OUCH! | Luty 2012

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu

- **Pozyskiwanie aplikacji**
- **Konfigurowanie i korzystanie z aplikacji**
- **Aktualizacja aplikacji**
- **Zakupy poprzez aplikacje**

Zabezpieczanie aplikacji w urządzeniach mobilnych

EDYTOR GOŚCINNY

Kevin Johnson jest edytorem gościnnym tego wydania. Kevin jest starszym konsultantem bezpieczeństwa w Secure Ideas, prowadzi serwis MySecurityScanner.com i jest starszym instruktorem Instytutu SANS. Więcej możesz dowiedzieć się na www.secureideas.net i www.mysecurityscanner.com.

WSTĘP

Urządzenia mobilne stały się jednym z podstawowych narzędzi używanych zarówno w naszym życiu osobistym, jak i zawodowym. To co sprawia, że urządzenia mobilne są tak popularne to tysiące aplikacji jakie każdy z nas może dla siebie wybrać i używać. Jednakże, wraz z ogromnymi możliwościami i elastycznością aplikacji idzie szereg ryzyk, których należy być świadomym. W tym biuletynie przedstawiamy niebezpieczeństwa związane z aplikacjami w urządzeniach mobilnych oraz sposoby ich bezpiecznej instalacji i użytkowania.

POZYSKIWANIE APLIKACJI

Pierwszym krokiem jaki należy podjąć chcąc rozpocząć korzystanie z aplikacji jest zawsze upewnienie się, że została ona pobrana z bezpiecznego i zaufanego źródła. Cyberprzestępcy tworzą złośliwe aplikacje bardzo przypominające te prawdziwe, ale zainfekowane wirusami lub robakami. Jeśli przypadkowo zainstalowałeś jedną z takich aplikacji, może ona przejąć kontrolę nad Twoim urządzeniem przenośnym. Pobierając programy tylko ze znanych, zaufanych źródeł można zmniejszyć ryzyko zainstalowania zainfekowanych aplikacji. Jednak nawet w dobrze znanych sklepach z aplikacjami zdarza się znaleźć złośliwą. Może zdarzyć się to szczególnie w przypadku takich urządzeń jak Android, dla których rynki aplikacji nie są ściśle kontrolowane. Aby zmniejszyć ryzyko unikaj instalowania aplikacji, które są zupełnie nowe, pobrane przez zaledwie kilka osób lub posiadające niewiele komentarzy. Im dłużej aplikacja jest dostępna i im więcej posiada pozytywnych komentarzy, tym jest bardziej prawdopodobne, że jest ona zaufana. Instaluj tylko aplikacje, których rzeczywiście potrzebujesz. Każda dodatkowa aplikacja stwarza możliwość wykorzystania nowych luk w zabezpieczeniach, więc jeśli przestajesz z niej korzystać, należy ją usunąć z urządzenia przenośnego.

Ponadto, możesz zostać skuszony do zdobycia uprawnień super-użytkownika lub wykonania jailbreak'u – operacji, w wyniku której możliwa jest instalacja aplikacji nie dopuszczonych do sprzedaży w oficjalnym sklepie lub zmiana istniejących funkcjonalności. Bardzo przed tym przestrzegamy, gdyż „jailbreaking" nie tylko omija lub eliminuje wiele z zabezpieczeń wbudowanych w urządzenie mobilne, ale także często powoduje utratę gwarancji lub umowy wsparcia.

Zabezpieczanie aplikacji w urządzeniach mobilnych

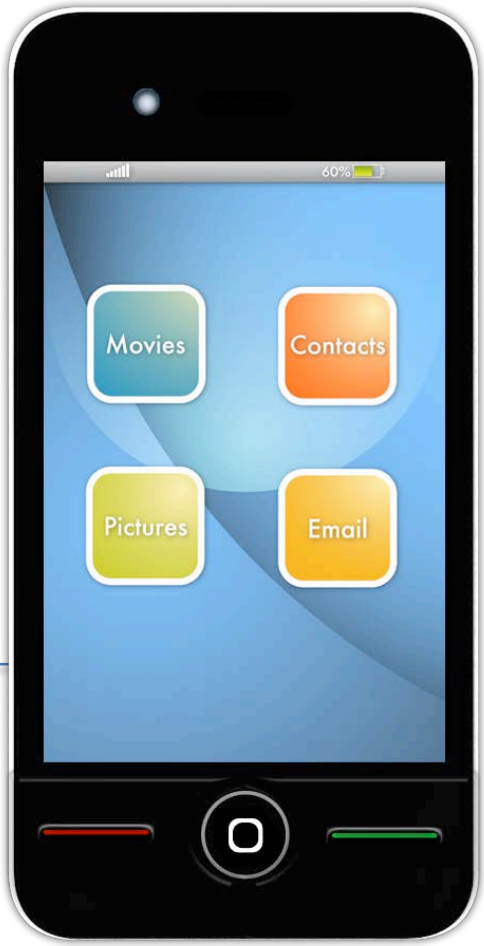
KONFIGURACJA I KORZYSTANIE Z APLIKACJI

Po zainstalowaniu aplikacji z zaufanego źródła, następnym krokiem jest upewnienie się czy jest ona bezpiecznie skonfigurowana i czy zapewnia odpowiednią ochronę naszej prywatności. Instalacja i/lub konfiguracja niektórych aplikacji wymaga udzielenia jej określonych przywilejów i uprawnień. W zależności od urządzenia, aplikacje te poproszą o potwierdzenie przed udzieleniem zezwoleniem. Zawsze rozważ przed zezwoleniem na dostęp czy Twoja aplikacja naprawdę potrzebuje tych uprawnień. Na przykład, niektóre aplikacje wykorzystują usługę geo-lokalizacji. Jeśli udostępnisz aplikacji swoją lokalizację geograficzną, może być to jednoznaczne z pozwoleniem twórcy tej aplikacji na śledzenie gdzie się przemieszczasz. Ponadto, każdy publiczny komentarz który wyślesz przez urządzenie może zawierać również informację o lokalizacji, przez co każdy może się dowiedzieć gdzie się aktualnie znajdujesz. Jeśli nie jesteś przekonany do udzielania uprawnień jakich żąda aplikacja, po prostu poszukaj innej aplikacji, która lepiej spełni Twoje wymagania.

Bądź ostrożny używając aplikacji, które żądają przechowywania poufnych informacji. Nawet jeśli aplikacja jest licencjonowana, nie ma gwarancji, że deweloper stworzył ją zgodnie z dobrymi praktykami kodowania w celu zapewnienia właściwej ochrony danych podczas przechowywania w urządzeniu lub podczas przesyłania przez Internet. Aplikacje, które przechowują poufne informacje mogą być bardzo przydatne, ale są również doskonałym celem dla cyberprzestępców. Przeczytaj szczegółowy opis aplikacji i opinie innych użytkowników aby się upewnić, że nie zaistniały dotychczas żadne problemy z bezpieczeństwem aplikacji.

AKTUALIZACJA APLIKACJI

Aplikacje, podobnie jak system operacyjny komputera czy urządzenia mobilnego, muszą być aktualizowane. Przestępcy nieustannie poszukują i w końcu znajdują luki w aplikacjach. Następnie przygotowują ataki, które wykorzystują te luki. Twórcy aplikacji równocześnie tworzą i publikują aktualizacje aby naprawić znane im słabości oprogramowania i chronić urządzenie. Im częściej aktualizacje są sprawdzane i instalowane, tym lepiej. Zalecamy monitorowanie aplikacji i ich aktualizację przynajmniej raz w miesiącu. Ponadto, niektóre aplikacje mogą być domyślne skonfigurowane aby dokonywać



Kluczem do posiadania bezpiecznych aplikacji mobilnych jest instalowanie ich tylko z zaufanych, bezpiecznych źródeł oraz upewnienie się, że są one aktualne

Zabezpieczanie aplikacji w urządzeniach mobilnych

automatycznych uaktualnień, jednak należy pamiętać, że może się to wiązać z automatycznym przyznaniem aplikacji dodatkowych uprawnień, jeżeli tego zażąda.

ZAKUPY POPRZEZ APLIKACJE

Wiele aplikacji umożliwia zakup dodatkowych funkcji, nowych treści lub usunięcie reklam. Częstym błędem niektórych jest zapisanie swoich danych uwierzytelniających do sklepu z aplikacjami lokalnie w urządzeniu, co pozwala na łatwe dokonywanie zakupów w przyszłości wewnątrz aplikacji. Nie zalecamy przechowywania danych do logowania do sklepu z aplikacjami na urządzeniu przenośnym. Pomimo, że jest to wygodne, dane te mogą stać się dostępne lub wykorzystane przez każdego, kto może mieć dostęp do telefonu komórkowego lub w przypadku jeśli zdalnie włamano się do urządzenia. Innym sposobem jest zastosowanie karty upominkowej lub wirtualnych kart kredytowych jednorazowego użytku.

PODSUMOWANIE

Gorąco zachęcamy do przestrzegania wszystkich omówionych w tym numerze dobrych praktyk. Urządzenia mobilne i aplikacje są nadal stosunkowo młodą i szybko rozwijającą się dziedziną. Dużym problemem wciąż jest to, że istnieje niewiele dostępnego oprogramowania zabezpieczającego, aby chronić siebie i swoje aplikacje. To Ty sam jesteś najlepszą ochroną dla swoich mobilnych urządzeń.

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.

Webcast Sophos o bezpieczeństwie w Android:

http://preview.tinyurl.com/73q5u76

5 sposobów ochrony aplikacji mobilnych:

http://preview.tinyurl.com/5wpghmp

iPhone przegląd zabezpieczeń:

http://preview.tinyurl.com/783hg2v

iPhone zagrożenia aplikacji:

http://preview.tinyurl.com/3w5a5cc

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