dr inż. Teresa Mendyk-Krajewska
Instytut Informatyki, Wydział Informatyki i Zarządzania
Politechnika Wrocławska

Bezpieczeństwo internetowej komunikacji społecznej

WPROWADZENIE

Wykorzystywanie Internetu do komunikacji społecznej stało się powszechne. Dziś to portale społecznościowe stanowią platformę wzajemnego kontaktu użytkowników sieci globalnej z każdego miejsca na świecie.

Umożliwiają wymianę myśli, dzielenie się pasją i doświadczeniami, jednoczesne przekazywanie informacji na swój temat grupie osób (np. o miejscu pobytu, stanie emocjonalnym), pozwalają na prezentację zdjęć i pokazywanie znajomych. Tworzą płaszczyznę do kreowania własnego wizerunku, poszukiwania społecznego wsparcia, organizowania akcji społecznych i podejmowania działań politycznych.

To dzięki szybkiej komunikacji anonimowi użytkownicy z różnych krajów (Anonymous) mogą prowadzić akcje protestacyjne. Na znak protestu, łącząc się doraźnie w grupę, atakują[1] głównie strony rządowe, bankowe i korporacyjne[2].

W świat tych mediów wkroczyły też firmy (np. mBank czy Play), które wykorzystują je do przekazywania informacji i nawiązywania kontaktów z klientami. Profile firm i znanych marek (jak Coca Cola czy Starbucks) chętnie są dodawane przez użytkowników do grona znajomych[3] ze względu na zainteresowanie ich produktami, z powodu przeprowadzanych konkursów i promocji, bądź w odpowiedzi na bezpośrednie zaproszenie.

Dla wielu informacje otrzymane z mediów społecznościowych – portali, czy blogów, są ważniejsze od podawanych w tradycyjnych środkach przekazu.

Niestety, sieć globalna stanowi też przestrzeń dla eksponowania agresji i propagacji zagrożeń. Wraz z rozwojem Internetu i rozszerzaniem jego możliwości oraz przenoszeniem coraz większych obszarów życia do wirtualnej rzeczywistości – rośnie zagrożenie dla jego bezpiecznego użytkowania.

---

[1] Atak DDoS (*Distributed Denial of Service*) – rozproszony atak DoS; polega na blokadzie dostępności usługi z wielu komputerów jednocześnie.

[2] Jedną z akcji grupy był sprzeciw dla zapowiedzi podpisania przez Polskę porozumienia ACTA.

[3] Można też użyć opcji subscribe/like.

POPULARNOŚĆ SERWISÓW SPOŁECZNOŚCIOWYCH A ZAGROŻENIA

Wszelkie komunikatory internetowe umożliwiające w sieci globalnej bezpośredni kontakt większej liczbie osób zawsze cieszyły się dużym zainteresowaniem użytkowników dbających o kontakty towarzyskie. Popularne do niedawna narzędzia, takie jak sieci IRC (*Internet Relay Chat*)[4], Gadu-Gadu[5], a nawet Skype[6] wypierane są przez serwisy społecznościowe.

Najpopularniejszym z nich jest Facebook, którego projekt opracowany został na Uniwersytecie Harvarda w Stanach Zjednoczonych przez Marka Zuckerberga w 2004 roku (początkowo przeznaczony do wyszukiwania i kontynuowania szkolnych znajomości). Od maja 2008 roku działa polska wersja językowa serwisu. Użytkownicy Facebooka mogą tworzyć sieci i grupy, dzielić się wiadomościami i zdjęciami oraz korzystać z aplikacji, które są własnością serwisu.

Dzięki wewnętrznej platformie aplikacji internetowych można pisać własne programy i udostępniać je innym. Najwięcej użytkowników Facebooka[7] notuje się w Stanach Zjednoczonych (156 mln osób) drugie miejsce zajmuje Indonezja (ponad 40 mln), na kolejnych pozycjach znalazły się: Indie, Wielka Brytania, Turcja i Brazylia. Dziesiąte miejsce w tym rankingu zajęły Niemcy, zaś Polska z liczbą ponad 7 mln użytkowników znalazła się na dwudziestej czwartej pozycji[8].

Jednym z popularnych serwisów społecznościowych w Polsce jest nk.pl (do połowy 2010 roku Nasza-Klasa[9]) – portal utworzony w 2006 roku przez kilku studentów informatyki Uniwersytetu Wrocławskiego, stanowiący obecnie wielopoziomową platformę komunikacji. Serwis udostępnia listy szkół i klas oraz organizacji (jak np. harcerstwo), jednostek wojskowych itp. Stworzone są fora dyskusyjne podzielone na wątki (dla szkół, klas i niezależne), udostępnione są dwie metody komunikacji (poczta i komunikator internetowy), dołączono też gry komputerowe. W czerwcu 2010 roku liczbę aktywnych kont użytkowników tego portalu szacowano na 14 milionów.

[4] Kanały bezpośredniej komunikacji w sieci Internet.

[5] Komunikator internetowy opracowany przez firmę GG Network, uruchomiony w 2000 roku – przede wszystkim do prowadzenia rozmów tekstowych, ale też przesyłania plików, prowadzenia konferencji i rozmów głosowych.

[6] Komunikator internetowy oparty na technologii peer-to-peer; umożliwia prowadzenie darmowych rozmów głosowych oraz obserwację rozmówcy (dzięki zastosowaniu kamery internetowej), a także płatnych rozmów z użytkownikami telefonów stacjonarnych i komórkowych (w technologii VoIP (*Voice over IP*)); od 2005 roku na rynku polskim.

[7] Dane z listopada 2011 roku.

[8] http://wiadomosci.wp.pl/kat,1016019,title,Zniszcza-najpopularniejszy-serwis-spolecznosciowy,wid,13959144,wiadomosc.html?ticaid=1f415.

[9] Zmiana nazwy nastąpiła z powodu zmiany charakteru serwisu.

Innym popularnym serwisem jest You Tube – portal założony w 2005 roku umożliwiający bezpłatne umieszczanie i oglądanie filmów. Do dyspozycji użytkowników pozostają też MySpace[10] (oferuje m.in. prowadzenie blogów, możliwość tworzenia galerii zdjęć oraz profili muzycznych), Twitter[11], Google+[12] i wiele innych.

Niestety, Internet to także przestrzeń działalności bezprawnej i występowania różnego rodzaju zjawisk negatywnych, na przykład stosowania przemocy psychicznej (tzw. cybermobbing, e-mobbing) zatem pod groźbą kary zabrania się między innymi[13]:

- nawoływania do nienawiści (np. na tle różnic narodowościowych, rasowych, wyznaniowych itd.),
- zniesławiania, znieważania i nękania,
- stosowania gróźb,
- naruszania dóbr osobistych,
- rozpowszechniania wizerunku bez zgody zainteresowanego.

Z doniesień mediów wynika, że takie problemy na portalach społecznościowych dotyczą coraz większej liczby osób.

Jednym z istotnych zagrożeń jest bezprawne wykorzystywanie przejętych danych. Istnieje na przykład możliwość podszycia się pod inną osobę, co pozwala na wyrządzenie szkody majątkowej (np. poprzez wyłudzenie) lub osobistej (utrata reputacji).

Można wyróżnić kilka aspektów dotyczących bezpieczeństwa internetowej komunikacji społecznej. Popularność serwisów społecznościowych ułatwia przestępcom atakowanie systemów poprzez przenoszenie tą drogą szkodliwych kodów, a użytkownicy tych mediów narażeni są na wyciek poufnych danych oraz nieuprawniony wgląd do publikowanych przez siebie informacji, a nawet działania szpiegowskie.

Udostępniając informacje o sobie na forum publicznym stają się potencjalnymi ofiarami przestępczej działalności w cyberprzestrzeni.

Może właśnie występowanie różnego rodzaju negatywnych zjawisk oraz zaniepokojenie kwestią prywatności są przyczyną dość nagłego i znaczącego spadku popularności Facebooka obserwowanego od ponad roku w niektórych krajach, na przykład w Stanach Zjednoczonych Ameryki oraz Wielkiej Brytanii.

---

[10] Serwis założony w 2003 roku; w 2008 roku pojawiła się jego polska wersja; oferuje możliwości reklamowe wykorzystywane przez branże: muzyczną, filmową i telewizyjną.

[11] Serwis założony w 2006 roku udostępniający usługę mikroblogowania umożliwiającą wysyłanie i odczytywanie krótkich wiadomości tekstowych (tzw. tweetów).

[12] Łączy dostępne już usługi społecznościowe Google (Google Profile i Google Buzz) z wieloma nowymi funkcjami (np. wideospotkania), ma dedykowaną aplikację na mobilny system operacyjny Android i telefony iPhone.

[13] *Jak się bronić przed agresją w sieci*, „Świat wiedzy", październik 2011.

ZAGROŻENIA BEZPIECZEŃSTWA SIECIOWEGO W ASPEKCIE INTERNETOWEJ KOMUNIKACJI SPOŁECZNEJ

Systemy komputerowe wykazują podatność na zagrożenia między innymi z powodu wad oprogramowania wynikających z błędów programistycznych, niedostatecznego testowania finalnych produktów i nieprawidłowej konfiguracji użytkowanych systemów. Liczne zagrożenia, takie jak wirusy, robaki sieciowe, konie trojańskie czy exploity[14] umożliwiają pozyskanie poufnych danych lub przejęcie kontroli nad komputerem.

Przestępcy sieciowi zawsze pojawiają się tam, gdzie są duże skupiska potencjalnych ofiar, bo mogą ukrywając się wśród nich, działać na masową skalę. Chętnie zatem wykorzystują komunikatory internetowe i portale społecznościowe do rozprzestrzeniania szkodliwego oprogramowania, bowiem prawdopodobieństwo kliknięcia odsyłacza do strony lub pobranie z sieci treści (wiadomości, aplikacji) jest większe w przypadku nadawcy znajomego, budzącego zaufanie. Stąd częstym zagrożeniem w tym środowisku są fikcyjne profile, zainfekowane linki, fałszywe wiadomości, szkodliwe aplikacje, czy masowo rozsyłany spam.

Przykładowo, w III kwartale 2011 roku najczęściej przekierowania do niebezpiecznych stron znajdowały się na Facebooku, kolejne miejsca zajęły Google i Yandex (najbardziej popularna wyszukiwarka w rosyjskojęzycznym Internecie). Wyniki zebrane przez firmę Kaspersky Lab przedstawiono na rysunku 1.

Rys. 1. Zasoby internetowe najczęściej zawierające szkodliwe odsyłacze w III kw. 2011 roku

Źródło: opracowanie własne na podstawie: www.viruslist.pl/analysis.html?newsid=690.

Efektem tych szkodliwych działań może być kradzież danych osobowych[15] lub dostępowych (np. do kont bankowych), czy przekierowywanie na strony pornograficzne. Często drogą infekcji są odsyłacze do stron WWW umieszczane

[14] Programy umożliwiające wykorzystywanie znanych wad (luk) oprogramowania do zaatakowania systemu informatycznego.

[15] Dane osobowe, zgodnie z dyrektywą (art. 2) to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania (której tożsamość można ustalić) osoby fizycznej.

w przesyłanych wiadomościach spamowych generowanych przez boty[16] w języku zależnym od kraju odbiorcy. Przykładem robaka rozsyłającego spam ze szkodliwymi odsyłaczami jest Zeroll. Użytkowników zachęca się do kliknięcia w załączony link, kusząc na przykład ofertą obejrzenia zdjęć o intrygujących tytułach. W konsekwencji, na ich komputerach instalowane i uruchamiane jest oprogramowanie typu downloader (np. srce.exe), pobierające szkodliwe kody (np. robaka IM-Worm.Win32.XorBot.a[17]).

Innym przykładem zagrożenia jest rozpowszechnianie wśród użytkowników Facebooka maili z prośbą o autoryzację ich konta. Po uaktywnieniu dołączonego odsyłacza i podaniu hasła dla potwierdzenia tożsamości – konto zostaje przejęte przez przestępców. Z kont, nad którymi zdalnie przejęto kontrolę mogą być tworzone botnety[18]. Istnieje duże prawdopodobieństwo, że komputery użytkowników portali społecznościowych już są wykorzystywane w tym celu z powodu ich dużej podatności na infekcje[19].

Jedna z wersji robaka Koobface (rozpowszechnia on linki do stron ze szkodliwym kodem) potrafi zarejestrować się na Facebooku potwierdzając nowo powstały profil przy użyciu konta założonego na Gmailu. Wcześniejsze jego wersje rozprzestrzeniały się w innych serwisach (takich jak MySpace, Netlog czy Twitter).

Jednym z rodzajów zagrożenia jest ukrywanie odnośników do zainfekowanych stron WWW pod niebudzącymi podejrzeń skróconymi adresami URL w wiadomościach publikowanych w serwisach społecznościowych. Niektóre adresy (np. stron ze zdjęciami czy muzyką) są bardzo długie i nie mieszczą się w wiadomościach (np. na portalu Twitter), stąd potrzeba ograniczenia liczby znaków adresu do określonej długości.

Ponieważ skrócone adresy URL składają się z losowych liter, to użytkownicy nie mogą określić, do czego one przekierowują. Atakujący wykorzystują anonimowość tych adresów do podsyłania zainfekowanych stron internetowych (exploitami, botami, koniami trojańskimi itp.). Według danych firmy Kaspersky Lab, różne szkodliwe adresy URL (Malicious URL) w III kwartale 2011 roku znalazły się na pierwszym miejscu najczęściej wykrywanych zagrożeń online w Internecie (ponad 75%)[20]. W II kwartale 2012 roku zagrożenia tego typu stanowiły już 85,8%[21].

[16] Tu: programy w węzłach sieci botnet, do tworzenia sieci z zainfekowanych komputerów i ich zdalnego kontrolowania; m.in. mogą być pobierane z zainfekowanych treści (wiadomości na forach, spamu) lub rozprzestrzeniać się samodzielnie, jak wirusy i robaki.

[17] Wykorzystuje komunikator Yahoo Messenger, by wysyłać dalsze zainfekowane wiadomości.

[18] Sieci złożone z komputerów zainfekowanych szkodliwym oprogramowaniem, nad którymi przejęto kontrolę w celu ich wykorzystywania do bezprawnych działań.

[19] www.pcword.pl/news/368061/Facebook.botnetem.html.

[20] www.viruslist.pl/analysis.html?newsid=690.

[21] www.viruslist.pl/analysis.html?newsid=715.

Portale społecznościowe (np. Facebook czy Twitter) oraz strony serwisów informacyjnych są też wykorzystywane do rozpowszechniania zagrożenia w postaci fałszywego oprogramowania antywirusowego (scareware), co w ostatnich latach znacząco się nasila. Programy te mają nazwy i interfejsy podobne do zabezpieczeń oferowanych przez znane firmy specjalizujące się w tworzeniu oprogramowania ochronnego. Ich komunikaty mogą być wyświetlane także podczas przeglądania stron uznanych za wiarygodne. Fałszywe programy antywirusowe nie zapewniają żadnej ochrony – służą wyłudzaniu pieniędzy, a dodatkowo mogą rozprzestrzeniać takie zagrożenia jak wirusy, robaki czy konie trojańskie.

Wśród rozpowszechnianych fałszywych programów antywirusowych można wymienić:

- Internet Antivirus Pro (inne nazwy: General Antivirus lub Personal Antivirus) – udając skanowanie systemu poszukuje loginów i haseł,
- Privacy Center – instaluje szkodliwe kody; reklamowany jest w komentarzach do często odwiedzanych filmów (np. na You Tube),
- a także wiele innych, jak System Security, Win PC Defender, Alpha Antivirus, Windows Police Pro czy Malware Doctor.

Na fałszywą stronę firmy dystrybuującej oprogramowanie ochronne mogą przekierowywać ruch przeglądarki internetowej robaki sieciowe. Przykładem takiego działania było wyświetlanie swego czasu fałszywej strony AVG, zachęcającej do pobrania aplikacji Winspywareprotect, która starała się wyłudzić pieniądze za rzekome usunięcie zagrożeń z komputera użytkownika[22].

Dla użytkowników Facebooka istnieje jeszcze inne zagrożenie: nadrzędny administrator musi być ostrożny podczas przydzielania praw do zarządzania stronami (czasem mogą one wymagać kilku administratorów), istnieje bowiem możliwość usunięcia autora strony i całkowitego jej przejęcia przez nowo mianowanego administratora. Jest to możliwe z powodu luki w ustawieniach sieci społecznościowej – co w 2011 roku udowodniła firma Sophos specjalizująca się w technologiach ochrony informacji[23].

Szczególnie trudno jest się obronić przed atakiem o charakterze socjotechnicznym (tzw. phishing[24]), gdyż wykorzystuje się w nim naiwność, nieuwagę i niewiedzę użytkownika, by skłonić go do pożądanych dla przestępców działań. Dla zwiększenia skuteczności tego typu ataków zostały opracowane specjalne narzędzia do szybkiego wyszukiwania i przetwarzania danych, między innymi z serwisów społecznościowych. Aplikacje te umożliwiają mapowanie interneto-

[22] http://hacking.pl/wiadomosci/15155/falszywe-avg.

[23] http://technologie.gazeta.pl/internet/1,116487,10290604,_informacja_prasowa __luka_na_facebooku_umozliwia_przejmowanie.html.

[24] Atak polegający na wysyłaniu ogromnej liczby wiadomości w oczekiwaniu na wykonanie przez użytkownika określonej czynności, np. połączenia z fałszywą stroną WWW i przekazania poufnych danych (np. loginu i hasła).

wych znajomości i podawanych informacji, co pozwala ukierunkować atak na ściśle określonych użytkowników. Dzięki temu przestępcy coraz częściej posługują się danymi adresata, a przesyłając treści „spersonalizowane" czynią atak bardziej wiarygodnym zwiększając tym samym jego skuteczność (tzw. spear phishing).

ATAKOWANIE INTERNETOWYCH SYSTEMÓW BAZODANOWYCH

Internetowe systemy baz danych (przechowują, przetwarzają i udostępniają zgromadzone dane) zawsze były w wysokim stopniu narażone na zagrożenia.

Atakowanie systemów bazodanowych jest możliwe głównie z powodu wad oprogramowania – systemów zarządzania bazami danych (jak np. Oracle czy MySQL) i systemów operacyjnych, czyli środowiska ich eksploatacji. Przykładowo, tylko w lipcu 2012 roku firma Oracle w Critical Patch Update zamieściła aż 87 poprawek dla wielu swoich produktów (m. in. dla Oracle Database Server – 4, Oracle E-Business Suite – 4, Oracle PeopleSoft Products – 9, dla Oracle MySQL – 6)[25]. Liczba i częstość udostępnianych poprawek ukazują skalę problemu. W drugiej połowie 2011 roku aż cztery z pięciu najpopularniejszych exploitów nękających użytkowników Internetu z Ameryki Północnej i Europy Zachodniej dotyczyły aplikacji Oracle Java (JRE)[26]. Wyniki badań firmy Kaspersky Lab zawarto w tabeli 1.

Tabela 1. Najpopularniejsze exploity atakujące systemy użytkowników Ameryki Północnej i Europy Zachodniej w II połowie 2011 roku

Nazwa exploita	Odsetek zaatakowanych użytkowników	Podatna aplikacja
Exploit.Java.CVE-2010-4452.a	20,6%	Oracle Java (JRE)
Exploit.JS.CVE-2010-4452.l	3,4%	Oracle Java (JRE)
Exploit.JS.Pdfka.exr	3,0%	Adobe PDF Reader
Exploit. JS.CVE-2010-4452.t	2,9%	Oracle Java (JRE)
Exploit. Java.CVE-2010-0840.d	2,6%	Oracle Java (JRE)

Źródło: www.viruslist.pl/analysis.html?newsid=720.

Aplikacje bazodanowe wykazują podatność między innymi na atak z odpowiednio spreparowanymi zapytaniami SQL (atak SQL/XPath Injection). Atak ten pozwala odczytać dane z bazy, umożliwia ich modyfikację lub usunięcie. Według raportu firmy 7Safe w 2010 roku ten typ ataku odpowiadał za 60% przypadków wypływu danych z systemów bazodanowych[27].

[25] www.oracle.com/technetwork/topics/security/cpujul2012-392727.html.
[26] www.viruslist.pl/analysis.html?newsid=720.
[27] www.7Safe.com/breach_report/Breach_report_2010.pdf.

Jako częstą przyczynę możliwości atakowania systemów baz danych wskazuje się też niezabezpieczone odniesienia do obiektów, zbyt słabe mechanizmy uwierzytelniania i zarządzania sesją oraz błędy w konfiguracji serwerów (np. nieusunięte konta domyślne, otwarty dostęp do katalogów, przechowywanie haseł i poufnych informacji w postaci jawnej).

Systemy bazodanowe mogą być też atakowane przez robaki sieciowe. Przykładem jest popularny Slammer, który kilka lat temu infekował serwery SQL firmy Microsoft na całym świecie rozprzestrzeniając się z niespotykaną szybkością. Do wzrostu zagrożenia przyczyniają się też wszelkie zaniedbania zarówno ze strony obsługującego system personelu, jak i samych użytkowników.

Efektem skutecznego atakowania systemów może być wypływ danych z sieciowych serwerów bazodanowych, ich nieuprawnione użycie, blokada dostępności danych, ich modyfikacja lub zniszczenie.

Przypadki wypływu danych z internetowych systemów baz danych zdarzają się często i są nagłaśniane w trosce o bezpieczeństwo użytkowników usług sieciowych. Jesienią 2009 roku informowano o przechwyceniu i ujawnieniu w Internecie (przy pomocy koni trojańskich, jak np. Trojan-PSW.Win32.Dybalom.aoo) około 50 tysięcy nazw i haseł kont serwisów społecznościowych. W lipcu 2010 roku nastąpił wyciek danych z Facebooka, podobne problemy miała też Nasza-Klasa. Konsekwencją takich zdarzeń może być kradzież tożsamości.

Jednym z poważniejszych tego typu incydentów była kradzież w 2011 roku danych osobowych (imię, nazwisko, adres pocztowy, numer telefonu) 35 milionów użytkowników Internetu w Korei Południowej. Przejęcie danych było wynikiem włamania do serwerów firmy SK Telekom, właściciela wyszukiwarki Nibu i portalu społecznościowego CyWorld[28]. W czerwcu 2012 roku miał miejsce wyciek danych i haseł z międzynarodowego serwisu Linkedln[29], specjalizującego się w kontaktach zawodowo-biznesowych[30]. Okazało się, że użytkownicy posługiwali się prostymi hasłami, a ten popularny serwis społecznościowy nie stosował dostatecznie mocnego mechanizmu dla ich zabezpieczania.

PROBLEM PRYWATNOŚCI W SIECIACH SPOŁECZNOŚCIOWYCH NA PRZYKŁADZIE FACEBOOKA

Intensywna komunikacja społeczna za pośrednictwem Internetu stwarza zagrożenie bardziej lub mniej legalnego prowadzenia podsłuchu (szpiegowania) użytkowników i dowolnego wykorzystywania gromadzonych o nich informacji.

[28] www.viruslist.pl/analysis.html?newsid=690.

[29] Założony w listopadzie 2011 r. dostępny w kilka językach, od kwietnia 2012 r. także po polsku.

[30] www.viruslist.pl/analysis.html?newsid=715.

Wiele zarzutów kierowanych jest pod adresem samych administratorów portali społecznościowych. Niejednokrotnie informowano już o wycieku danych z Facebooka i podejmowano akcje, których celem było zwrócenie uwagi na stosowanie zbyt słabych zabezpieczeń. Na przykład, aby uruchomić aplikację użytkownik musi udostępnić swój identyfikator, który następnie umożliwia poznanie różnych upublicznionych przez niego informacji, zależnie od konfiguracji poziomu prywatności (nazwę użytkownika, wiek, zawód, zainteresowania, przyjaciół itd.). Jesienią 2010 roku doniesiono, że na skutek wad wykorzystywanej aplikacji autorstwa innej firmy na zewnątrz wydostały się dane użytkowników kilku popularnych gier komputerowych (w tym miłośników jednej z najpopularniejszych gier – Farmville)[31]. W tym przypadku bezprawnie przejęte identyfikatory przekazano do 25 firm reklamowych, przy czym jedna z nich (RapLeaf) utworzyła na tej podstawie kompletne profile użytkowników w celu ich sprzedaży. W reakcji na zdarzenie działalność aplikacji pobierających dane została przez Facebook zawieszona, jednak okazało się, że problem tkwił w działaniu mechanizmów przeglądarek internetowych.

Nie tylko gry, ale i popularne kilka lat temu quizy, będące dla wielu jedną z atrakcji serwisu, ujawniały zbyt dużo informacji o użytkownikach. Oczywiście można nie udostępnić aplikacji swoich danych (niekiedy żądane są też zdjęcia i informacje dotyczących znajomych), ale wówczas nie ma możliwości kontynuowania zabawy. Przedstawiciele amerykańskiej organizacji ACLU (*American Civil Liberties Union*) są zgodni, że takie praktyki nie są niczym uzasadnione[32].

Liczne kontrowersje budzi stosowana praktyka gromadzenia różnymi metodami poufnych informacji użytkowników z naruszeniem ich prywatności. Wobec Facebooka niejednokrotnie formułowano zarzuty, iż nie zapewnia podstawowej ochrony danych osobowych, a także udziela dostępu do kont między innymi agencjom rządowym, umożliwiając im śledzenie użytkowników. Okazało się, że portal przechowuje bez zgody użytkowników również dane już z profilu usunięte – i takie postępowanie wywołało falę protestów. Facebooka można użyć też do poznania imienia i nazwiska właściciela dowolnego adresu e-mailowego, a niekiedy uzyskać o nim więcej informacji. Ponadto mechanizmy tego serwisu umożliwiają rozpowszechnianie zdjęć bez zgody ich właściciela, na przykład przez znajomych mających do nich dostęp. W tym celu można posłużyć się odnośnikiem do strony ze zdjęciem lub skopiowanym adresem URL do samego zdjęcia. Pozwala to też poznać co najmniej imię i nazwisko danej osoby. Facebook zachowuje bowiem kopie zdjęć (nawet po dezaktywacji lub usunięciu konta) i udostępnia je osobom znającym adres[33]. Prowadzoną politykę w zakre-

[31] http://tech.wp.pl/kat,1009785,title,Facebook-traci-kontrole-nad-wlasnym-serwisem,wid,12775849,wiadomosc.html?ticaid=1f415.

[32] www.pcword.pl/artykuly/365314_2/Ochrona prywatnosci.na.Facebooku.i.Twitterze.html.

[33] www.pcword.pl/artykuly/368832_4/Facebook.najwiekszy.zdrajca.swiata.html.

sie przechowywania na serwerach dla dezaktywowanych kont danych profilowych tłumaczy się umożliwieniem powrotu użytkownikom do serwisu.

Z kolei na początku 2011 roku Facebook zezwolił aplikacjom sieciowym firm trzecich na dostęp do adresów i numerów telefonów komórkowych swoich użytkowników, o czym informowano na jednym z oficjalnych blogów portalu[34].

Innym zarzutem, jaki postawiono temu medium społecznościowemu, jest wykorzystywanie aplikacji do automatycznego rozpoznawania twarzy na zdjęciach, bez zgody danej osoby – co jest niezgodne z unijnym prawem[35].

Internauci są w sieci „obserwowani" między innymi z powodu cenności wiedzy na temat ich preferencji dla firm, które licząc na potencjalnych klientów, wysyłają im odpowiednio dopasowane reklamy i oferty handlowe. Internet to także źródło wiedzy o obywatelach dla państwa, dlatego też dostawcy usług sieciowych są zobowiązani do udostępniania gromadzonych danych odpowiednim służbom (policji, prokuraturze, urzędom skarbowym itp.). Gorzej, jeśli niedostatecznie chronione dane (nazwisko, adres zamieszkania, adres mailowy, numer telefonu, numer karty płatniczej) dostają się w niepowołane ręce i są bezprawnie wykorzystane na przykład dla uzyskania intratnych korzyści.

Sami użytkownicy Facebooka także mogą naruszać prawo, nawet o tym nie wiedząc, ponieważ przetwarzają dane osobowe (swoje, znajomych i obcych), podlegające szczególnej ochronie. Ich przetwarzanie w sposób niedozwolony jest karalne, zatem bez zgody zainteresowanego nie wolno[36]:

- oznaczać osób na zdjęciach zbiorowych,
- mylić imion i nazwisk (np. w podpisach zdjęć),
- umieszczać informacji wrażliwych (np. o orientacji seksualnej), ani poruszać takich kwestii,
- publikować zdjęć osób (z wyjątkiem tych publicznie znanych),
- przetwarzać takich danych jak: pochodzenie, poglądy polityczne, przekonania religijne, przynależność, danych o stanie zdrowia, nałogach itp. (chyba że osoba, której to dotyczy, wyraziła pisemną zgodę).

Nie wszystkie kraje, nawet w ramach Unii Europejskiej, mają takie same przepisy o ochronie danych osobowych. Na terenie państw członkowskich UE funkcjonują dwa podstawowe źródła: rozporządzenia (obowiązują bezpośrednio i nie podlegają przeniesieniu do prawa krajowego[37]) oraz dyrektywy (akty prawne wyznaczające państwom pewne cele, które powinny być osiągnięte w określonym czasie; pozostawia się im wybór form, metod i środków działania).

[34] http://technowinki.onet.pl/inne/wiadomosci/facebook-udostepnia-tworcom-aplikacji-nasze-adresy,1,4112305,artykul.html.

[35] http://technologie.gazeta.pl/internet,1,104530,10527462,Rozpoznawanie_twarzy_moze_byc_zakazane_w_Niemczech.html.

[36] http://wiadomosci.onet.pl/tylko-w-onecie/co-moze-wynikac-z-niewinnego-zdjecia-na-facebooku,1,5249846,wiadomosc.html.

[37] Ma to skutkować identycznym ich brzmieniem.

Zgodnie z art. 16 traktatu o funkcjonowaniu Unii Europejskiej każda osoba ma prawo do ochrony swoich danych osobowych. Wśród aktów dotyczących ochrony danych można wymienić:

- art. 8 Europejskiej Konwencji Praw Człowieka – gwarantuje prawo do poszanowania życia prywatnego i rodzinnego,
- konwencję nr 108 Rady Europy (organizacji niezależnej od UE) o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych,
- art. 8 Karty Praw Podstawowych,
- art. 81 Ustawy o prawie autorskim i prawach pokrewnych – gwarantuje prawo do ochrony przed nieupoważnionym rozpowszechnianiem wizerunku (tj. publikowaniem zdjęć, filmów) i naruszaniem dóbr osobistych.

PODSTAWOWE ZASADY BEZPIECZEŃSTWA

Mimo wzrastającej popularności internetowej komunikacji społecznej wielu użytkowników nie stosuje nawet podstawowych środków bezpieczeństwa. Dla osiągnięcia maksymalnego poziomu ochrony należy przede wszystkim na bieżąco aktualizować system operacyjny i użytkowane aplikacje, szczególnie te popularne, najbardziej narażone na zagrożenia (jak przeglądarki internetowe i pakiety biurowe) oraz systematycznie skanować komputer przy pomocy najnowszej wersji firmowego pakietu, chroniącego system na wielu płaszczyznach.

Wśród podstawowych zasad bezpieczeństwa dla internetowej komunikacji społecznej można wymienić:

- stosowanie odpowiednich ustawień prywatności,
- zastosowanie możliwie złożonego hasła dostępowego,
- częste, systematyczne zmienianie hasła (np. raz w miesiącu),
- niekorzystanie z opcji zapamiętywania hasła,
- używanie programu ochronnego weryfikującego bezpieczeństwo stron WWW zanim zostanie użyty odnośnik (przykładem AVG LinkScaner),
- blokowanie wyskakujących okienek,
- usuwanie historii przeglądanych stron WWW,
- nieakceptowanie zaproszenia do grona znajomych od osób nieznanych,
- uważne czytanie regulaminów serwisów, do których się zapisujemy,
- informowanie administratora serwisu o zidentyfikowanych zagrożeniach.

Serwisy udostępniają szereg opcji dotyczących prywatności. Między innymi istnieją możliwości ukrycia swojej obecności na portalu, wyłączenia informowania innych o odwiedzaniu ich profili, ukrycia wybranych elementów dla użytkowników spoza listy kontaktów.

Przy zastosowaniu wszystkich środków ostrożności nader ważna jest także wiedza użytkownika z zakresu bezpiecznego użytkowania systemu i jego właściwe postępowanie. Wiele ataków ma charakter socjotechniczny, zatem obo-

wiązuje zasada ograniczonego zaufania do innych użytkowników i wszelkich sieciowych ofert. Między innymi nie należy otwierać poczty elektronicznej i jej załączników pochodzących z niezaufanego źródła, trzeba systematycznie sprawdzać ustawienia prywatności w profilu, wykazywać ostrożność przy akceptacji nowych propozycji (kontaktów, odsyłaczy do stron WWW). Nie wolno udostępniać swoich danych poufnych (numeru dowodu osobistego, konta bankowego itp.). Należy pamiętać, że w przypadku przechwycenia danych niepowołany odbiorca otrzyma tyle informacji, ile użytkownik sam umieścił w swoim profilu.

O ochronę serwisu musi też troszczyć się jego właściciel. Wobec zarzutów pod adresem Facebooka, jego przedstawiciele twierdzą, że o bezpieczeństwo dbają specjalistyczne, systematycznie aktualizowane systemy, których celem jest wykrywanie fałszywych kont i zapobieganie bezprawnemu gromadzeniu danych.

PODSUMOWANIE

Wiele jest zagrożeń dla internetowej komunikacji społecznej, liczne problemy stwarzają sami członkowie sieciowej społeczności nie przestrzegając podstawowych zasad ochrony. Popularne serwisy coraz częściej stają się przedmiotem ataków, co prowadzi do masowego wypływu danych. Z badań wynika, że pomimo poświęcania bezpieczeństwu sieciowemu od wielu lat zwiększonej uwagi i mimo wysokiej świadomości zagrożeń wśród użytkowników – niewielu z nich podejmuje stosowne działania, by zapobiec potencjalnym problemom.

Wobec złożonych ataków hakerskich samo oprogramowanie antywirusowe już nie wystarcza. Potrzebne są kompleksowe rozwiązania zapewniające ochronę w czasie rzeczywistym, odpowiednio dopasowane do potrzeb użytkownika czy firmy oraz mocniejsze algorytmy uwierzytelniania i przechowywania haseł. Brak jest też nowoczesnych, skutecznych zabezpieczeń sieciowych w warstwie aplikacji. Zbyt mało o bezpieczeństwo serwisów dbają sami właściciele i administratorzy, którzy nimi zarządzają. Jednak najważniejszą kwestią jest opracowanie odpowiednich regulacji prawnych, jednolitych dla wszystkich krajów, bo tylko przy wzajemnej ich współpracy walka z negatywnymi zjawiskami i przestępczością w sieci może być skuteczna.

LITERATURA

Bailyn E., *Przechytrzyć social media*, Helion, Gliwice 2013.

Castells M., *Społeczeństwo sieci*, Wydawnictwo PWN, Warszawa 2010.

Evans L., *Social Media Marketing. Odkryj potencjał Facebooka, Twittera i innych portali społecznościowych*, Helion, Gliwice 2011.

http://hacking.pl/wiadomosci/15155/falszywe-avg (dostęp 29.08.2012).

http://tech.wp.pl/kat,1009785,title,Facebook-traci-kontrole-nad-wlasnym-serwisem,wid,12775849,wiadomosc.html?ticaid=1f415 (dostęp 28.08.2012).

http://technowinki.onet.pl/inne/wiadomosci/facebook-udostepnia-tworcom-aplikacji-nasze-adresy,1,4112305,artykul.html (dostęp 18.09.2012).

http://wiadomosci.wp.pl/kat,1016019,title,Zniszcza-najpopularniejszy-serwis-spolecznosciowy,wid,13959144,wiadomosc.html?ticaid=1f415 (dostęp 5.11.2011).

Jak się bronić przed agresją w sieci, „Świat wiedzy", październik 2011.

Kirpatrick D., *Efekt Facebooka*, Wolters Kluwer Polska, Warszawa 2011.

www.7Safe.com/breach_report/Breach_report_2010.pdf.

www.oracle.com/technetwork/topics/security/cpujul2012-392727.html (dostęp 17.07.2012).

www.pcword.pl/artykuly/365314_2/Ochrona prywatnosci.na.Facebooku.i.Twitterze.html (dostęp 20.09.2012).

www.pcword.pl/artykuly/368832_4/Facebook.najwiekszy.zdrajca.swiata.html (dostęp 20.04.2011).

www.pcword.pl/news/368061/Facebook.botnetem.html (dostęp 25.09.2012).

www.viruslist.pl/analysis.html?newsid=690 (dostęp 8.03.2012).

www.viruslist.pl/analysis.html?newsid=715 (dostęp 25.09.2012).

www.viruslist.pl/analysis.html?newsid=720 (dostęp 25.09.2012).

Streszczenie

Internetowe portale społecznościowe – popularna forma komunikacji społecznej (np. Facebook, Twitter, MySpace, nk.pl), to platformy kontaktu, tworzenia wizerunku, wymiany myśli i zdjęć. Powszechne ich używanie powoduje, że są wykorzystywane również do eksponowania agresji, stosowania przemocy psychicznej i propagacji zagrożeń. Użytkownicy serwisów społecznościowych, stanowiąc potencjalne ofiary przestępczej działalności, narażeni są na wyciek poufnych, czy wrażliwych danych, nieuprawniony wgląd do publikowanych przez siebie informacji, a nawet działania szpiegowskie. Mogą być nękani, zniesławieni i narażeni na rozpowszechnianie ich wizerunku bez ich zgody. Przestępcom sieciowym łatwo jest ukryć się i działać na masową skalę wśród dużego skupiska użytkowników. Efektem szkodliwej działalności może być kradzież danych osobowych lub dostępowych (np. do kont bankowych), czy tworzenie botnetów z kont, nad którymi przejęto kontrolę. W środowisku serwisów WWW łatwo prowadzić ataki o charakterze socjotechnicznym (phishing), wykorzystując ufność, naiwność, czy nieuwagę użytkowników. Dla zwiększenia ich skuteczności opracowane zostały specjalne narzędzia do szybkiego wyszukiwania i przetwarzania danych.

W wysokim stopniu na zagrożenia narażone są internetowe systemy baz danych, które można skutecznie atakować głównie z powodu wad oprogramowania. Aplikacje bazodanowe wykazują podatność między innymi na atak z odpowiednio spreparowanymi zapytaniami SQL. Jako częstą przyczynę możliwości atakowania systemów baz danych wskazuje się też niezabezpieczone odniesienia do obiektów, zbyt słabe mechanizmy uwierzytelniania i zarządzania sesją oraz błędy w konfiguracji serwerów.

Komunikacja społeczna za pośrednictwem Internetu stwarza też zagrożenie prowadzenia podsłuchu użytkowników i dowolnego wykorzystywania gromadzonych informacji. Wiele takich zarzutów kierowanych jest pod adresem samych administratorów portali społecznościowych.

Użytkownicy także mogą nieświadomie naruszać prawo, ponieważ przetwarzają dane osobowe podlegające szczególnej ochronie.

Safety of Internet Social Communication

Summary

Social networking portals – a popular form of social communication (e.g. Facebook, Twitter, MySpace, nk.pl) are platforms of contact, creating an image, exchanging thoughts and photos. Common application of them is the reason why they are also used to express aggression, use emotional abuse and propagate threats. The social service users, while being potential victims of criminal activity, are exposed to confidential or sensitive data leak or unauthorized access to the information published by them or even to spy activities. They can be harassed and exposed to their image being disseminated without their consent. It is easy for network criminals to hide and act on a mass scale among a large group of users. The result of harmful activity can be the theft of personal data or access data (e.g. to bank accounts) or the creation of botnets of accounts over which control has been taken. In the webpage environment it is easy to conduct attacks of socio-technical nature (phishing) using the users' confidence, gullibility or inattention. To increase their reliability special devices have been created to search for and process data quickly.

Database internet systems are exposed to threats to a large degree, since they can be effectively attacked mainly for the reason of software faults. Database applications show susceptibility to, among others, the attack with properly prepared SQL queries. Also, the non-protected references to objects, too poor confirmation mechanisms and session management mechanisms as well as server configuration errors are indicated as a frequent reason for the possibility of database system attacks.

Social communication through the Internet creates also a threat of users' tapping and free use of the information gathered. Numerous charges of this kind are addressed to the social portal administrators themselves. The users may also infringe the law being unaware of it, because they process personal data that are subject to special protection.