Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu

Bezpieczeństwo serwisów społecznościowych

REDAKTOR GOŚCINNY

Redaktorem gościnnym tego wydania OUCH! jest Lenny Zeltser. Lenny zajmuje się zabezpieczaniem od strony IT i ochroną procesów biznesowych klientów Radiant Systems oraz uczy zwalczania złośliwego oprogramowania w Instytucie SANS. Jest aktywnym użytkownikiem Twittera jako @lennyzeltser oraz prowadzi blog o security blog.zeltser.com.

WSTĘP

W tym miesiącu przyjrzymy się portalom społecznościowym takim jak Facebook, Twitter, Google+ czy LinkedIn. Są to potężne narzędzia pozwalające na nawiązywanie kontaktu pomiędzy ich użytkownikami, a także na dzielenie się między sobą treściami z ludźmi na całym świecie. Jednakże wraz z tymi wszystkimi możliwościami wiąże się znaczne ryzyko, nie tylko dla Ciebie, ale dla Twojego pracodawcy, rodziny i przyjaciół. W tym biuletynie przedstawimy jakie niebezpieczeństwa czyhają na użytkowników i jak korzystać z tego typu serwisów w sposób bezpieczny.

PRYWATNOŚĆ

Powszechną obawą dotyczącą serwisów społecznościowych jest ryzyko utraty prywatności i zamieszczenia zbyt wielu informacji o sobie. Nieumiejętne dzielenie się informacjami może prowadzić do:

- **Zniszczenia Twojej kariery**: Krępujące informacje zamieszczone w sieci mogą wpłynąć negatywnie na Twoją przyszłość. Wiele organizacji traktuje przeglądanie serwisów społecznościowych w poszukiwaniu informacji o kandydacie do pracy jako cześć procesu rekrutacyjnego. Każdy wstydliwy post, niezależnie od tego jak dawno został opublikowany, może sprawić że nie dostaniemy wymarzonej posady. Ponadto zdarza się, że podobne działania w stosunku do aplikujących studentów przeprowadzają szkoły wyższe.

- **Ataki bezpośrednio na Ciebie**: Cyberprzestępcy mogą zbierać dostępne informacje aby potem użyć ich przeciwko Tobie. Na przykład, będąc w posiadaniu pewnych informacji osobistych mogą z łatwością odgadnąć odpowiedź na „sekretne pytanie" wykorzystywane przy odzyskiwaniu hasła w innych serwisach internetowych, a może nawet ubiegać się o przyznanie przy ich użyciu kredytu.

- **Ataki na Twojego pracodawcę**: Informacje udostępniane na stronach portali społecznościowych przez pracowników konkretnych firm lub podmiotów mogą posłużyć jako doskonałe źródło danych dla konkurencji lub być wykorzystane przez przestępców przygotowujących się do ataku na serwery pracodawcy. Ponadto, działania podejmowane przez pracowników w Internecie mogą niekiedy mimowolnie odbić się na wizerunku firmy. Upewnij się jaka polityka odnośnie serwisów społecznościowych obowiązuje w Twoim miejscu pracy i jak powinieneś zabezpieczyć dane i reputację Twojej organizacji.

Najbardziej efektywnym sposobem ochrony przed tymi zagrożeniami jest ostrożność w publikowaniu informacji o

Bezpieczeństwo serwisów społecznościowych

sobie. Zawsze rozważ czy informacje, które udostępniasz dzisiaj mogłyby zostać użyte przeciwko Tobie w przyszłości. Zawęź ustawienia prywatności na swoim profilu społecznościowym tak, aby ograniczyć osobom niepowołanym dostęp do informacji osobistych które opublikowałeś lub będziesz publikował w serwisie. Pamiętaj jednak, że wszystkie zamieszczone informacje, pomimo poprawnych ustawień prywatności mogą zawsze nieumyślnie wyciec z serwisu poprzez inną usługę (na przykład aplikację na Facebooku, której udzieliłeś odpowiednich pozwoleń) lub połączonych z Twoim profilem znajomych. Dlatego zamieszczając jakiekolwiek informacje w serwisie najlepiej jest założyć, że każda z nich stanie się kiedyś dostępna publicznie. Takie podejście może uchronić przed wieloma przykrymi konsekwencjami. Bądź świadomy jakie treści inni zamieszczają o Tobie. Jeśli Twoi znajomi publikują informacje, zdjęcia lub inne dane dotyczące Twojej osoby, a Ty nie chcesz aby je udostępniano publicznie, poproś o ich usunięcie.

BEZPIECZEŃSTWO

Poza tym, że serwisy społecznościowe mogą przyczynić się do szkodliwych wycieków informacji, bardzo łatwo także wykorzystać je jako platformę do atakowania Twojego systemu komputerowego lub popełniania oszustw.

- **Login**: Chroń swoje konto w serwisach społecznościowych silnym hasłem (zobacz: wydanie OUCH z maja 2011). Nie ujawniaj tego hasła nikomu, ani nie używaj go na innych stronach. Niektóre serwisy społecznościowe takie jak Facebook czy Google+ wspierają dodatkowo silniejsze metody uwierzytelniania, takie jak hasła jednorazowe przy logowaniu z komputerów publicznych czy użycie telefonu w procesie logowania. Uruchom te opcje jeśli jest taka możliwość.

- **Szyfrowanie**: Wiele portali takich jak Facebook, Google+ czy Twitter pozwala wymusić aby komunikacja z nimi była szyfrowana (poprzez protokół zwany HTTPS). Jeśli tylko jest to możliwe włącz opcję szyfrowania HTTPS.

Portale społecznościowe są potężnym i zapewniającym dużo rozrywki narzędziem. Ale uważaj na to, co w nich udostępniasz i komu ufasz.

- **Email**: Zachowaj ostrożność klikając w linki umieszczone w wiadomościach email, które rzekomo pochodzą z serwisów społecznościowych. Zamiast tego, najlepiej wejdź na stronę serwisu poprzez zachowaną zakładkę i bezpośrednio na niej sprawdź wiadomości i powiadomienia.

- **Linki**: Uważaj na linki, w które klikasz na profilach innych osób lub stronach publicznych. Wirusy i robaki rozprzestrzeniają się tym sposobem wyjątkowo łatwo. Jeśli nazwa linku wydaje się być dziwna, podejrzana lub nazbyt zachęcająca, nie klikaj w niego, nawet jeśli pochodzi od najbardziej zaufanego przyjaciela. Możliwe że jego konto

Bezpieczeństwo serwisów społecznościowych

zostało przejęte lub zainfekowane i teraz poprzez to konto rozprzestrzeniane jest złośliwe oprogramowanie.

- **Oszustwa**: Przestępcy czerpią pełnymi garściami z otwartości wpisanej w naturę portali społecznościowych aby oszukiwać ich użytkowników. Takie oszustwo może niekiedy udawać ofertę pracy lub pieniędzy i z reguły brzmi zbyt optymistyczne. Inną popularną metodą działania przestępców jest wykorzystywanie przejętego konta do kontaktowania się ze znajomymi jego właściciela z prośbą o pomoc finansową, której rzekomo potrzebuje w wyniku utracenia swoich pieniędzy podczas pobytu za granicą. Bądź wyczulony, kiedy poprzez portal społecznościowy zgłasza się do Ciebie przyjaciel prosząc o pieniądze lub obcy proponując ofertę wydającą się być zbyt optymistyczną.

- **Aplikacje**: Niektóre portale społecznościowe dają możliwość dodania lub instalacji aplikacji stron trzecich, takich jak np. gry. Trzeba mieć na uwadze, że kontrola jakości tych aplikacji jest bardzo niska lub nie ma miejsca w ogóle, a jednocześnie mogą one mieć pełny dostęp do Twojego konta i informacji którymi się dzielisz na portalu. Złośliwe aplikacje mogą wykorzystywać ten dostęp do interakcji z Twoimi znajomymi w Twoim imieniu albo do wykradzenia i wykorzystania pozyskanych danych. Bądź ostrożny, instaluj tylko zaufane aplikacje z powszechnie znanych stron i upewnij się, że są one aktualizowane. Jeśli przestajesz korzystać z aplikacji, usuń ją.

Serwisy społecznościowe są potężnym i zapewniającym dużo rozrywki narzędziem. Pozwalają w prosty i łatwo przyswajalny sposób komunikować się z całym światem. Jeśli będziesz stosował się do wymienionych wskazówek, powinieneś móc cieszyć się w pełni z bezpiecznego korzystania z dobrodziejstw internetowych społeczności.

ŹRÓDŁA

Niektóre odnośniki w biuletynie zostały skrócone przy użyciu usługi TinyURL dla lepszej czytelności tekstu. Dla zachowania bezpieczeństwa, OUCH! używa funkcji podglądu TinyURL, która pozwala podejrzeć docelowy adres odnośnika oraz pyta o pozwolenie przed wejściem na stronę o docelowym adresie.

OnGuard Online: http://preview.tinyurl.com/5yjgjt

Microsoft: http://preview.tinyurl.com/3q4qzzr

US CERT: http://preview.tinyurl.com/df9f2d

Facebook: http://www.facebook.com/safety

Twitter: http://preview.tinyurl.com/3mb92rp

DOWIEDZ SIĘ WIĘCEJ

Zasubskrybuj comiesięczny Biuletyn Bezpieczeństwa Komputerowego – SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS z zakresu bezpieczeństwa komputerowego i osobowego. Odwiedź http://www.securingthehuman.org i dowiedz się więcej.

POLSKI PRZEKŁAD

CERT Polska jest zespołem działającym w strukturach NASK powołanym do reagownia na zdarzenia naruszające bezpieczeństwo w polskiej sieci Internet.
Należy do organizacji FIRST, w ramach której współpracuje z podobnymi zespołami na całym świecie.
WWW: http://www.cert.pl
Twitter: @CERT_Polska
Facebook: http://facebook.com/CERT.Polska

Redakcja: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, Carmen Ruyle Hardy
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak and Paweł Jacewicz