Hanna Mazur, Zygmunt Mazur

Ochrona prywatności i bezpieczeństwo danych w kontekście korzystania z serwisów społecznościowych

Ekonomiczne Problemy Usług nr 68, 726-734

2011

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 651 EKONOMICZNE PROBLEMY USŁUG NR 68 2011

HANNA MAZUR, ZYGMUNT MAZUR
Politechnika Wrocławska

OCHRONA PRYWATNOŚCI I BEZPIECZEŃSTWO DANYCH W KONTEKŚCIE KORZYSTANIA Z SERWISÓW SPOŁECZNOŚCIOWYCH

Wprowadzenie

Serwis (portal) społecznościowy (*social networking*) to zespół interaktywnych stron WWW z możliwością gromadzenia danych, tworzenia własnych profili przez użytkowników oraz komunikacji między nimi. Popularność serwisów społecznościowych nie maleje. Ich liczba stale rośnie, liczba ich użytkowników – również, a częstość odwiedzania serwisów świadczy o ich niesłabnącym powodzeniu. Ich funkcjonalności są stale rozbudowywane i dostosowywane do rosnących potrzeb i zmieniających się oczekiwań użytkowników. Internauci muszą mieć jednak świadomość, że każda ich działalność w sieci pozostawia ślad i pomimo że serwisy informują o zapewnieniu bezpieczeństwa zgromadzonych danych, to oni sami również muszą dbać o ochronę prywatności i bezpieczeństwo zamieszczanych danych.

Wiele osób potępia zakładanie kont w serwisach społecznościowych, a już podawanie prawdziwych danych o sobie i o swoich bliskich, ujawnianie stanu majątkowego czy zamieszczanie szczegółowych danych o stylu życia, znajomych i podróżach jest dla nich zupełnie niezrozumiałe. Tymczasem konta na serwisach społecznościowych mają politycy, artyści, firmy, organizacje, uczelnie wyższe. Niestety, internauci często nie dbają o ochronę swojej prywatności i zamieszczają zbyt szczegółowe informacje i dane personalne, filmy i fotografie, i to nie tylko swoje, ale również znajomych. Te dane, ujawniane i gromadzone w sposób dobrowolny, są dla innych niezwykle atrakcyjne. Dużym zagrożeniem dla bezpieczeństwa sieciowego są rozpowszechniane poprzez serwisy aplikacje o złośliwym działaniu umożliwiające wykradanie danych z kont użytkowników (i nie tylko).

Wśród studentów uczelni wyższej w 2009 roku autorzy artykułu przeprowadzili badania ankietowe na temat korzystania przez nich z serwisów społecznościowych. Celem badań była ocena popularności serwisów w ich środowisku, czynników decydujących o założeniu i likwidacji konta oraz świadomości zagrożeń bezpieczeństwa danych osobowych. Wyniki tych badań zostały przedstawione w dalszej części artykułu.

1. Rozwój serwisów społecznościowych

Pierwszy serwis został utworzony w sieci w 1995 roku przez R. Conradsa pod nazwą *Classmates.com* w celu umożliwienia komunikowania się ze sobą byłych członków danej grupy (klasa, wojsko itp.). Kolejnym serwisem umożliwiającym użytkownikom zakładanie własnych profili, komunikowanie się ze sobą oraz wyszukiwanie osób o podobnych zainteresowaniach był serwis *SixDegrees.com* (1997). Społeczność internetowa, zwana też wirtualną (*virtual community*, *e-community*, *on-line community*), to grupa ludzi komunikujących się za pośrednictwem Internetu. Duże zasługi w opisywaniu rozwoju społeczności wirtualnych przypisuje się H. Rheingoldowi[1], który był również założycielem serwisu społecznościowego o nazwie *Brainstorms* (1998 r.), mającego charakter konferencji internetowych.

Różnorodność portali społecznościowych jest ogromna. Powstają serwisy tematyczne, branżowe, lokalne i rozproszone geograficznie, masowe i o bardzo niewielkiej liczbie użytkowników, jak np. skupiające mieszkańców tylko jednego bloku mieszkalnego. W Polsce ogromną popularnością cieszą się serwisy *nk.pl* (14 mln użytkowników), *Facebook* (500 mln użytkowników, w tym ok. 4 mln użytkowników polskich), *MySpace*, *LinkedIn*, *grono.net*, *fotka.pl*, ale wielu użytkowników mają również na przykład serwisy społecznościowe dla klientów banków[2], nauczycieli (*naukowy.pl*), tenisistów (*Tenisklub.pl*) czy logistyków (*logistyka.net.pl*). Oferta usług i możliwości serwisów jest niezwykle różnorodna. Wiele z nich oferuje gromadzenie danych, opisów, katalogowanie zdjęć wraz z opisami, zamieszczanie filmów, korzystanie z komunikatorów internetowych i z poczty elektronicznej, wysyłanie wiadomości do innych użytkowników serwisu, listy i fora dyskusyjne, blogi, mikroblogi itd.

Ze względu na dostępność dla użytkowników wyróżnia się:

- wewnętrzne serwisy społecznościowe (*internal social networking*), dostępne tylko dla określonej grupy użytkowników (np. członków stowarzysze-

[1] H. Rheingold: *The virtual community*, 1998, www.rheingold.com/vc/book

[2] J. Dąbrowski: *Społeczności internetowe – wyzwanie czy szansa?*, Zeszyty Naukowe Uniwersytetu Szczecińskiego nr 597, Szczecin 2010.

nia, pracowników firmy czy uczniów danej szkoły) lub dla pewnej grupy początkowej i osób przez nią zapraszanych (znajomych),
- zewnętrzne serwisy społecznościowe (*external social networking*), które są publicznie dostępne dla wszystkich.

Obecnie serwisy społecznościowe coraz bardziej przejmują funkcję centrów komunikacyjnych.

W 2009 roku wiele emocji wzbudziła inicjatywa serwisu *Facebook*, aby wpisy jego użytkowników pojawiały się w wyszukiwarce *Bing*. W 2010 r. wyszukiwarka ta udostępniła spersonalizowane wyszukiwanie, uwzględniające wpisy na *Facebooku* (w przypadku osób mających tam konto). W ostatnim czasie promocja serwisu *Facebook* jest ogromna. Na wielu stronach internetowych znajdują się przyciski *Lubię to* umożliwiające bezpośrednie informowanie znajomych z *Facebooka* o stronie wartej zainteresowania. Ale też bardzo dużo wirusów kierowanych jest do użytkowników *Facebooka*, na przykład użytkownik jest zachęcany do zalogowania się na podanej stronie (zainfekowanej), na której rzekomo napisali o nim jego znajomi.

Z powodu szerokiej dostępności i popularności znacznie bardziej na wszelkiego rodzaju ataki, w celu pozyskania danych, narażone są serwisy zewnętrzne. Przestępcy umieszczają na stronach WWW złośliwy kod (niewidoczny dla odwiedzającego stronę) i nakłaniają użytkowników do wejścia na dany adres. Podczas przeglądania strony w tle, wykorzystując istniejące luki w oprogramowaniu (np. w systemie operacyjnym, przeglądarce, oprogramowaniu narzędziowym, kontrolkach ActiveX), na komputerze użytkownika instaluje się złośliwe oprogramowanie przechwytujące cenne dane (w tym loginy i hasła do kont internetowych).

2. Polityki bezpieczeństwa serwisów społecznościowych

Polityka prywatności określa sposób postępowania z danymi osobowymi podczas korzystania przez użytkownika z usług danego systemu. Bezpieczeństwo korzystania z serwisów społecznościowych zależy od wielu czynników, ale w dużej mierze od właścicieli kont. Portale w swoich politykach bezpieczeństwa (które zazwyczaj publikują na stronach WWW, chociaż zdarza się, że nie do końca robią to uczciwie) na ogół zapewniają o nieprzekazywaniu danych „podmiotom do tego nieuprawnionym".

Zazwyczaj serwisy umożliwiają użytkownikowi wgląd w zgromadzone swoje dane i ich edycję. Nieco gorzej jest z usuwaniem danych, gdyż usługa ta nie zawsze jest realizowana zgodnie z wyobrażeniem właściciela danych. Znane są przypadki dalszego przechowywania danych, pomimo żądania ich usunięcia. Nie wiadomo również co tak naprawdę dzieje się z wszelkiego rodzaju danymi usuwanymi przez właścicieli kont.

Wiele serwisów oferuje opcję dodawania znajomych do „ulubionych", ale nie wszystkie wymuszają uzyskanie zgody od dodawanej osoby.

Ze względu na częste korzystanie z serwisów społecznościowych za pomocą komputerów firmowych polityka bezpieczeństwa tych serwisów rzutuje na bezpieczeństwo sieci firmowych. Pracodawcy muszą być świadomi zagrożeń wynikających z korzystania przez pracowników z portali społecznościowych, i to nie tylko w godzinach pracy i z komputerów firmowych, ale również poza pracą. Z badań przeprowadzonych w USA w lipcu 2010 r. przez firmę Panda Security *Wskaźnik ryzyka mediów społecznościowych* wynika, że 33% małych i średnich firm w USA zostało zainfekowanych złośliwym kodem poprzez portale społecznościowe, a 23% doświadczyło kradzieży tożsamości. Ponadto 77% pracowników korzysta z portali społecznościowych w godzinach pracy[3].

3. Zagrożenia bezpieczeństwa serwisów społecznościowych

W Polsce zainteresowanie serwisami społecznościowymi jest nie mniejsze niż w innych krajach. Z raportu *Polski Internet 2008/2009*[4] przygotowanego przez firmę Gemius wynika, że aż 87% polskich internautów stanowią osoby w wieku 16–24 lat, a przeciętny polski internauta poświęca na przeglądanie Internetu 1,5 godziny dziennie. Częstymi użytkownikami serwisów społecznościowych są dzieci i młodzież. Ta grupa użytkowników cechuje się łatwowiernością i naiwnością, jest podatna na manipulację i bardzo łatwo ulega emocjom. Nie przywiązuje należytej wagi do zamieszczanych danych. Ale i dorośli często bagatelizują zagrożenia i również padają ofiarami oszustów wykorzystujących ich niewiedzę, pośpiech, lekkomyślność.

Bezpieczne korzystanie z portali społecznościowych wymaga przestrzegania pewnych zasad, na przykład nie powinno się podawać zbyt wielu danych osobowych swoich, a tym bardziej znajomych, należy z rozwagą wchodzić na podawane strony, zmieniać hasła itd. Zasady te bardzo często są jednak nieprzestrzegane. Po mechanicznym kliknięciu przycisku *Przypomnij później* może okazać się, że właśnie komputer został zainfekowany.

Wraz z rozwojem funkcjonalności serwisów społecznościowych i ze wzrostem ich popularności powiększa się też liczba zagrożeń projektowanych do rozprzestrzeniania ich za pomocą tych serwisów. Znane są liczne przypadki wycieku danych z serwisów społecznościowych. W marcu 2010 roku serwisy społecznościowe (*Facebook*, *Twitter*) były atakowane przez robaka Koobface. W lutym 2011 roku właściciele kont na *Facebooku* byli zachęcani do kliknięcia linku pobierające-

[3] www.wirtualnemedia.pl/artykul/serwisy-spolecznosciowe-niebezpieczne-dla-firm

[4] www.gemius.pl/pl/raporty/2009-02/01

go robaka Lolbot.Q (umożliwiającego dostęp do danych profili) oraz otrzymywali e-maile z załączonym plikiem o nazwie *Facebook_details.exe*, który był koniem trojańskim (Asprox.N)[5]. Analitycy z PandaLabs szacują, że w 2010 r. odkryto ponad 20 mln odmian złośliwego oprogramowania[6]. Z badań Eurostatu wynika, że w 2010 r. ok. 4% internautów europejskich stwierdziło wykorzystywanie (bez ich zgody) danych osobowych, kontaktowych, zdjęć i filmów. Najwięcej przypadków kradzieży danych osobowych było w Grecji i w Bułgarii – po 7%, w Polsce – 3%[7].

Aktualnym problemem jest wykorzystywanie portali społecznościowych do rozpowszechniania zaszyfrowanych i dynamicznych złośliwych kodów.

4. Wyniki autorskich badań ankietowych na temat portali społecznościowych

W celu oceny świadomości zagrożeń bezpieczeństwa danych osobowych na serwisach społecznościowych oraz oceny popularności tych serwisów autorzy przeprowadzili badania ankietowe na grupie 180 studentów:

- 35 studentów I roku Studium Kształcenia Podstawowego (SKP),
- 145 studentów III roku Wydziału Informatyka i Zarządzanie (IZ).

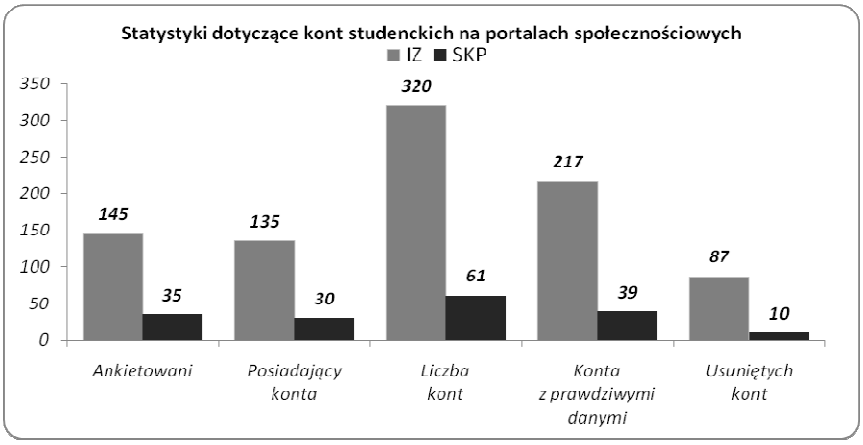
Udział w wypełnianiu ankiety był dobrowolny i anonimowy. Ankieta została przeprowadzona w miesiącach listopad–grudzień 2009 roku i zawierała 8 pytań. Ankietowani nie musieli odpowiadać na wszystkie pytania i część osób skorzystała z tej opcji. W trzech pytaniach można było zaznaczyć kilka odpowiedzi. Były również pytania otwarte.

Pierwszym zaskoczeniem przy analizie wyników ankiety była ogromna liczba kont na serwisach społecznościowych założonych przez studentów: 135 studentów IZ założyło 320 kont i aż na 217 kontach podało prawdziwe dane, 10 studentów IZ i 5 SKP nie założyło żadnego konta (rysunek 1). Spośród ankietowanych 35 studentów z SKP 30 założyło 61 kont i na 39 kontach podało prawdziwe dane (5 studentów SKP nie założyło konta). Należy jednak odnotować, że studenci rezygnują z kont (IZ – z 87, SKP – z 10).

[5] www.di.com.pl/news/35811,0,Facebook_ulubiona_przyneta_cyberoszustow.html

[6] www.di.com.pl/news/35098,0,Najciekawsze_zagrozenia_2010_roku.html

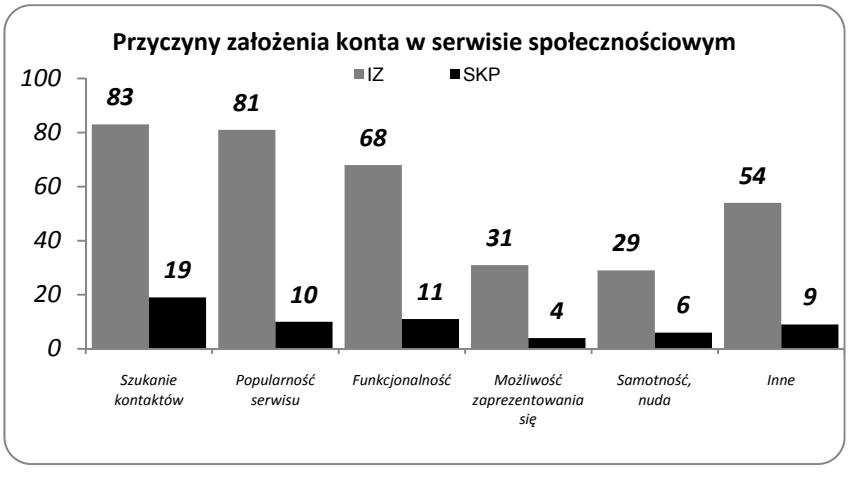
[7] www.epp.eurostat.ec.europa.eu



Rys. 1. Statystyki dotyczące kont ankietowanych na portalach społecznościowych

Źródło: opracowanie własne.

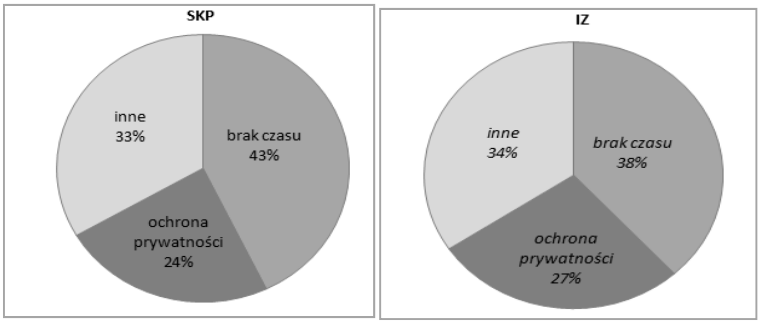
W obu grupach największą popularnością cieszył się serwis *nk.pl* (124 kont studentów IZ i 25 kont SKP), a następnie *Facebook* (46 – IZ i 7 kont SKP). Przyczyny założenia konta to najczęściej szukanie kontaktów ze znajomymi, popularność serwisu, odpowiednia do potrzeb funkcjonalność, możliwość zaprezentowania się oraz samotność i nuda (rysunek 2). W dalszej kolejności wymieniane było szukanie nowych znajomości (19 – IZ, 5 – SKP), możliwość zdobycia wiedzy, dokształcanie (7 – IZ, 1 – SKP) oraz presja otoczenia (6 – IZ).



Rys. 2. Przyczyny założenia konta w serwisie społecznościowym

Źródło: opracowanie własne.

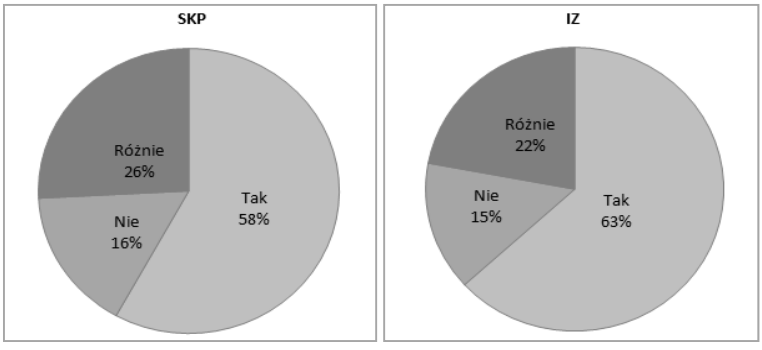
Wśród przyczyn wypisania się z serwisu najczęściej wymieniane były: brak czasu oraz ochrona swojej prywatności. Inne przyczyny to: znudzenie, nieodpowiednia funkcjonalność serwisu, obawa przed pracodawcą (rysunek 3).



Rys. 3. Przyczyny rezygnacji z konta w serwisie społecznościowym

Źródło: opracowanie własne.

Większość studentów przywiązuje wagę do ujawnianych danych i zdjęć (rysunek 4) oraz do danych zamieszczanych o nich przez inne osoby (IZ: 54% – Tak, 19% – Nie, 27% – Różnie; SKP: 71% – Tak, 10% – Nie, 19% – Różnie). 12% ankietowanych z IZ i 32% z SKP zażądało usunięcia danych ich dotyczących, a zamieszczonych przez inne osoby, z kolei 7% z IZ i 10% z SKP zostało poproszonych przez inne osoby o usunięcie zamieszczonych danych (zdjęć).



Rys. 4. Procentowe zestawienie odpowiedzi ankietowanych na pytanie o przywiązywanie wagi do informacji ujawnianych w Internecie

Źródło: opracowanie własne.

Przeprowadzona ankieta wykazała bardzo duże zainteresowanie studentów serwisami społecznościowymi. Świadomi zagrożeń nie zawsze podają prawdziwe dane podczas zakładania kont i wielu z nich, m.in. ze względu na ochronę swojej prywatności (27% wszystkich ankietowanych) zrezygnowało z posiadanego konta.

Podsumowanie

Internauci, z różnych powodów (np. samotność, moda, ciekawość, potrzeba), zakładają konta na wielu portalach społecznościowych i umieszczają tam wiele istotnych prawdziwych danych – i to nie tylko o sobie. Użytkownicy portali społecznościowych są narażeni na *phishing*, spam, nadużycia, kradzież danych, obraźliwe komentarze. Z dostępnych raportów i statystyk wynika, że właściciele kont albo nie zdają sobie sprawy z zagrożeń, albo je bagatelizują. Również przeprowadzone przez autorów badania ankietowe wykazały, że właściciele kont na portalach społecznościowych w wielu przypadkach żądali usunięcia danych zamieszczonych przez innych użytkowników kont lub sami musieli usunąć dane dotyczące innych osób (na ich prośbę).

Wielu internautów występowanie zagrożenia bezpieczeństwa dla danych ze strony portali społecznościowych nie zniechęca do korzystania z tej formy kontaktów, ale powinno być brane pod uwagę przez pracodawców. Powinna być opracowana i prowadzona odpowiednia polityka bezpieczeństwa uwzględniająca fakt korzystania przez pracowników z tych serwisów (i być może radykalnie to ograniczająca), powinny odbywać się szkolenia w kierunku podniesienia ich świadomości w tym zakresie oraz należałoby stosować odpowiednie zabezpieczenia, na przykład poprzez monitorowanie aktywności internetowej pracownika.

Literatura

1. Dąbrowski J.: *Społeczności internetowe – wyzwanie czy szansa?*, Zeszyty Naukowe Uniwersytetu Szczecińskiego nr 597, Szczecin 2010.
2. Rheingold H.: *The virtual community* 1998, www.rheingold.com/vc/book
3. *Polski Internet 2008/2009*, www.gemius.pl/pl/raporty/2009-02/01
4. www.di.com.pl/news/35098,0,Najciekawsze_zagrozenia_2010_roku.html
5. www.di.com.pl/news/35811,0,Facebook_ulubiona_przyneta_cyberoszustow.html
6. www.epp.eurostat.ec.europa.eu
7. www.wirtualnemedia.pl/artykul/serwisy-spolecznosciowe-niebezpieczne-dla-firm

PRIVACY PROTECTION AND DATA SECURITY IN SOCIAL NETWORKING

Summary

For a variety of reasons, internet users register at social networks and provide many important, real details about their and others' lives. The members of these online communities are exposed to phishing, spam, data theft, insulting comments and other abuses. Many users either do not realize or simply ignore the existing threats. In this paper we present the results of a survey which we carried out among university students.

Translated by Hanna Mazur, Zygmunt Mazur