ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2012
Seria: ORGANIZACJA I ZARZĄDZANIE z. 63a Nr kol. 1891

Jacek GRUBER, Ireneusz J. JÓŹWIAK, Kamil MERKS
Politechnika Wrocławska
Wydział Informatyki i Zarządzania

ZAGROŻENIA DLA INFORMACJI UDOSTĘPNIANYCH NA PORTALACH SPOŁECZNOŚCIOWYCH

Streszczenie. W artykule omówiono zagrożenia dla informacji udostępnianych na portalach społecznościowych. Opisano historię portali. Przedstawiono największe zagrożenia i pokazano sposoby radzenia sobie z nimi przez portale społecznościowe. Opisano politykę prywatności na przykładzie portalu Facebook oraz ustawienia opcji konfiguracyjnych dla tej polityki, zwiększające bezpieczeństwo użytkowników.

THREATS TO INFORMATION SHARED WITH SOCIAL NETWORKS

Summary. The history of social networking sites are discussed briefly. Key risks are described and ways to deal with these threats by social networking sites are described later in this work. Closer has been described an example of privacy policy on the example of Facebook, and configuration options are described in this policy to increase the safety of users on Facebook.

1. Wprowadzenie

Posiadanie profilu na popularnym portalu społecznościowym jest obecnie pożądane, a często wymagane. Użytkownicy sieci społecznościowej dzielą się swoimi prywatnymi informacjami i zdjęciami z innymi, nie zdając sobie sprawy z tego, że każdy ich wpis może zostać wykorzystany przeciwko nim. Bardzo łatwo określić preferencje użytkownika, stworzyć jego społecznościowe Curriculum Vitae [2], a następnie wykorzystać te informacje to zdobycia jego zaufania, uzyskania innych prywatnych informacji, dotarcia do danych, które atakujący chce przechwycić [4].

W niniejszej pracy omówiono problemy związane z bezpieczeństwem informacji umieszczanych i utrzymywanych na portalach społecznościowych. Wskazano, na co trzeba zwrócić największą uwagę, mając konto na portalu społecznościowym, jak można zostać oszukanym, przy użyciu jakich narzędzi dane członków społeczności mogą zostać wykorzystanie w złych intencjach oraz jak z tymi problemami można sobie poradzić.

2. Początki portali społecznościowych

Historia portali społecznościowych zaczyna się w 1979 roku, gdy powstał UseNet – system grup dyskusyjnych [5]. Nie był on pierwszym powstałym portalem, ale rozpoczął wymianę informacji między użytkownikami w skali masowej. Wiadomości przypominające pocztę elektroniczną użytkownicy wysyłają do serwerów UseNet. Serwery tworzące sieć P2P (starej generacji) automatycznie wymieniają je między sobą.

Kolejnym kamieniem milowym w historii było powstanie pierwszego portalu społecznościowego Classmates w 1995 roku [11]. We wstępnym założeniu portal miał pomagać odnaleźć się jego użytkownikom oraz nawiązać kontakt ze znajomymi i przyjaciółmi ze szkoły, uczelni, pracy. Classmates był pierwowzorem portalu Nasza Klasa, który został założony 11 listopada 2006 roku [1]. W początkowej fazie portal Nasza Klasa oferował niemal identyczną funkcjonalność, co jego protoplasta. Tak było do czasu przekształcenia się Naszej Klasy w portal nk [7] i obrania za wzór portalu Facebook [3] – obecnie najpopularniejszego i największego serwisu społecznościowego w Internecie. Zarejestrowani użytkownicy portalu Facebook mogą tworzyć sieci i grupy, dzielić się wiadomościami i zdjęciami oraz korzystać z różnych aplikacji. Facebook jest zintegrowany z większością „szanujących się" stron i portali internetowych. Pozwala na udostępnianie i dzielenie się treściami ze stron zewnętrznych oraz dodawanie zdjęć. Jako pierwszy wprowadził funkcję „lubienia" linków, stron, postów znajomych i innych treści. Dzięki niektórym funkcjom komunikatora Skype, portal Facebook umożliwia prowadzenie rozmów wideo i dzielenie się pulpitem. Jest on najbardziej zaawansowanym portalem i wyznacznikiem nowych funkcjonalności dla konkurencji. Jedynym konkurentem, który obecnie może dorównać Facebookowi, jest Google+ [6], który łączy w sobie dostępne już usługi społecznościowe Google Profile i Google Buzz, oraz udostępnia nowe funkcje, jak kręgi znajomych i wideospotkania. Niewątpliwie największą zaletą jest jego integracja z innymi usługami

Google [9]. Posiadanie konta pocztowego na Gmail umożliwia szybkie znalezienie znajomych. Dodatkowym atutem jest możliwość połączenia konta pocztowego z internetowym albumem zdjęć Picasa Web i udostępnianie zdjęć na swoim profilu bezpośrednio z tego albumu.

3. Typy zagrożeń dla informacji na portalach społecznościowych

Korzystanie z portali społecznościowych, poza oczywistymi zaletami, niesie również wiele zagrożeń [2],[4]. Wszystkie informacje, które świadomie lub nieświadomie udostępniamy mogą stać się celem ataku. W przypadku portali społecznościowych należy pamiętać, że niezależnie od tego, jak bardzo użytkownik się zabezpieczy, jego bezpieczeństwo w znacznym stopniu zależy od jego własnych ustawień prywatności na portalu i ustawień prywatności jego znajomych.

Podstawowym zagrożeniem, z jakimi musimy się liczyć, jest zbieranie danych o użytkownikach, cyfrowych dossier, czyli odpowiedników CV. Są to wszystkie informacje, które użytkownicy sami publikują: swoje miejsca zamieszkania, informacje o wykształceniu, wykonywanej pracy, swoje zdjęcia, kontakty, statusy, polubione strony lub linki. Wszystkie te informacje i dane osobowe mogą zostać użyte przeciw publikującym je osobom.

Przykładem pozyskiwania cyfrowego dossier jest odzyskiwanie hasła do profilu użytkownika. Dla wielu użytkowników hasłem tym może być panieńskie nazwisko matki, które często można znaleźć w sekcji rodzina. Hasłem może być imię zwierzęcia, które łatwo wydobyć, na przykład z podpisu pod zdjęciem.

Można też zbierać dane historyczne, które już kiedyś użytkownicy opublikowali. Dane te mogą zostać użyte do różnych celów, często w sposób niekorzystny dla autorów publikacji.

Do standardowych sposobów pozyskiwania danych o użytkownikach należy rozpoznawanie twarzy. Wraz z możliwością oznaczania osób na zdjęciach, wrosła łatwość rozpoznania twarzy użytkownika lub osoby, nawet jeśli nie opublikował on zdjęcia profilowego – wystarczy, że dana osoba została oznaczona na zdjęciu znajomych z portalu. Można również wyszukiwać obrazy po zawartości CBIR (ang. *content-based image retrieval*), podobnie jak w przypadku rozpoznawania twarzy. Na zdjęciach można oznaczać lokacje geograficzne, przedmioty i inne cechy.

Pozyskiwaniu danych i informacji sprzyjają trudności z całkowitym usuwaniem kont na portalach społecznościowych. Wszystkie dane udostępniane tym portalom są przechowywane na serwerach zewnętrznych, dlatego nawet w przypadku usunięcia profilu, kopia tych danych nie jest usuwana.

Do poważnych zagrożeń należy spam. Jak w każdym popularnym medium informacyjnym, trzeba się liczyć z otrzymywaniem niechcianych wiadomości i reklam.

Bardzo ważne zagrożenia to XSS (ang. *cross site scripting*), wirusy oraz robaki. Zagrożenia te są istotne, ponieważ wykorzystują luki w zabezpieczeniach albo działają, wykonując złośliwe skrypty osadzone w kodzie programów i stron portali. Dodatkowo taki wrogi kod zagraża również lokalnym plikom na maszynach użytkowników lub pliki te są wykonywane, realizując na tych maszynach niedozwolone do zdalnego wykonywania i niechciane przez użytkowników operacje.

Do istotnych zagrożeń należą agregatory SNS (ang. *social networking service*), powielające portale społecznościowe dla niewielkiego grona użytkowników, wtedy udostępniane dane często nie są zabezpieczone lub mogą oferować zabezpieczenia pozorne. Są one podobne do agregatorów zakupów grupowych, promocji i ofert. W rzeczywistości agregatory są sposobem na pozyskiwanie lub wyciąganie informacji.

Ważnym zagrożeniem jest phishing. Jest to stosowanie taktyk socjotechnicznych (ang. *social engineering*) do wydobywania od użytkowników ich sekretnych informacji. Użytkownicy ulegają phishingowi świadomie lub jest on realizowany automatycznie, za pośrednictwem programów i algorytmów zainstalowanych oraz działających bez wiedzy użytkowników.

Przejmowanie profili i szarganie reputacji w wyniku kradzieży tożsamości, to również bardzo istotne zagrożenia. Tak zwany *guy haker profiles*, który zdobędzie dane potrzebne do zalogowania do profilu ofiary, może je wykorzystać do przejęcia tego profilu, użycia loginu i hasła do logowania do innych usług, a także do szargania opinii przez opublikowanie w profilu ofiary kompromitujących informacji.

Szczególnie dokuczliwym zagrożeniem jest wykorzystywana niekiedy możliwość zwyczajnego znęcania się, poprzez wysyłanie obraźliwych wiadomości, szantaż i nękanie użytkowników i osób.

4. Ustawienia prywatności

Członkowie wirtualnych społeczności są podatni na każde z omówionych wyżej zagrożeń. Niezależnie od tego, jak dobre są i będą zabezpieczenia portali, atakującemu zawsze uda się znaleźć lukę w systemie. Lukę tę stanowić może w końcu sam użytkownik, który staje również ofiarą swojej nieroztropności. Dlatego też każdy z portali przygotował politykę prywatności, w której użytkownik ma możliwość ustawienia zasad prywatności swojego konta tak, jak sam tego chce. Wybór konkretnych opcji będzie miał wpływ na wszystkie aspekty korzystania z portalu, poczynając od wyglądu, liczby postów, reklam, upowszechniania profilu i przechowywanych informacji.

Ustawienia prywatności omówiono na przykładzie portalu Facebook, gdyż są tam najbardziej rozwinięte opcje, które pozwalają na największą liczbę konfiguracji [8],[10]. Użytkownik powinien pamiętać, że jego własne bezpieczeństwo jest również zależne od ustawień prywatności jego znajomych. Można nawet przyjąć, że ustawienia naszych znajomych mają większy wpływ na nasze bezpieczeństwo na portalu.

Ustawienia prywatności podzielone są na następujące sekcje:

- sekcja określenia swojego domyślnego ustawienia prywatności. W tej sekcji mamy do wyboru profile: Publiczny, Znajomi, Ustawienia niestandardowe. Ustawienia niestandardowe pozwalają na wybieranie osób spośród znajomych, które nie będą mogły w pełni korzystać z naszego profilu,
- sekcja nawiązywania połączenia. Określa ona, kto może wyszukać nasz profil poprzez mail lub numer telefonu oraz kto może do nas wysyłać wiadomości i zaproszenia,
- sekcja osi czasu i oznaczeń. Jest wiele ustawień dotyczących dostępności osi czasu dla innych użytkowników, publikowania na niej postów i oznaczania na zdjęciach,
- sekcja reklamy, aplikacji i witryny. W tej sekcji ustawienia: aplikacji, z których korzystamy, sposobu przekazywania informacji aplikacjom i witrynom przez naszych znajomych i rodzaju wyświetlanych reklam,
- sekcja ograniczania grona odbiorców starszych postów. W tej sekcji następuje określenie, jak mają być widoczne posty, które nie mieszczą się na pierwszej stronie profilu,
- sekcja zablokowania osoby i aplikacji. W tej sekcji następuje blokowanie osób, zaproszeń i aplikacji.

Oprócz tych bardziej zaawansowanych ustawień profilu, mamy również standardowe, jak: zmiana imienia i nazwiska, nazwy użytkownika, adresów e-mail, hasła, języka używanego na

portalu. Są też ustawienia wpływające bezpośrednio na bezpieczeństwo: pytanie pomocnicze, bezpieczne przeglądanie, powiadomienia o logowaniu, zatwierdzanie logowania (potwierdzenie hasłem otrzymanym SMS-em), hasła dostępu do aplikacji, rozpoznawanie urządzeń i dostosowanie ustawień do tego, z jakiego urządzenia korzystamy, a dodatkowo możliwość ustawień płatności i reklam społecznościowych.

Każde z tych ustawień pozwala ochronić nasze dane, a w połączeniu z ustawieniami prywatności daje poczucie bezpieczeństwa. Dzięki ich właściwej konfiguracji, podatności ograniczają się do ataków na luki w zabezpieczeniach infrastruktury portalu. Te ostatnie nie zdarzają się tak często, a w przypadku największych portali są bardzo szybko usuwane.

5. Zagrożenia

Jak już wspomniano w rozdziale 3, istnieje kilkanaście typów zagrożeń dla informacji na portalach społecznościowych. Mogą być one ze sobą połączone i użyte w kilku miejscach jednocześnie. Wcześniej omówiono je ogólnie, a obecnie postaramy się je przybliżyć, odwołując się do konkretnych wirusów, robaków, exploitów czy aplikacji eksploatujących te zagrożenia i podatności. Najpopularniejsze z nich to [8],[10]:

- *Automatyczne lubienie zewnętrznych stron* – użytkownik wchodzi za pomocą odnośnika na stronę zewnętrzną, polubioną przez swojego znajomego. W tym momencie, bez jego wiedzy, na tzw. tablicy pojawia się „lubię to” z tą witryną. Użytkownik nie jest w żaden sposób informowany o tym fakcie, zauważa to dopiero, gdy ktoś znajomy go o tym poinformuje,
- *Aplikacje informujące o odwiedzinach profilu* – użytkownicy sami je instalują, ponieważ myślą, że to bezpieczne aplikacje. Udostępniają im prawo nie tylko do własnych danych, ale również do publikowania na tablicy i na tablicach znajomych. W ten sposób aplikacja może takie dane udostępniać na zewnątrz portalu, nawet, gdy nasze ustawienia prywatności portalu na to nie pozwalają,
- *Informacje na czacie od nieznajomych* – wirusy, które się za nimi kryją, są umieszczane na stronach zewnętrznych i często „symulują” działania użytkownika – po kliknięciu uruchamiany jest skrypt, który, jeśli tylko jesteśmy zalogowani na Facebooku (np. w innej karcie lub innym oknie przeglądarki), może robić za nas praktycznie wszystko.

Jednak, aby było to możliwe, użytkownik musi ręcznie uruchomić ten skrypt, często również zaakceptować ostrzeżenie,

- *Koobface Virus* –aplikacja umożliwiająca obejrzenie filmu lub zdjęcia wysłanego przez znajomego, po kliknięciu na odnośnik do naszego komputera pobierane są kopie wirusa, które przystępują do ataku na nasze dane i rozprzestrzeniają się poprzez nośniki zewnętrzne,
- *Profileye Worm* – pokazuje osoby, które wchodzą na nasz profil, uzyskując dostęp do wszystkich informacji użytkownika,
- *Error Check Worm* – pokazuje komunikat błędu, który „wyświetlił się" innemu użytkownikowi podczas przeglądania naszego profilu,
- *Facebook Shuts You Down* – Facebook spowoduje zamknięcie systemu z powodu błędu, następnie dostanie się on do wszystkich niezabezpieczonych danych, może spowodować uszkodzenie systemu w trakcie restartu,
- *Dorkbot* – robak zbierający prywatne informacje o użytkownikach. Wykrada on loginy i hasła, a zdobyte dane wysyła do swojego twórcy za pośrednictwem protokołu HTTP. Równocześnie robak łączy się z dwiema domenami, z którymi komunikuje się dzięki protokołowi IRC. Dzięki temu twórca zagrożenia może zdalnie m.in. pobierać i instalować na zainfekowanym komputerze dowolne pliki oraz monitorować ruch sieciowy. Dorkbot ma wbudowaną funkcję blokowania dostępu do stron internetowych niemal wszystkich producentów rozwiązań antywirusowych, dlatego po wykryciu zagrożenia będzie już za późno na przeciwdziałanie,
- *Koobface.b* **–** tworzy wiadomości spamowe i wysyła je do znajomych ofiary za pośrednictwem strony Facebook. Wiadomości i komentarze generowane przez robaki zawierają nazwiska znanych osób, popularne zwroty młodzieżowe i inne informacje, których jedynym zadaniem jest przyciągnięcie naszej uwagi,
- *Ramnit* **–** największe z zagrożeń, ze względu na ciągłą ewolucję programu i brak wiedzy na temat tego, do czego jest zdolny. Na różnych komputerach może tworzyć inne zagrożenia lub podszywać się pod innego wirusa, dzięki czemu nawet sprawdzone metody nie będą na niego działać.

Każde z tych zagrożeń oraz wiele innych wykorzystuje podatność użytkowników, ich zbyt duże zaufanie oraz luki w zabezpieczeniach – dlatego są tak groźne. Personel utrzymujący portale społecznościowe jest ograniczony kadrowo, ma stale zbyt mało pracowników oddelegowanych do poszukiwania luk i tworzenia zabezpieczeń, dlatego powstaje

dedykowane do tego oprogramowanie, takie jak program Bug Bounty, mające na celu nagradzanie użytkowników portali, którzy znajdą i dokładnie opiszą lukę w zabezpieczeniach lub nieprawidłowości w działaniu portalu. Większość zagrożeń dotyczy portalu Facebook, ale jest to spowodowane tym, że im większy jest portal i im więcej skupia wokół siebie użytkowników, tym łatwiej jest wykraść z niego interesujące dane.

Ułatwieniem dla programistów portali jest to, że dany typ zagrożenia działa najczęściej tylko na własnej platformie i eksploatuje pojedynczą lukę zabezpieczeń lub podatność. To z kolei przekłada się na łatwiejsze i szybsze jej usunięcie. Organizowane są też coroczne konkursy np. Facebook Hacker Cup, które pozwalają obsłudze infrastruktury portali znaleźć młodą, zdolną kadrę, osoby które sprawdzają się jako pracownicy działów bezpieczeństwa portali społecznościowych.

6. Podsumowanie

Największą luką w zabezpieczeniach portali są sami użytkownicy. Zdecydowana większość zagrożeń jest propagowana przez nieświadomość członków społeczności. Bez ich udziału nikt nie byłby w stanie wykorzystać możliwości kradzieży ich danych. Portale wprowadzają coraz nowsze zabezpieczenia, lecz jak długo bezpieczeństwo użytkownika będzie zależało przede wszystkim od niego samego, tak długo on, jego reputacja i profil oraz jego sekretne dane, będą w ciągłym zagrożeniu.

Na większości portali można znaleźć pomoc w zakresie bezpieczeństwa wśród omówień na tzw. FAQ (*frequently asked questions*), gdzie użytkownicy znajdują odpowiedzi na najważniejsze pytania, które wcześniej inni użytkownicy już zadawali. Mogą być one pomocne w przypadku zapobiegania lub zaistnieniu zagrożenia dla zawartych na portalu informacji.

Bibliografia

1. Bodziony I.: Nasza-klasa.pl – najpopularniejszy serwis społecznościowy w Polsce. Interaktywnie.Com. 13.05.2008. http://interaktywnie.com/biznes/newsy/raporty-i-badania/nasza-klasapl--najpopularniejszy-serwis-spolecznosciowy-w-polsce-1150, 22/05/2012.

2. Bahadur G., Inasi J., De Carvalho A.: Securing the Clicks Network Security in the Age of Social Media, 2011.
3. Eldon E.: 2008 Growth Puts Facebook In Better Position to Make Money. VentureBeat, San Francisco, December 18, 2008, http://venturebeat.com/2008/12/18/2008-growth-puts-facebook-in-better-position-to-make-money/, 2/05/2012.
4. Harwood M., Goncalves M., Mathew PembleM.: Security Strategies in Web Applications and Social Networking, 2011.
5. Leug Ch., Fisher D.: From Usenet to CoWebs: interacting with social information spaces. Springer, 2003.
6. Miller C.C.: Another Try by Google to Take On Facebook. Business DayTechnology. The New York Times, June 28, 2011.
   http://www.nytimes.com/2011/06/29/technology/29google.html?_r=2, 2/05/2012.
7. Ratuszniak B: Nowa NK.pl. Serwis walczy o użytkowników. Interaktywnie.Com. 22.06.2010. http://interaktywnie.com/biznes/artykuly/biznes/nowa-nk-pl-serwis-walczy-o-uzytkownikow-14368, 22/05/2012.
8. Informacje i wiadomości w miejscach i na witrynach oraz na portalach poświęconych bezpieczeństwu aplikacji, portali internetowych, wyjaśnienia dla użytkowników (FAQ) portalu Facebook.
   http://Allfacebook.com, http://Niebezpiecznik.pl/tag/facebook/,
   http://pl-pl.connect.facebook.com/note.php?note_id=202395456446946, 22/05/2012.
9. Nasza historia w szczegółach. Wszystko o Google, Firma, Historia.
   http://www.google.com/about/company/history/, 22/05/2012.
10. Publikacje internetowe o zagrożeniach bezpieczeństwa portali społecznościowych. http://Plus.google.com, http://e-ochronadanych.pl/a,1151,portale-spolecznosciowe-a-ochrona-danych-osobowych-wybrane-zagadnienia.html,
    http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy,
    http://giodo.gov.pl/259/id_art/3204/j/pl, 22/05/2012.
11. Where people come to remember. About Classmates Online, Inc.. Classmates, 2006.
    http://www.cbsnews.com/stories/2003/05/05/60ii/main552363.shtml, 22/05/2012.

Abstract

The social network, each user provides their personal information and other photos. Is not aware that any of his post can be used against him. It is very easy to determine user preferences, create the social Curriculum Vitae, and then use this information to gain his trust, obtain other private information, reaching out to the data that an attacker wants to capture. In this paper, problems related to security of the information provided and maintained on social networking sites are discussed. Pointed out, what you should pay most attention with an account on social networking site, and how you can be cheated, using what tools the community can be used for bad intentions, as well as how these problems can be dealt with.