ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 797 STUDIA INFORMATICA NR 33 2013

Grzegorz Szymański[*]
Arkadiusz Kowalczyk[**]
Politechnika Łódzka

FACEBOOK REALNYM ZAGROŻENIEM WSPÓŁCZESNEGO SPOŁECZEŃSTWA

Streszczenie

Facebook jest jednym z pierwszych serwisów społecznościowych. 26 stycznia 2010 roku w serwisie było zarejestrowanych ponad 350 milionów użytkowników. Jednak w lipcu 2010 roku liczba ta wzrosła do ponad 500 milionów, obecnie liczy ponad miliard fanów. Facebook.com to jedno z najczęściej odwiedzanych *on-line* miejsc na świecie. Od maja 2008 roku użytkownicy mogą pracować w polskiej wersji językowej portalu. W styczniu 2010 roku facebook.com w Polsce osiągnął liczbę 5–6 milionów zarejestrowanych użytkowników. Wraz z rosnącą popularnością zwiększa się również zagrożenie bezpieczeństwa. Użytkownicy Internetu, szczególnie w wieku poniżej 18 lat, coraz więcej czasu spędzają na portalach społecznościowych, a są to przeważnie osoby otwarte i chętnie korzystające ze wszystkich nowości i narzędzi internetowych.

Słowa kluczowe: Facebook, elektroniczne przestępstwa, oszuści w portalach społecznościowych

Wprowadzenie

Serwisy społecznościowe są współcześnie bardzo popularną odmianą serwisów internetowych oddziałujących na codzienność społeczeństwa. Portal w prosty sposób umożliwia użytkownikom interakcję z wybranymi osobami, nie tylko za pomocą wymiany opinii i komentarzy, ale głównie zdjęć, filmów, linków i informacji. Mechanizmy polecania, oceniania i komentowania powodują, że internau-

[*] grzegorz.szymanski@p.lodz.pl
[**] kowalczyk.arkadiusz@o2.pl

ta nie tylko ma możliwość korzystania z ogromnej bazy informacji, ale również wpływa na ich popularność i wartość (Mazurek 2008, s. 111). Do kluczowych funkcjonalności *social mediów* należy zaliczyć: tworzenie własnego profilu użytkownika, wyszukiwanie i segmentację znajomych, prywatną komunikację z innymi użytkownikami oraz budowanie grup tematycznych. (Frankowski, Juneja 2009, s. 16). Współczesne *social media* można posegregować według wybranych kryteriów. Ze względu na dostępność serwisy dzielimy na publiczne (umożliwiające swobodny i nieograniczony dostęp do zasobów) oraz prywatne (łączące zamknięte grupy użytkowników). Charakter portali dzieli je na zawodowe i towarzyskie, natomiast koszty użytkowania wprowadzają segregację na darmowe, płatne oraz sponsorowane.

Zdecydowanym liderem światowych *social mediów* jest Facebook, który 15 września 2012 roku liczył miliard użytkowników. Mark Zuckerberg założył serwis, którego grupą docelową mieli być tylko studenci Harvardu, obecnie jednak stanowi on idealny przykład rozwoju globalizacji. Atrakcyjność Facebooka polega przede wszystkim na wysokim stopniu interaktywności i zaangażowania jego użytkowników. W porównaniu do konkurencji oferuje wiele atrakcyjnych narzędzi, które dzięki polecaniu znajomym przyciągają nowych wielbicieli. Żaden ze współczesnych portali społecznościowych nie osiągnął tak dużej międzynarodowej popularności. Mimo że takie serwisy, jak Pinterest czy Instagram, będą przyciągać w najbliższej przyszłości coraz większą liczbę wyspecjalizowanych użytkowników, to Facebook nie przestanie dominować na rynku mediów społecznościowych. Dynamiczny i permanentny wzrost jego popularności implikuje z jednej strony wzrost zagrożeń, z drugiej natomiast wymusza na usługodawcy wdrażanie coraz skuteczniejszych metod i narzędzi zwiększających bezpieczeństwo użytkowników. Celem niniejszej publikacji jest weryfikacja hipotezy mówiącej, że wraz ze wzrostem popularności portalu społecznościowego Facebook zmniejsza się bezpieczeństwo jego użytkowników.

1. Rosnąca popularność Facebooka

Siłę marki Facebook potwierdzają statystyki – według analizy danych przedstawionych w BuzzFeed Social Intelligence Report (Smith, 2012,), Google w najbliższej przyszłości przestanie być głównym źródłem ruchu dla

serwisów internetowych. Jak wynika z danych zebranych z 200 serwisów internetowych, które były odwiedzane przez ponad 300 mln użytkowników miesięcznie, liczba wejść na portalu Facebook pod koniec 2012 roku przerosła liczbę odwiedzin w wyszukiwarce Google będącej do tej pory niekwestionowanym liderem ruchu. Facebook jest jednym z najmłodszych serwisów społecznościowych i jednocześnie największym portalem na świecie. 26 stycznia 2010 roku liczył on ponad 350 milionów zarejestrowanych użytkowników, zaś już w połowie lipca 2010 roku jej twórca Mark Zuckenberg ogłosił, że zarejestrowało się już ponad 500 milionów użytkowników, na początku 2014 roku zaś liczba ta przekroczyła już 1,3 miliarda, odnotowując średni roczny przyrost liczby fanów portalu na poziomie 20%. Wśród współczesnych statystyk Facebooka warto jeszcze podkreślić, że co drugi użytkownik loguje się do serwisu codziennie, średni czas jednej wizyty wynosi 18 minut, a przeciętny użytkownik posiada około 130 znajomych. Co każde 20 minut na platformie powstaje 3 miliony wiadomości, wysyłanych jest 2 miliony „zapytań o przyjaźń" oraz kreowanych jest milion udostępnień treści (Statisticbrain, 2014). Obecnie serwis dostępny jest w 70 różnych językach, a od 15 maja 2008 roku użytkownicy mogą korzystać z polskiej wersji językowej portalu. Na początku 2010 roku w Polsce odnotowano 6 milionów zarejestrowanych użytkowników, a pod koniec 2013 liczba ta wzrosła do 11,3 miliona (Social Times, 2013). 52% polskich użytkowników to kobiety, najpopularniejszą grupą wiekową stanowią osoby w wieku od 19 do 25 lat, nieco mniejszym gronem są użytkownicy w wieku 26–35 lat oraz 13–18 lat.

Istotną zaletą portalu oraz determinantą popularności jest efektywna adaptacja podstawowych funkcjonalności oczekiwanych przez internautów w postaci (Treadaway i Smith 2012, s. 64–65):

- utrzymywania biernego kontaktu z przyjaciółmi i znajomym,
- pozyskiwania nowych informacji o znajomych,
- komentowania zdjęć, linków i opinii,
- prowadzenia internetowego życia towarzyskiego poprzez transfer zdjęć, uczestnictwo w wydarzeniach, grach oraz pozostałych aplikacjach,
- zastępowania innych form komunikacji elektronicznej wewnętrznym komunikatorem,
- możliwość tworzenia i uczestnictwa w grupach zainteresowań,
- możliwość reklamowania własnej firmy,
- dostęp do statystyk profilu.

2. „Czarna strona" Facebooka

Gwałtowna i globalna popularność Facebooka musiała zostać zauważona przez internetowych oszustów, naciągaczy oraz pozostałe osoby wykorzystujące najprzeróżniejsze narzędzia i techniki w celu popełnienia internetowego przestępstwa. Współcześnie największą wadą portali społecznościowych jest brak anonimowości ich użytkowników. Zdecydowana większość odbiorców treści ma dostęp do wszelkich informacji o konkretnym profilu. Nawet jeżeli wszystkie informacje zostaną przekazywane tylko ścisłej grupie odbiorców, to cyberprzestępcy potrafią zostać przyjacielem potencjalnej ofiary, podszywając się pod znajomego. W Internecie można zaleźć wiele przykładów dostępu do kontentu osób trzecich. W Kanadzie pewien ubezpieczyciel odebrał klientce prawo do zasiłku chorobowego, ponieważ na podstawie zdjęć zamieszczonych na Facebooku uznał, że jest zdolna do pracy. Inny przypadkiem było zwolnienie z pracy w jednej ze znanych firm branży ubezpieczeniowej Nationale Suisse. Kobieta wzięła zwolnienie z pracy, tłumacząc, że migrena nie pozwala jej pracować, korzystając z komputera i musi leżeć w zacienionym pomieszczeniu. W tym czasie jednak logowała się na portalu społecznościowym, co zostało odnotowane przez władze firmy (Wysocka, 2013). Pracownicy Facebooka, broniąc się przed zarzutami bezpodstawnych udostępnień danych, opublikowali raport Global Government Requests Report (Facebook, 2013), w którym prezentują zestawienie próśb światowych władz o udostępnienie danych z konkretnych profili użytkowników, wykaz zawiera także procentowo ujęte pozytywnie rozpatrzone wnioski. Najczęściej dostępu do informacji (z ponad 20 tysięcy kont) domagał się rząd Stanów Zjednoczonych – dane uzyskał w 79% przypadków. Mniej zainteresowane prywatnymi danymi swoich obywateli były władze Indii (4144), Wielkiej Brytanii (2337), Włoch (2306), Niemiec (2068) oraz Francji (1598). Z Polski nadeszło 233 zapytania dotyczące 158 kont, jednak zdecydowana większość nie posiadała odpowiednich uzasadnień prawnych, gdyż jedynie 9% zostało rozpatrzonych pozytywnie. Zapytania dotyczyły wszelkich rodzajów informacji – od wezwań policyjnych dotyczących użytkowników wyłudzających dane, po zastrzeżone sądowe nakazy ujawnienia adresów IP opozycjonistów.

Brak konkretnych informacji dotyczących przekazanych przez Facebooka danych jest kolejną przyczyną zmniejszania się zaufania wobec serwisów społecznościowych. Zmieniając politykę na otwartą dla użytkowników, Facebook zapewnił, że w najbliższej przyszłości takie raporty będą publikowane regularnie,

analogicznie do stosowanej strategii w firmach Google i Microsoft. Otwartość koncepcji potwierdzają także zmiany w regulaminie polityki reklamowej, w którym od końca 2013 roku można znaleźć konkretny zapis informujący o udzielaniu serwisowi przez użytkowników zgody na wykorzystywanie ich danych do celów reklamowych. Do tej pory takie sformułowanie było ukryte pod wieloma paragrafami i zapisane w nieprzejrzystej formie. Obecnie sprecyzowano sposób wykorzystania imion i nazwisk użytkowników, ich zdjęć profilowych oraz wprowadzanych treści. Jasno określono, że decydując się na usługi Facebooka, użytkownik automatycznie zgadza się na komercyjne wykorzystywanie prywatnych danych. Kolejną barierą dalszej dynamicznej popularyzacji serwisu jest planowana zmiana polityki reklamowej. Już na początku 2014 roku wprowadzono w wybranych krajach reklamę wideo, która wyświetlana jest na profilach osób prywatnych. Inwazyjną techniką jest automatyczne uruchamianie spotu reklamowego wraz z włączonym dźwiękiem, co z pewnością zniechęci internautów.

Miliard użytkowników przyciąga setki oszustów, wśród których najpopularniejszymi są tzw. zbieracze „lajków" lub kreatorzy „farm fanów". Najczęściej wykorzystywanym mechanizmem jest metoda *publish_stream*, polegająca na zaprojektowaniu aplikacji, która po jej zaakceptowaniu przez użytkownika automatycznie publikuje informacje reklamowe w jego imieniu. Zaawansowane funkcje pozwalają kreować posty, nawet w przypadku, gdy główny użytkownik nie jest zalogowany do serwisu społecznościowego. Istotą jest zaprojektowanie zachęcającego do kliknięcia profilu, niestety (dla użytkowników) jego forma nie musi być wyjątkowo kreatywna i innowacyjna. Obecnie w Polsce większość internetowego ruchu w portalach społecznościowych to SPAM – użytkownicy bez namysłu klikają w większość napotkanych próśb, treści i zdjęć. Przykładowo *fanpage* o nazwie „Piątek, piąteczek, piątunio" gromadzący fanów piątku ma obecnie 247 tysięcy fanów, co jest wartością prawie dwukrotnie wyższą od liczby fanów o profilu mistrza olimpijskiego Kamila Stocha, pięciokrotnie wyższą od amatorów profilu Prezydenta RP Bronisława Komorowskiego oraz tylko o 100 tysięcy mniejszą od liczby wielbicieli Adama Małysza. Wykorzystując mechanizm marketingu wirusowego oraz polecanie przez znajomych, aplikacja bardzo szybko gromadzi rzesze fanów (Pankiewicz, 2008, s. 68).

Bardziej zaawansowani przestępcy wykorzystują technikę *clickjacking* (zwaną na Facebooku *likejacking*), w której użytkownik prowokowany jest do kliknięcia w atrakcyjne zdjęcia lub treść na profilu znajomego. Jednak po kliknięciu następuje przeniesienie do strony internetowej, która automatycznie i dyskretnie

aktywuje „polubienie" jej przez użytkownika. Tak zgromadzone grono nieświadomych wielbicieli zostaje „spieniężone". I w tym przypadku istnieje kilka możliwości, z których najprostszą jest wystawienie na aukcji internetowej oferty sprzedaży konkretnej liczby fanów. Po zakończeniu transakcji profil jest przejmowany przez zwycięzcę aukcji. Innymi metodami uzyskania zarobku jest sprzedaż powierzchni reklamowej, pojedynczych wpisów lub mailing do zgromadzonych fanów.

Inną formą przestępstw na Facebooku jest podszywanie się pod inną osobę, przeważnie celebrytę, znanego sportowca lub polityka. Założenie konta na dowolnie wprowadzone dane jest proste, weryfikacji podlega jedynie podany adres e-mail. Jeżeli konto dotyczy znanej osoby, to znalezienie w Internecie zdjęcia do profilu jest bezproblemowym zadaniem, podobnie w przypadku podszywania się pod konkretne przedsiębiorstwo czy markę. Kolejnym krokiem cyberoszusta jest zgromadzenie znajomych, które znacznie ułatwia wcześniej wprowadzone zdjęcie „ofiary". Po zebraniu zadowalającej liczby fanów i uzyskaniu ich zaufania, oszust tworzy treść, której celem może być zniesławienie lub kreowanie treści reklamowych, charakteryzujących się wysokim współczynnikiem konwersji ze względu na duże zaufanie do opinii i ofert prezentowanych przez znajomych.

Bardziej złożoną metodą oszustwa jest przejęcie istniejącego profilu. Zaletą tej techniki dla przestępcy jest dostęp do istniejącego, zaufanego konta, a co za tym idzie do zgromadzonych fanów, przekonanych, że autorem prezentowanych treści jest właściciel profilu. Główną jej wadą jest natomiast krótki czas dostępu do przejętego konta, gdyż najczęściej dość szybko właściciel zostaje poinformowany o zdarzeniu. Aby utrudnić funkcjonowanie techniki przejmowania kont użytkowników, Facebook wprowadził narzędzia ochronne, wśród których najskuteczniejsze jest informowanie wiadomością e-mail lub SMS-em właściciela, jeżeli nastąpiło zalogowania z innego niż zazwyczaj numeru IP, przeglądarki lub systemu operacyjnego. Oczywiście, jeżeli złodziej profilu zmieni hasło dostępu, to główny użytkownik nie będzie miał możliwości logowania, ale przynajmniej zostanie poinformowany, iż prawdopodobnie został ofiarą *phishingu* i będzie mógł podjąć kroki prawne oraz zablokować konto. Aby zwiększyć bezpieczeństwo, sami użytkownicy powinny stosować przynajmniej minimum podstawowych zasad, wśród których najważniejszą jest nieudostępnianie haseł oraz niestosowanie najprostszych i znanych fraz. Firma Splashdata opublikowała listę 25 najpopularniejszych haseł (tabela 1) wykorzystywanych w różnego rodzaju portalach na świecie, wśród których na pierwszych miejscach znajdują się łatwe do zgadnięcia kombinacje, jak: password, 123456, 12345678, abc123, qwerty.

Tabela 1

25 najpopularniejszych haseł stosowanych przez użytkowników w światowych serwisach internetowych

Popularność	Tekst hasła	Zmiana w stosunku do 2011 roku
1.	Password	brak zmiany
2.	123456	brak zmiany
3.	12345678	brak zmiany
4.	abc123	awans o 1
5.	Qwerty	spadek o 1
6.	Monkey	brak zmiany
7.	Letmein	awans o 1
8.	Dragon	awans o 2
9.	111111	awans o 3
10.	Baseball	awans o 1
11.	Iloveyou	awans o 2
12.	trustno1	spadek o 3
13.	1234567	spadek o 6
14.	Sunshine	awans o 1
15.	Master	spadek o 1
16.	123123	awans o 4
17.	Welcome	nowe
18.	Shadow	awans o 1
19.	Ashley	spadek o 3
20.	Football	awans o 5
21.	Jesus	nowe
22.	Michael	awans o 2
23.	Ninja	nowe
24.	Mustang	nowe
25.	password1	nowe

Źródło: Splashdata (2013).

Wśród metod hakowania kont na Facebooku należy wyróżnić także takie metody, jak: atak phishingowy, polegający na stworzeniu identycznie wyglądającej strony jak FB, której zadaniem jest uzyskanie loginu i hasła. Bardziej zaawansowaną techniką jest wykorzystanie programu typu *keylogger* lub *backdoor*, które pozwalają przejąć komputer ofiary. Cyberprzestępcy bardzo często hakują

konta e-mail, które są zintegrowane z profilem użytkownika w portalu społecznościowym, a dostęp do nich pozwala na zmianę hasła do Facebooka. Wśród mniej znanych metod znajdują się *session hijacking* oraz *sniffing*, czyli przejmowanie sesji na komputerze użytkownika oraz informatyczne podsłuchiwanie komunikacji komputera ofiary z serwerem FB.

Facebook jest także miejscem wielu przestępstw związanych z uwiedzeniem nieletnich oraz groźbami karalnymi. Groźby karalne, zgodnie z Ustawą z dnia 6 czerwca 1997 r. Kodeks karny (DzU nr 88, poz. 553, z późn. zm.) stanowią przestępstwa przeciwko wolności. W Polsce ten, kto grozi innej osobie popełnieniem przestępstwa na jej szkodę lub szkodę osoby najbliższej i jeżeli groźba wzbudza w zagrożonym uzasadnioną obawę, że będzie spełniona, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Groźba karalna obowiązuje również w komunikacji elektronicznej, konieczne jest jedynie, aby sposób jej wyrażenia wzbudził u pokrzywdzonego uzasadnioną obawę, że będzie spełniona. Natomiast uwodzenie osób małoletnich przez Internet, czyli *grooming* (Gruchoła 2011, s. 79–81), jest działaniem podejmowanym przez przestępcę w celu nawiązania więzi emocjonalnej z dzieckiem lub osobą nieletnią, aby zmniejszyć jego opory przed osobistym spotkaniem z zamiarem wykorzystania seksualnego. Mechanizm jest stosowany także do przekonania osoby małoletniej do prostytucji lub udziału w pornografii dziecięcej.

Podsumowanie

Podsumowując, należy stwierdzić, że portal społecznościowy Facebook, będący obecnie najpopularniejszym w świecie serwisem internetowym, przyciąga, prócz fanów, także cyberprzestępców. Jedną z determinantów zwiększających aktywność oszustów jest fakt, iż około 25% użytkowników to osoby małoletnie (13–18 lat), które są bardziej podatne na wszelkiego rodzaju manipulacje, a ich niewielkie doświadczenie życiowe kształtuje emocjonalne i bardzo często nieodpowiedzialne zachowania. Pozorna anonimowość internetowa zmniejsza czujność i bezpieczeństwo, co bezlitośnie wykorzystują cyberprzestępcy. Ponadto brak jest odpowiednio skutecznych aparatów i mechanizmów w sektorze *social mediów*, które pozwalałyby chociażby wiarygodniej weryfikować internetowego rozmówcę. Użytkownicy Facebooka nie mają możliwości efektywnej weryfikacji tożsamości innej osoby. Praktycznie jedynym gwarantem autentyczności danego profilu są zamieszczane na nim zdjęcia oraz identyfikacja wspólnych znajomych. Jednak oba warunki wykorzystywane są bardzo często na niekorzyść użytkowników, współcześnie przestępcy w łatwy sposób mogą uzyskać fotografię ofiary,

a powszechna chęć posiadania jak największej liczby fanów, występująca głównie wśród młodzieży, pozwala bezproblemowo dostać się przestępcy do grona znajomych. Analizując rozważania teoretyczne oraz przedstawione fakty i szeroki wachlarz możliwości popełnienia przestępstw na Facebooku, należy uznać przedstawioną we wstępie artykułu hipotezę za prawdziwą. Wraz ze wzrostem popularności portalu społecznościowego Facebook zmniejsza się bezpieczeństwo jego użytkowników. Mimo iż ostatnie zmiany w regulaminie i polityce prywatności portalu uświadomiły użytkownikom mechanizmy wykorzystywania i przechowywania wprowadzanych danych, to nie przyczyniły się do zapewniania odpowiedniego poziomu bezpieczeństwa.

Bibliografia

Frankowski P., Juneja A. (2009), *Serwisy społecznościowe, budowa, administracja i moderacja*, Helion, Gliwice.

Gruchoła M. (2011), *Ochrona małoletnich internautów w prawie i praktyce Unii Europejskiej,* Rozprawy Społeczne*,* t. V, nr 1.

Hartman A., Sifonis J., Kador J. (2001), *E-biznes – strategie sukcesu w gospodarce internetowej*, LIBER, Warszawa.

Facebook (2013), www.facebook.com/about/government _requests (dostęp 16.12.2013).

Social Times (2013), http://pl.socialtimes.me/stat/PL (dostęp 9.12.2013).

Splashdata (2013), http://splashdata.com/press/pr121023.htm (dostęp 9.12.2013).

Statisticbrain (2014), www.statisticbrain.com/facebook-statistics (dostęp 4.01.2014).

Mazurek G. (2008), *Blogi i wirtualne społeczności – wykorzystanie w marketingu*, Wolters Kluwet, Kraków.

Pankiewicz K. (2008), *E-marketing w akcji*, Helion, Gliwice.

Shih C. (2012), *Era Facebooka, Wykorzystaj sieci społecznościowe do promocji, sprzedaży i komunikacji z Twoimi klientami*, Helion, Gliwice.

Smith B. (2012), *One Chart That Explains The Transformation Of Media In 2012*, www.buzzfeed.com/bensmith/one-chart-that-explains-the-transformation-of-medi?mkt_tok=3RkMMJWWfF9wsRoksqvAde%2FhmjTEU5z16O0rUKSzgokz2EFye+LIHETpodcMTspgMbDYEhcSI4JkxgVAR+ece5lB (dostęp 16.12.2013).

Treadaway C., Smith M. (2012), *Godzina dziennie z Facebook marketingiem*, Helion, Gliwice.

Wysocka J., *5 najgorszych wad Facebooka*, www.papilot.pl/lifestyle-ciekawostki /11491/2/5-najgorszych-wad-Facebooka.html#galleryimage (dostęp 16.12.2013).

FACEBOOK AS A REAL THREAT OF CONTEMPORARY SOCIETY

Summary

Facebook is one of the earliest social networking sites and also the largest portal in the world. 26th January 2010 it had more than 350 million registered users. However in July 2010 has already registered over 500 million users, now more than a billion fans. Facebook.com is one of the most popular online sites in the world. Since May 2008, users can work the Polish language version of the portal. And in January 2010 in Poland, facebook.com has reached the number of registered users in the number of 5–6 million. With the growing popularity also increases security threat. Internet users, especially under the age of 18 years, more and more time to spend on social networking sites, and these are usually people willing to use all the innovation and new online tools.

Translated by Grzegorz Szymański

Keywords: facebook, electronic crime, crooks in social networks