Teresa Mendyk-Krajewska, Zygmunt Mazur, Hanna Mazur

Rozwój usług internetowych w dobie gwałtownego wzrostu zagrożeń bezpieczeństwa sieciowego

Ekonomiczne Problemy Usług nr 57, 197-204

2010

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 597 EKONOMICZNE PROBLEMY USŁUG NR 57 2010

TERESA MENDYK-KRAJEWSKA, ZYGMUNT MAZUR, HANNA MAZUR
Politechnika Wrocławska, Wydział Informatyki i Zarządzania, Instytut Informatyki
{teresa.mendyk-krajewska, zygmunt.mazur, hanna.mazur}@pwr.wroc.pl

ROZWÓJ USŁUG INTERNETOWYCH W DOBIE GWAŁTOWNEGO WZROSTU ZAGROŻEŃ BEZPIECZEŃSTWA SIECIOWEGO

Wprowadzenie

Sieć Internet stała się niezbędnym i wygodnym narzędziem do prowadzenia działalności gospodarczej i biznesowej, a dzięki technologii bezprzewodowej zwiększył się zasięg dostępności usług internetowych. Nieustannie poszerza się też ofertę usług, zwiększając tym samym zainteresowanie nimi potencjalnych klientów. Mimo zauważalnego wzrostu świadomości użytkowników z zakresu bezpieczeństwa sieciowego oraz udostępniania coraz bardziej efektywnych, kompleksowych narzędzi ochronnych, korzystanie z usług sieciowych nie jest całkowicie bezpieczne. Przyczyn problemów z bezpieczną realizacją usług w sieci globalnej jest wiele. Znaczący wpływ ma coraz bardziej złożone, zawierające wady (podatne na ataki) oprogramowanie systemów komputerowych (systemy operacyjne, ich komponenty, programy użytkowe, oprogramowanie sieciowe) oraz powszechna dostępność narzędzi umożliwiających podjęcie ataku nawet osobom niedoświadczonym. Wielu użytkowników, bagatelizując realne zagrożenia, nie poszerza wiedzy z zakresu zagadnień dotyczących ochrony systemu, niedostatecznie chroniąc swoje zasoby (stosowanie podstawowych zasad bezpieczeństwa dawno przestało wystarczać).

Przestępstwa popełniane w Internecie powodują ogromne straty finansowe. Najczęściej celem ataków jest przechwycenie chronionej informacji, np. danych osobowych, blokada usług lub przejęcie systemu dla prowadzenia bezprawnej działalności w sieci. Dostawcy dostępu do Internetu, oferując użytkownikom coraz więcej atrakcyjnych usług, są jednocześnie zobowiązani do zapewniania im wysokiego poziomu ochrony, jednak w praktyce jest to skomplikowane zadanie. Środo-

wisko zagrożeń jest bowiem zmienne i trudne do pełnej identyfikacji. Techniki hakerskie i technologie szkodliwego oprogramowania cechuje szybki rozwój i różnorodność, ponadto zadania związane z ochroną systemów komputerowych są złożone i czasochłonne, a wysoki poziom ochrony wymaga ponoszenia dodatkowych kosztów.

Zapewnienie bezpieczeństwa sieciowego stanowi poważne wyzwanie zarówno dla twórców oprogramowania i producentów sprzętu, jak i wszelkich instytucji zajmujących się zagadnieniem ochrony sieci.

1. Rozwój usług sieciowych

Oferta usług sieciowych stale się powiększa. Poprzez sieć można dokonywać zakupów, przeprowadzać transakcje finansowe, realizować płatności, odtwarzać pliki muzyczne i filmy, odtwarzać audycje radiowe i programy telewizyjne, śledzić obraz z kamer monitorujących, realizować mobilne usługi lokalizacyjne informujące o położeniu wybranych obiektów (hoteli, zabytków, ulic, budynków użyteczności publicznej itp.) czy natężeniu ruchu drogowego w czasie rzeczywistym. Szczególnie szybko rozwija się handel elektroniczny[1] i usługi bankowe. Użytkownicy Internetu coraz chętniej robią zakupy z wykorzystaniem sieci przede wszystkim ze względu na wygodę oraz zwykle niższą cenę niż w tradycyjnych sklepach. Na wzrost zainteresowania użytkowników usługami internetowymi duży wpływ ma rozwój technologii bezprzewodowych, które zwiększają komfort realizacji usług i umożliwiają ich wykonywanie z dowolnego miejsca w dowolnym czasie.

Z badań firmy D-Link Technology Trend wynika, że dostęp do Internetu w krajach Europy Środkowo-Wschodniej w 2008 r. nadal dość znacznie odbiegał od średniej europejskiej[2]. Przy unijnej średniej wynoszącej 54% gospodarstw domowych mających dostęp do sieci globalnej sytuacja w krajach naszego regionu wygląda znacznie gorzej. Najlepiej w tym rankingu wypadają Holandia oraz kraje skandynawskie, gdzie wskaźnik ten wynosi blisko 80%.

W Polsce zainteresowanie Internetem jest nie mniejsze niż w innych krajach, a użytkownicy sieci chętnie korzystają z dostępnych usług. W 2008 roku liczbę Polaków dokonujących zakupów w sieci szacowano na prawie 6 milionów. Z badań CBOS wynika, że odsetek kupujących stale rośnie: w 2008 r. zakupów przez sieć dokonywało 25% ankietowanych, a w 2009 r. – 32%[3]. Okazuje się, że rodacy chętnie kupują również poza granicami kraju. W serwisie aukcyjnym eBay w 2008 roku

[1] Wszelkie sposoby kontaktu z klientem i zawierania transakcji handlowych wykorzystujące elektroniczne środki przekazu.

[2] http://iik.onet.pl/1832590,1,2877,newsy.html

[3] http://interaktywnie.com/biznes/newsy/raporty-i-badania/cbos-ponad-polowa-polakow-ma-dostep-do-internetu-4127

zarejestrowanych było 900 tysięcy Polaków, którzy głównie korzystali, jak wynika z danych firmy, z aukcji w Niemczech, USA i Wielkiej Brytanii. Badania CBOS wskazują również na wzrost liczby osób korzystających z usług bankowych dostępnych przez Internet: z 17% w 2008 r. do 20% w 2009 r. Najpopularniejsze internetowe usługi bankowe to: uzyskiwanie informacji o rachunku (np. historia operacji), dokonywanie przelewów, otwieranie, modyfikowanie i likwidacja lokat, zlecenia stałe (m.in. ich definiowanie, modyfikacja, odwołanie), realizowanie płatności, obsługa kredytów (zlecenie wniosku, spłata itd.).

Przykładem usługi bankowości elektronicznej[4] jest PKO Inteligo oferowane przez PKO BP. Klient dysponuje unikatowym ośmiocyfrowym numerem (hasło pierwszego logowania do aktywacji wszystkich elektronicznych kanałów dostępu otrzymuje podczas podpisywania umowy) i kartą kodów jednorazowych przeznaczonych do autoryzacji dokonywanych operacji. Zmiany swojego hasła dostępowego (8-16 znaków alfanumerycznych) dokonuje po pierwszym zalogowaniu się. Uwierzytelnianie stron oraz poufność przesyłanych danych zapewnia protokół SSL[5] v.3 ze 128-bitowym kluczem.

2. Bezpieczeństwo usług w Internecie

Bezpieczeństwo usług internetowych zależy od wielu czynników, między innymi od aktualizacji użytkowanego oprogramowania, od stosowanych protokołów transmisyjnych (w tym sposobów weryfikacji użytkowników i mocy zaimplementowanych mechanizmów kryptograficznych) oraz od administrowania zgromadzonymi i przetwarzanymi danymi.

Dla bezpiecznego realizowania usług sieciowych stosuje się coraz bardziej zaawansowane mechanizmy ochronne. Przed atakami na konta bankowe chroni oprogramowanie antywirusowe zawierające moduł sprawdzający obecność odwiedzanej strony WWW w specjalnym rejestrze niebezpiecznych witryn. Ponadto przeglądarki internetowe mogą być wyposażone w mechanizmy filtrujące (antyphishingowe) rozpoznające, a niekiedy i blokujące sfałszowane strony. W tworzeniu takich list biorą udział także użytkownicy Internetu, zgłaszając zespołom zajmującym się problematyką bezpieczeństwa podejrzane strony, co wymaga weryfikacji i wydłuża czas reakcji na zagrożenie.

Niewątpliwie do usług wymagających najwyższego poziomu ochrony należą usługi bankowości elektronicznej. Internetowe konta bankowe zawsze stanowiły

---

[4] Bankowość elektroniczna – obsługa rachunku za pośrednictwem elektronicznych kanałów dostępu.

[5] *Secure Socket Layer* – protokół transmisyjny, w wersji 3 znany jako TLS (*Transport Layer Security*), zapewnia poufność i integralność danych, umożliwia uwierzytelnianie klienta i serwera.

obiekt zainteresowania włamywaczy sieciowych. Ich bezpieczeństwo zależy przede wszystkim od zasad i mechanizmów ochrony stosowanych przez banki: metod uwierzytelniania (m.in. liczby i długości stosowanych haseł), dozwolonej liczby prób logowania lub operacji, dopuszczalnego okresu bezczynności, rodzaju stosowanych technik kryptograficznych, a także odporności systemów na infekowanie szkodliwym kodem (jak konie trojańskie czy programy szpiegujące) i na inne rodzaje ataków.

Bezpieczne korzystanie z zasobów Internetu wymaga przestrzegania pewnych zasad. Na przykład podczas realizacji transakcji finansowych należy:

- sprawdzać poprawność adresu URL,
- sprawdzać, czy połączenie jest szyfrowane (użycie protokołu https),
- sprawdzać ważność i ścieżkę certyfikatu,
- kontrolować rejestr ostatniego logowania i ostatnich operacji,
- korzystać z limitów dla przelewów[6],
- po zakończeniu realizacji transakcji wylogować się z systemu,
- wszelkich podejrzanych sytuacjach informować zainteresowaną jednostkę (bank, sklep internetowy itd.),
- unikać zakupów on-line i korzystania z internetowej bankowości z komputerów publicznie dostępnych (np. kawiarenek internetowych) oraz słabo zabezpieczonych sieci bezprzewodowych.

Do ochrony przesyłu danych stosuje się protokoły (np. SSH[7], SSL czy IPSec[8]) wykorzystujące algorytmy kryptograficzne. Protokoły te umożliwiają między innymi dokonanie wyboru algorytmu szyfrowania, zaszyfrowanie danych, uwierzytelnianie serwera i sprawdzanie aktualności jego certyfikatów oraz weryfikację podpisów cyfrowych w komunikatach. Instytucje wykorzystujące Internet do przeprowadzania transakcji handlowych i finansowych mają obowiązek zabezpieczenia danych osobowych klientów. Obowiązek ten wynika z art. 36 ustawy o Ochronie danych osobowych z 29.08.1997 r.[9].

3. Zagrożenia bezpieczeństwa sieciowego

Realizowanie usług sieciowych, w szczególności usług bankowych czy dokonywanie transakcji handlowych, nie jest całkowicie bezpieczne. Zjawisko zagroże-

---

[6] Maksymalna kwota ustalona przez posiadacza rachunku, na jaką w danym okresie mogą zostać złożone dyspozycje przelewów.

[7] *Secure Shell* – protokół bezpiecznego logowania na zdalnych komputerach i korzystania z innych usług sieciowych; zapewnia szyfrowanie danych i uwierzytelnianie stron połączenia.

[8] Zbiór protokołów do implementacji bezpiecznych połączeń oraz wymiany kluczy szyfrujących pomiędzy stronami.

[9] Tekst jednolity z 17.06.2002 r. Dz.U. 2002 nr 101 poz. 926.

nia sieciowego wraz z rozwojem Internetu niezmiennie wykazuje tendencję rosnącą. Głównym celem ataków jest pozyskanie poufnych danych (informacji medycznych, biznesowych, danych osobowych), które – stanowiąc wartość – mogą być bezpośrednio wykorzystane lub sprzedane. Celem destrukcyjnych działań może być też blokada usług (ataki DoS[10], DDoS[11]). Bezprawna działalność w Internecie stanowi intratny proceder, a zajmują się nią wyspecjalizowane grupy przestępców, wykorzystując wady oprogramowania (np. błędy w przeglądarkach internetowych) lub naiwność użytkowników (ataki socjotechniczne). Atakowane są aplikacje i protokoły sieciowe, infekowane są strony internetowe popularnych, godnych zaufania serwisów, tworzone są fałszywe strony WWW (banków, instytucji finansowych) oraz fałszywe programy ochronne. Do przeprowadzenia ataku wykorzystywane są luki w systemie operacyjnym i aplikacjach, błędy konfiguracyjne oprogramowania, błędy użytkownika (np. niekończenie połączenia) oraz wady protokołów transmisyjnych.

Do najpopularniejszych w ostatnim czasie należą ataki na aplikacje sieciowe. Wykorzystuje się w tym celu różne metody, między innymi: manipulowanie parametrami transmisji (przy wykorzystaniu plików cookies, adresów URL, nagłówków http lub pól formularza udostępnianego przez aplikację), iniekcję kodu SQL (wykorzystując podatność aplikacji na obsługę spreparowanych zapytań SQL; wyróżnia się: ataki na składnię zapytania, składnię języka i logikę zapytania), atak XSS (*Cross Site Scripting* – infekowanie aplikacji sieciowej i przekazywanie szkodliwego kodu użytkownikowi w chwili korzystania przez niego z danej strony WWW), atak CSRF (*Cross Site Request Forgeries* – wymusza na użytkowniku wykonanie niepożądanej operacji względem wskazanej przez atakującego aplikacji), ataki na procesy uwierzytelniania, ataki na zasoby pasma sieci (np. DoS, DDoS, SYN Flooding, UDP Flooding), ataki na sesję użytkownika (np. przechwycenie lub odgadnięcie identyfikatora, na podstawie którego przydzielane są mu odpowiednie uprawnienia i zasoby).

Duże zagrożenie stanowią specjalne programy (*keyloggery*), które zainstalowane na komputerze użytkownika przechwytują wartości wciskanych na klawiaturze klawiszy, pozwalając nielegalnie przejąć jego prywatne dane. Jednym z najpoważniejszych zagrożeń są konie trojańskie[12], które mogą doprowadzić do zablokowania uprawnionemu użytkownikowi wykonania usługi (już po wpisaniu i akceptacji hasła), i symulując wystąpienie jakiegoś błędu, wykonać własną operację. Przykładem konia trojańskiego do przechwytywania danych wprowadzanych podczas korzystania z kont internetowych jest Backdoor.Nibu.H.

---

[10] *Denial of Services* – ma na celu zablokowanie korzystania z zasobów lub usług systemu komputerowego poprzez wyczerpanie potencjału danego zasobu lub systemu.

[11] *Distributed DoS* – atak DoS przeprowadzany jednocześnie z wielu komputerów.

[12] Szkodliwe oprogramowanie realizujące różne funkcje bez wiedzy użytkownika.

W silnikach JavaScript we wszystkich popularnych przeglądarkach odkryto błąd, który umożliwia sprawdzenie, czy dana osoba jest zalogowana na witrynie, którą odwiedza. Istnieje sposób, by włamać się na daną stronę WWW i umieścić na niej kod HTML, który będzie wyświetlał okienko pop-up (wyglądające na pochodzące z serwisu, z którego użytkownik korzysta) z prośbą o podanie loginu i hasła. Ważne, by okienko pokazywało się tylko użytkownikom, którzy już zalogowali się do danego serwisu (np. banku), gdyż kolejna prośba o podanie danych nie wzbudzi podejrzeń. Przykłady wad oprogramowania, które pozwalają przeprowadzić skuteczny atak, można by mnożyć. Wykrywane w oprogramowaniu luki są systematycznie przez producentów usuwane, jednak problem polega na tym, że wielu użytkowników rzadko aktualizuje oprogramowanie użytkowe.

W ostatnim czasie wiele niebezpiecznych infekcji pochodzi z legalnie działających, lecz słabo zabezpieczonych stron internetowych, na których przestępcy umieszczają szkodliwe kody (najczęściej poprzez popularny atak SQL Injection). Praktyka pokazuje, że właściciele stron WWW za mało dbają o bezpieczeństwo witryn, którymi zarządzają.

Wiele ataków ma charakter socjotechniczny, w których przestępcy starają się zdobyć zaufanie użytkowników, by skłonić ich do pożądanych dla siebie działań. Przed nimi jeszcze trudniej jest się użytkownikom obronić, bo wykorzystują ich naiwność, nieuwagę, niewiedzę. Phishing[13] od dawna jest jednym z najpowszechniej notowanych ataków. Dla zwiększenia skuteczności prowadzenia phishingu zostały opracowane specjalne narzędzia. Pozwalają one na szybkie wyszukiwanie i przetwarzanie danych z serwisów społecznościowych oraz innych źródeł internetowych (np. serwisów firmowych). Aplikacje tego typu umożliwiają śledzenie internetowych znajomości, relacji i podawanych różnego rodzaju informacji, dzięki czemu atak może być kierowany na ściśle określonych użytkowników. Stąd ostatnio coraz częściej obok działań polegających na podstępnym wyłudzaniu poufnych danych od przypadkowych adresatów (część z nich fałszywe wiadomości traktuje jak prawdziwe), stosowany jest *spear phishing*, polegający na przesyłaniu treści „spersonalizowanych". Przestępcy, posługując się posiadanymi danymi adresata (imię, nazwisko, nazwa firmy), czynią przekaz bardziej wiarygodnym. W spreparowanych listach nadawcy często podszywają się pod znane instytucje. Jeden z głośnych tego typu ataków polegał na wysłaniu do kierowników firm e-maili informujących o pozwaniu ich do sądu. Skuteczność jego działania tłumaczy się strachem przed wymiarem sprawiedliwości.

Z końcem 2008 roku pojawiła się informacja o odkryciu słabości w internetowym systemie certyfikatów protokołu SSL. Udowodniono, że można utworzyć sfałszowany certyfikat dla dowolnej strony WWW (wykorzystując słabość funkcji

[13] Wysyłanie olbrzymiej liczby wiadomości i oczekiwanie, że odbiorcy wykonają sugerowane połączenie z fałszywą stroną WWW i przekażą swoje dane (np. loginy i hasła).

MD5) – i jest on akceptowany przez większość popularnych przeglądarek internetowych. Zatem metodę tę można wykorzystać do tworzenia certyfikatów fałszywym stronom internetowym (np. stronom podszywającym się pod banki). Firmy posługujące się algorytmem MD5 przy tworzeniu certyfikatów powinny umożliwić użytkownikom bezpłatne zastąpienie go innymi mocniejszymi mechanizmami (SHA-1[14], SHA-2, SHA-3).

Utrata danych w sieciach komputerowych staje się coraz poważniejszym problemem. Organizacja Identity Theft Resource Center doniosła, że w 2008 r. liczba incydentów tego typu wzrosła o 47% w stosunku do roku 2007. Do największej liczby przypadków utraty danych doszło w przedsiębiorstwach prywatnych (37%), na kolejnych pozycjach uplasowały się: edukacja, agendy rządowe i wojskowe, służba zdrowia i sektor finansowy[15]. Za utratę danych odpowiadają jednak nie tylko przestępcy sieciowi, ale również pracownicy firm, którzy poufne informacje kradną świadomie. Najczęściej deklarowaną przyczyną takiego postępowania jest chęć niesienia pomocy w znalezieniu pracy osobie bliskiej, wykorzystanie danych do uzyskania nowej posady lub innego użycia w przyszłości. Oczywiście wiele informacji jest z firmy wynoszonych w nadziei osiągnięcia z tego korzyści materialnych.

Badania amerykańskiego centrum ds. przestępczości w sieci – National Internet Crime Center – wykazują, że w 2008 roku liczba oszustw internetowych związanych z realizacją usług wzrosła aż o 33% w stosunku do roku 2007[16].

Podsumowanie

Zagrożenia bezpieczeństwa sieciowego mogą stanowić istotną barierę rozwoju usług internetowych. Podstawą bezpieczeństwa systemów informatycznych jest prowadzenie odpowiedniej polityki (zgodnie z obowiązującymi standardami, normami i zaleceniami) w zakresie zabezpieczania zasobów systemu i monitorowania skuteczności stosowanej ochrony. Obowiązek właściwego zabezpieczenia gromadzonych i przetwarzanych danych (odpowiednio do ich wartości) oraz skuteczna ochrona systemu informatycznego przed nieupoważnionym dostępem spoczywa na administratorze. Od niego wymaga się zatem prawidłowego instalowania i funkcjonowania systemu informatycznego, minimalizowania ryzyka utraty danych, monitorowania pracy systemu, zapobiegania atakom, a także stałego doskonalenia się w zakresie zagadnień dotyczących bezpieczeństwa.

---

[14] *Secure Hash Algorithm* – SHA-1 tworzy skrót długości 160 bitów; nowe funkcje dają w wyniku odpowiednio 256 i 512 bitów.

[15] www.idtheftcenter.org/artman2/publish/lib_survey/Breaches_2008.shtml

[16] http://wiadomosci.onet.pl/1944002,441,item.html

Z powodu masowych zagrożeń pochodzących ze stron WWW wskazuje się, iż podstawą ochrony systemów komputerowych powinno być stosowanie technologii, które potrafią sprawdzać zawartość witryny w czasie rzeczywistym i wykrywać szkodliwy kod bez posiadania jego sygnatury.

Literatura

1. McClure S., Scambray J., Kurtz G., *Hacking zdemaskowany. Bezpieczeństwo sieci – sekrety i rozwiązania,* PWN, Warszawa 2006.
2. http://iik.onet.pl/1832590,1,2877,newsy.html
3. www.idtheftcenter.org/artman2/publish/lib_survey/Breaches_2008.shtml
4. http://wiadomosci.onet.pl/1944002,441,item.html
5. http://bezpieczenstwo.onet.pl/1488428,item,0,Phisherzy_atakuja_iTunes.html

THE DEVELOPMENT OF INTERNET SERVICES IN TIMES OF A RAPID GROWTH OF NETWORK SECURITY THREATS

Summary

As the Internet develops its resources become more and more attractive. Services available via the global network grow in number. Popularity of internet access increases mainly thanks to the development of wireless technologies which improve the comfort of network resources use. Unfortunately, due to the growth of network security threats, gaining and maintaining high level of security of gathered, processed and transferred data and realized services become the greatest problem.

Translated by Teresa Mendyk-Krajewska, Zygmunt Mazur, Hanna Mazur