Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu

- **Wstęp**
- **Prywatność**
- **Bezpieczeństwo**

Bezpieczeństwo w serwisach społecznościowych

REDAKTOR GOŚCINNY

Ted Demopoulos jest redaktorem gościnnym tego wydania. Jest konsultantem bezpieczeństwa z wieloletnim doświadczeniem i już od dziesięciu lat prowadzi kursy SANS, w tym SEC401/501 i MGT414/512. Dowiedz się więcej o Tedzie na http://demop.com.

WSTĘP

Portale społecznościowe, takie jak Facebook, Twitter, Google+, Pinterest i LinkedIn mają bardzo potężne możliwości i pozwalają pozostać w kontakcie i dzielić się treściami z ludźmi na całym świecie. Jednak w parze z tymi możliwościami idą pewne zagrożenia - nie tylko dla Ciebie, ale także dla Twojej rodziny, przyjaciół i pracodawcy. W tym biuletynie postaramy się je omówić oraz pokazać, jak korzystać z serwisów społecznościowych bardziej bezpiecznie.

PRYWATNOŚĆ

Częstą obawą dotyczącą serwisów społecznościowych jest nasza prywatność, ochrona danych osobowych a także poufnych informacji innych osób. Potencjalne zagrożenia to:

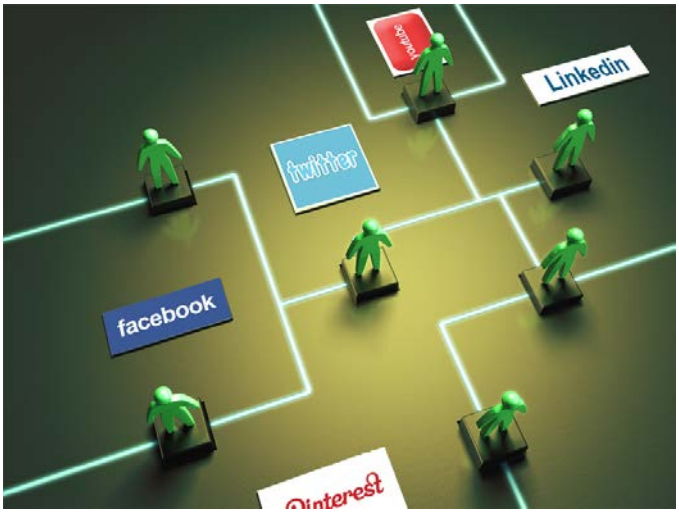
- **Wpływ na Twoją przyszłość**: Wiele organizacji przeszukuje serwisy społecznościowe w ramach weryfikacji tożsamości. Krępujące lub obciążające posty, bez względu na to jak dawno zostały opublikowane, mogą uniemożliwić uzyskanie zatrudnienia lub awansu. Opcje prywatności mogą Cię nie ochronić, ponieważ organizacje te mogą poprosić o polubienie lub dołączenie do ich stron przed procesem aplikacji.
- **Ataki wymierzone w Ciebie:** Cyberprzestępcy mogą gromadzić informacje o Tobie i użyć ich później do przeprowadzenia ataku. Mogą, na przykład, korzystać z udostępnionych przez Ciebie informacji, aby odgadnąć odpowiedź na "sekretne pytanie", zresetować Twoje hasło, przeprowadzić ukierunkowany atak e-mail (zwany spear phishing) lub ubiegać się o kartę kredytową przy użyciu Twojego imienia i nazwiska. Ponadto ataki te mogą zagrozić Ci także w świecie fizycznym, zwłaszcza jeśli przestępcy ustalą gdzie pracujesz lub mieszkasz.
- **Szkody dla pracodawcy:** Przestępcy lub konkurenci mogą używać poufnych informacji, które zamieszczasz o swojej organizacji przeciwko Twojemu pracodawcy. Ponadto, publikowane posty mogą wyrządzić szkodę dla jej reputacji. Pamiętaj, aby upewnić się jaka polityka obowiązuje w Twojej organizacji zanim opublikujesz cokolwiek na temat swojego pracodawcy.

Najlepszym zabezpieczeniem jest po prostu ograniczenie informacji zamieszczanych w serwisach społecznościowych. Owszem, opcje prywatności mogą

Bezpieczeństwo w serwisach społecznościowych

zapewnić jakąś ochronę, jednak należy pamiętać, że często są one mylące i bywają zmieniane bez Twojej wiedzy. Wówczas cokolwiek dotąd uważałeś za prywatne, może nagle stać się publiczne. Pamiętaj również, że Twoje informacje są chronione jedynie w takim stopniu jak ludzie, którym je udostępniasz. Z im większą ilością znajomych lub kontaktów dzielisz się prywatnymi informacjami, tym bardziej prawdopodobne, że dostaną się one do publicznej wiadomości. Ostatecznie najlepszym sposobem na ochronę prywatności jest przestrzeganie jednej zasady: jeśli nie chciałbyś aby mama lub szef zobaczyli Twój post, prawdopodobnie nie powinieneś go w ogóle publikować.

Miej również świadomość tego, co Twoi znajomi piszą o Tobie. To może być równie szkodliwe jeśli zamieszczają prywatne informacje lub Twoje żenujące zdjęcia. Upewnij się, że Twoi znajomi rozumieją co mogą a czego nie mogą o Tobie publikować. Jeśli jednak ktoś opublikował coś, co Ci sie nie podoba, poproś, aby to usunął. Ty również postępuj z szacunkiem i zastanów się dwa razy zanim udostępnisz informacje o innych.



Portale społecznościowe mają potężne możliwości i dostarczają rozrywki, jednak uważaj co na nich publikujesz i komu powierzasz swoje informacje.

BEZPIECZEŃSTWO

Oprócz niebezpieczeństw związanych z utratą prywatności, serwisy społecznościowe mogą być wykorzystywane przez cyberprzestępców aby dokonać ataku na Ciebie lub Twoje urządzenie. Oto kilka kroków, aby się przed tym chronić:

- **Login**: Chroń swoje konto w serwisie społecznościowym poprzez silne hasło i nie udostępniaj go nikomu ani nie wykorzystuj ponownie na innych stronach. Niektóre serwisy społecznościowe wspierają silniejsze uwierzytelnianie, takie jak dwuetapowa weryfikacja. W miarę możliwości używaj silniejszych metod uwierzytelniania.
- **Szyfrowanie**: Wiele serwisów społecznościowych pozwala na używanie szyfrowania o nazwie HTTPS, aby zabezpieczyć połączenie z witryną. W niektórych serwisach, takich jak Twitter i Google+ jest ono domyślnie włączone, podczas gdy w innych wymaga ręcznego uruchomienia w ustawieniach konta. W miarę możliwości używaj HTTPS.
- **E-mail**: Bądź podejrzliwy wobec wiadomości, które wydają się pochodzić z portalu społecznościowego - to mogą być sfałszowane wiadomości wysłane przez cyberprzestępców. Najbezpieczniejszym sposobem odpowiedzi na takie wiadomości jest zalogowanie się bezpośrednio na stronie (np. przy użyciu zapisanej zakładki) i sprawdzenie komunikatów lub powiadomień przez stronę internetową.
- **Złośliwe linki / Oszustwa:** Bądź nieufny w stosunku do podejrzanych linków zamieszczonych na portalach społecznościowych. Cyberprzestępcy mogą umieszczać je w takich serwisach, a po kliknięciu na

Bezpieczeństwo w serwisach społecznościowych

nie, użytkownik zostaje przekierowany na strony internetowe, które próbują zainfekować jego komputer. Pamiętaj, że tylko dlatego, że wiadomość jest wysyłana przez znajomego nie znaczy, że naprawdę jest jego autorstwa, gdyż jego konto mogło zostać skompromitowane. Jeżeli członek rodziny lub znajomy opublikował dziwny komunikat, którego nie można zweryfikować (np. mówiący o tym że został obrabowany i potrzebuje abyś mu wysłał pieniądze), zadzwoń do niego i potwierdź tę informację.

- **Aplikacje**: Niektóre serwisy społecznościowe umożliwiają dodanie lub zainstalowanie aplikacji innych producentów, na przykład takich jak gry. Należy pamiętać, że kontrola jakości tych aplikacji zazwyczaj jest bardzo słaba albo nie ma miejsca w ogóle, a przecież mogą one mieć pełny dostęp do Twojego konta i prywatnych informacji. Instaluj tylko te aplikacje, których aktualnie potrzebujesz, które pochodzą od dobrze znanych, zaufanych witryn i usuwaj je, gdy nie są Ci już potrzebne.

Portale społecznościowe mają ogromne możliwości i są przyjemnym sposobem komunikowania się ze światem. Jeśli zastosujesz się do przedstawionych tutaj wskazówek, będziesz mógł cieszyć się o wiele bezpieczniejszymi doświadczeniami w sieci. Aby uzyskać więcej informacji na temat bezpiecznego korzystania z serwisów społecznościowych lub w celu zgłoszenia podejrzanych działań, należy zapoznać się ze stronami zabezpieczeń serwisów z których korzystasz.

ŹRÓDŁA

W celu poprawy czytelności tekstu niektóre odnośniki w biuletynie zostały skrócone przy użyciu usługi TinyURL. 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.

11 wskazówek dla bezpiecznego korzystania z serwisów społecznościowych (j. ang.):
http://preview.tinyurl.com/b28a525

Centrum informacji o bezpieczeństwie:
https://www.facebook.com/safety

Ustawienia zabezpieczeń Facebook:
https://www.facebook.com/settings?tab=security

Słownik pojęcia bezpieczeństwa SANS (j. ang.):
http://preview.tinyurl.com/6wkpae5

Porada dnia SANS Security (j. ang.):
http://preview.tinyurl.com/6s2wrkp

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 reagowania 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
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak, Paweł Jacewicz