowana większość ankietowanych wykorzystuje w tym celu laptopy i netbooki, ale udział smartfonów systematycznie rośnie. W Stanach Zjednoczonych jedna czwarta użytkowników smartfonów wykorzystuje je jako główny sposób łączenia się z Internetem[13].

Wraz ze wzrostem funkcjonalności telefonów komórkowych obserwuje się dynamiczny wzrost kierowanych na nie zagrożeń. Urządzenia te coraz częściej posiadają możliwość korzystania z sieci Wi-Fi, co stwarza dodatkową okazję do ich infekowania. Ponieważ urządzenia mobilne cechuje duża różnorodność platform systemowych, twórcy wirusów tworzą dla nich kody „wieloplatformowe". Zidentyfikowano już tysiące sygnatur tych szkodliwych kodów, które wykonują wiele niepożądanych działań, takich jak: pobieranie plików z sieci Internet (np. innych szkodliwych kodów), blokowanie karty pamięci lub całego urządzenia, uszkadzanie, usuwanie lub nielegalne pozyskiwanie danych, zdalne udostępnianie urządzenia (a tym samym np. sieci lub poczty korporacyjnej), wysyłanie wiadomości SMS czy MMS[14], wyłączanie mechanizmów bezpieczeństwa systemu.

Przełomowym rokiem dla zagrożeń urządzeń mobilnych był rok 2010, kiedy to zaobserwowano gwałtowny ich wzrost. Szkodliwe programy potrafią rozprzestrzeniać się przy pomocy nośników przenośnych, MMS-ów i SMS-ów, z wykorzystaniem technologii Bluetooth czy portali, z których pobiera się pliki (dzwonki, grafikę, gry i aplikacje), też w przypadku użycia kodów QR (*Quick Response*)[15]. Nieautoryzowany dostęp do urządzeń mobilnych umożliwiają też luki wykrywane w oprogramowaniu systemowym (np. w niektórych wersjach systemu Symbian). Jako przykłady szkodliwego oprogramowania dla urządzeń mobilnych można wymienić konie trojańskie: Trojan-Spy.SymbOS.Pbstealer.a (umożliwia kradzież danych), Trojan-Spy.SymbOS.Zbot (kradzież danych istotnych do przeprowadzenia transakcji bankowych) oraz Trojan.SymbOS.Skuller (wykorzystuje lukę dla umożliwienia dostępu). W 2011 roku pojawiła się modyfikacja przeznaczonego dla komputerów stacjonarnych szkodliwego kodu ZeuS, tym razem skierowana na urządze-

[12] T. Kutera, *Jak Polacy łączą się z siecią?*, 24.11.2011.

[13] C. Kang, *Smartfonowa rewolucja w sieci*, 14.07.2011.

[14] SMS (*Short Message Service*) – usługa przesyłania krótkich wiadomości tekstowych, MMS (*Multimedia Message Service*) – usługa przesyłania wiadomości multimedialnych.

[15] Rodzaj matrycowego kodu kreskowego – stosowany z powodu niewygody wpisywania adresu URL pobieranej aplikacji do przeglądarki smartfona; po jego zeskanowaniu ze strony WWW można zostać przekierowanym na adres URL z zainfekowanym plikiem (APK lub JAR).

nia mobilne. Głównym działaniem konia trojańskiego ZitMo (*ZeuS in the Mobile*) jest przechwytywanie SMS-ów z wysyłanymi przez banki kodami mTAN (*Transaction Autentication Number*) do mobilnego uwierzytelniania transakcji. Inny rodzaj zagrożenia to automatyczne wymuszanie połączeń międzynarodowych z numerami o podwyższonej odpłatności (wykonywane np. przez wirus Not-a-virus:Porn-Dialer.SymbOS.Pornidal.a) oraz działanie niektórych darmowych aplikacji wymagających dokonywania płatności podczas ich używania. Jeden z najgłośniejszych ataków na telefony komórkowe miał miejsce w 2007 roku w Hiszpanii, kiedy to zostało zainfekowanych ponad 115 tys. użytkowników wariantem wirusa ComWar (który wyszukuje dostępne urządzenia pracujące w technologii Bluetooth i wysyła do nich zainfekowane archiwum SIS o losowej nazwie).

Jak wynika z danych firmy Kaspersky Lab, najpopularniejszym celem ataków jest obecnie system operacyjny Android, który działa na połowie wszystkich smartfonów. Cechuje go elastyczność i niedostateczna kontrola dystrybucji przeznaczonego dla niego oprogramowania. Udział szkodliwych kodów atakujących te urządzenia stanowi już ponad 46% wszystkich szkodliwych programów dla urządzeń mobilnych. Jako przykłady wśród szkodliwego oprogramowania dla systemu Android można wymienić konie trojańskie: Tap Snake (podszywa się pod popularną grę i wysyła dane o położeniu urządzenia, co umożliwia szczegółowe odtworzenie trasy obserwowanego użytkownika) oraz Trojan-SpyAndroidOs.Antammi.b, który pojawił się jako aplikacja do pobierania dzwonków, a w efekcie dokonuje kradzieży kontaktów, wiadomości, zdjęć i współrzędnych GPS. W 2011 roku laboratoria firmy AVG wykryły kolejnego konia trojańskiego, który zapisuje treści rozmów i wiadomości SMS, a przechwycone dane przesyłane są na wskazane serwery. Eksperci z Kaspersky Lab tylko w 2011 roku wykryli prawie trzykrotnie więcej zagrożeń dla smartfonów niż w ciągu ostatnich sześciu lat[16].

Wobec wzrostu tego typu problemów banki muszą zrewidować stosowane dotychczas formy przekazu poufnych danych. Dotąd bowiem często wysyłały na telefony komórkowe jednorazowe hasła dostępu i kody potwierdzające transakcje bankowe, co uchodziło za jeden z bezpieczniejszych sposobów ich przekazywania.

Ze wspomnianego wcześniej raportu *Norton Cybercrime Report* firmy Symantec wynika, iż 12% dorosłych osób padło już ofiarą ataku na telefony komórkowe, a liczba wykrywanych luk w mobilnych systemach operacyjnych wzrosła ze 115 (w 2009 r.) do 163 (w 2010 r.). Tymczasem tylko 15% osób korzystających z mobilnego dostępu do Internetu instaluje w telefonach komórkowych oprogramowanie ochronne (takie jak F-Secure Mobile Security czy Kaspersky Mobile Security przeznaczone m.in. dla systemów Symbian, Windows Mobile i Android), choć użytkowanie tych urządzeń wymaga stosowania analogicznych zabezpieczeń jak w przy-

[16] www.chip.pl/news/bezpieczenstwo/wirusy/2011/10/podsluchy-w-androidzie-angry-birds-unlocker-czyli-najwieksze-zagrozenia-internetu-2#ixzz1iZmwdWBN, 12.10.2011.

padku komputerów, gdyż ich posiadacze zaczynają doświadczać takich samych problemów co użytkownicy komputerów. Przewiduje się, że zainfekowane urządzenia można będzie wykorzystywać do tworzenia botnetów[17], podsłuchiwania rozmów telefonicznych czy masowego rozsyłania spamu.

Podsumowanie

Część społeczeństwa wykazuje brak ufności względem nowych technologii i sięga po nie niechętnie, lub w ogóle nie korzysta z proponowanych rozwiązań. Z jednej strony spowodowane jest to przyzwyczajeniem do tradycyjnych form zakupów i płatności, a z drugiej – świadomością zagrożeń dla bezpiecznej realizacji e-usług i prywatności oraz utrudnieniami (uciążliwość systemów zabezpieczeń) wprowadzanymi dla przeciwdziałania niekorzystnym zjawiskom. Większego zainteresowania nowymi formami płatności należy oczekiwać wraz ze wzrostem zaufania do transakcji realizowanych z wykorzystaniem nowoczesnych technologii. Dlatego potrzebne są zabezpieczenia, które zminimalizują ryzyko. Aby zwiększyć bezpieczeństwo, stosuje się coraz mocniejsze systemy kryptograficzne – silniejsze algorytmy (do szyfrowania danych, zapewnienia im integralności), dłuższe klucze (do szyfrowania danych i uwierzytelniania nadawcy) i coraz bardziej złożone protokoły realizujące te mechanizmy.

Niestety, przewiduje się, że w najbliższym czasie nastąpi zarówno wzrost liczby użytkowników mobilnego Internetu, jak i eskalacja zagrożeń dla urządzeń mobilnych. W odpowiedzi na takie prognozy firmy produkujące urządzenia koncentrują uwagę na odpowiednim ich zabezpieczaniu. Przykładowo, firma Google, której system Android cieszy się ogromną popularnością, ogłosiła z końcem 2011 roku opracowanie jego nowej wersji (4.0), w której wprowadzono szereg dodatkowych funkcji zwiększających ochronę systemu. Urządzenie zostało wyposażone w nową obsługę haseł (Keychain API), co pozwoli aplikacjom przechowywać klucze oraz uzyskiwać dostęp do nich i odpowiadających im certyfikatów, wprowadzono przydzielanie pamięci dla aplikacji (ASLR[18]) oraz pełne szyfrowanie urządzenia. Ponadto dodano zestaw narzędzi do obsługi sieci VPN i bezpiecznego przechowywania danych uwierzytelniających (ważne w przypadku potrzeby uzyskiwania dostępu ze smartfona do korporacyjnej poczty elektronicznej lub służbowych komputerów). Za najbardziej efektowną funkcję można uznać Face Unlock, pozwalającą odblokować urządzenie na podstawie twarzy właściciela. Niestety, wprowadzone zabezpieczenia mogą okazać się niewy-

[17] Sieci składające się z komputerów, nad którymi zdalnie przejęto sterowanie w celu ich wykorzystania do bezprawnych działań.

[18] *Address Space Layout Randomization* – metoda ochrony systemu poprzez losowe adresowanie pamięci dla poszczególnych procesów, stosowana w komputerach stacjonarnych (firma Apple wdrożyła ją w systemie iOS).

starczające w związku z obserwowanym wzrostem wykorzystywania prywatnych urządzeń mobilnych w celach służbowych.

Wszystkie problemy związane z zapewnieniem wysokiego poziomu ochrony systemów teleinformatycznych stanowią wyzwanie i są przedmiotem licznych prac badawczych, tak by nie stanowiły bariery dla dalszego rozwoju e-gospodarki.

Literatura

1. Bąkowski K., *Rośnie sprzedaż smartfonów, Android niezaprzeczalnym liderem*, www.komorkomania.pl/2011/11/16/rosnie-sprzedaz-smartfonow-android-niezaprzeczalnym-liderem, 16.11.2011.
2. Kang C., *Smartfonowa rewolucja w sieci*, www.technowinki.onet.pl/artykuly/smartfonowa-rewolucja-w-sieci,1,4792393,artykul.html, 14.07.2011.
3. Kutera T., *Jak Polacy łączą się z siecią?*, www.technologie.gazeta.pl/ internet/1,104530,10704353,Jak_Polacy_lacza_sie_z_siecia_.html, 24.11.2011.
4. Ziarek M., *Bezpieczeństwo sieci WiFi w Polsce 2010/2011: Wrocław*, www.viruslist.pl/analysis.html?newsid=681, 24.10.2011.
5. www.androidguys.com/2011/12/13/22-apps-kicked-from-android-market-over-premium-sms-toll-fraud, 13.12.2011.
6. www.chip.pl/news/bezpieczenstwo/wirusy/2011/10/podsluchy-w-androidzie-angry-birds-unlocker-czyli-najwieksze-zagrozenia-internetu-2#ixzz1iZmwdWBN.
7. www.norton.com/cybercrimereport, 2011.

RISK OF WIRELESS ACCESS TO NETWORK RESOURCES IN PROVISION OF E-BUSINESS AND E-SERVICES

Summary

We observe a dynamic development of wireless technology and mobile devices. Because of their many advantages they are now commonly used to access Internet, and in particular to use e-services in e-business. Unfortunately, this brings new risks for the security of using network resources. In this paper we discuss the problems of safe use of wireless networks and mobile devices, we present the extent of the problems, and provide numerous examples of malicious software.

Translated by Zygmunt Mazur