OUCH! | Styczeń 2015

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM NUMERZE..

Bezpieczne aplikacje mobilne

Wstęp

Urządzenia mobilne, takie jak tablety i smartfony stały się jedną z podstawowych technologii, z jakich korzystamy, zarówno w życiu osobistym, jak i zawodowym. To, co sprawia, że urządzenia mobilne są tak uniwersalne, to miliony aplikacji, które można na nich zainstalować. Pozwalają one nam być bardziej produktywnymi, szybko i skutecznie komunikować się i dzielić się materiałami z innymi, są wykorzystywane do nauki albo po prostu do zabawy. Jednakże, za szerokimi możliwościami aplikacji mobilnych idzie także ryzyko. Oto kilka kroków, które można podjąć, aby bezpiecznie korzystać z aplikacji mobilnych.

Redaktor gościnny

Chris Crowley w niezależnym konsultantem, certyfikowanym instruktorem SANS i autorem kursów. Jest aktywny na Twitterze **@CCrowMontance** i na Google Plus: **+ChrisCrowley**.

Instalowanie aplikacji mobilnych

Przede wszystkim należy zawsze pobierać aplikacje z bezpiecznego i zaufanego źródła. Pamiętaj, że każdy może stworzyć własną aplikację mobilną, więc trzeba uważać, skąd się je bierze. Cyberprzestępcy doskonale wyszlifowali swoje umiejętności w tworzeniu i dystrybucji zainfekowanych aplikacji mobilnych, które wyglądają jak legalne. Jeśli zainstaluje się jedną z nich, przestępcy mogą przejąć kontrolę nad urządzeniem mobilnym włączając w to czytanie wiadomości e-mail, podsłuchiwanie rozmów i dostep do listy kontaktów. Pobierając aplikacje tylko ze znanych, zaufanych źródeł zmniejsza się ryzyko omyłkowego zainstalowania zainfekowanej aplikacji. Możesz nie zdawać sobie sprawy, ale marka urządzenia mobilnego, którego używasz wpływa na możlwości w zakresie instalacji aplikacji:

Na urządzenia Apple, takie jak iPad czy iPhone, można pobrać tylko aplikacje mobilne z zarządzanego przez Apple środowiska, czyli Apple App Store. Zaletą tego rozwiązania jest to, że Apple dokonuje tam kontroli bezpieczeństwa zarówno aplikacji mobilnej jak i jej autorów. Pomimo, że Apple nie jest w stanie wyłapać wszystkich przestępców czy zainfekowanych aplikacji, to zastosowanie takiego środowiska znacznie zmniejsza ryzyko zainstalowania przez użytkownika zainfekowanej aplikacji. Ponadto, jeśli Apple znajdzie w swoim sklepie aplikację, którą uzna za zainfekowaną, szybko ją usunie. Windows Phone wykorzystuje podobne podejście do zarządzania aplikacjami.

Urządzenia mobilne z Androidem działają nieco inaczej. Android zapewnia większą elastyczność, pozwalając na pobranie aplikacji mobilnej z dowolnego miejsca w Internecie. Jednak wraz z tą elastycznością pojawia się potrzeba większej odpowiedzialności za to jakie aplikacje mobilne się pobiera i instaluje, ponieważ nie wszystkie z nich są poddawane przeglądowi. Google, podobnie jak Apple, utrzymuje zarządzany sklep z aplikacjami o nazwie Google Play. Aplikacje mobilne pobrane z Google Play przechodzą wcześniej podstawową kontrolę. Dlatego zalecamy pobierać aplikacje

Bezpieczne aplikacje mobilne

mobilne dla urządzeń z systemem Android tylko z Google Play. Należy unikać pobierania aplikacji na Androida z innych stron internetowych, ponieważ każdy, a w tym cyberprzestępcy, mogą łatwo stworzyć i rozpowszechniać tam złośliwe aplikacje mobilne i nakłaniając użytkownika do zainfekowania swojego urządzenia przenośnego. Jako dodatkową ochronę, warto rozważyć zainstalowanie antywirusa na telefonie komórkowym.

Aby zmniejszyć jeszcze bardziej ryzyko, unikaj aplikacji, które są zupełnie nowe i zostały pobrane przez niewiele osób lub takich, które mają bardzo mało pozytywnych komentarzy. Im dłużej aplikacja jest dostępna w sklepie i im więcej ma pozytywnych komentarzy, tym bardziej prawdopodobne, że można jej bezpiecznie używać. Ponadto instaluj tylko te aplikacje, których potrzebujesz i które naprawdę wykorzystujesz. Zadaj sobie pytanie: “Czy naprawdę potrzebuję tej aplikacji?”. Każda pojedyńcza aplikacja może posiadać luki, a także naruszać kwestie prywatności. Kiedy nie korzystasz już wiecej z danej aplikacji, po prostu ją usuń. Zawsze można zainstalować ją ponownie, jeśli zajdzie taka potrzeba.

Kluczem do bezpiecznego korzystania z aplikacji mobilnych jest instalowanie ich wyłącznie z zaufanych źródeł, upewnienie się, że są one zaktualizowane oraz weryfikacja uprawnień.

Możesz także ulec pokusie, aby wykonać jailbreak lub zrootować swoje urządzenie mobilne. Jest to proces polegający na niejako włamaniu się do własnego urzadzenia i instalacji na nim niezaakceptowanych oficjalnie aplikacji lub zmiany istniejących, wbudowanych funkcjonalności. Przestrzegamy przed jailbreakingiem lub rootowaniem, ponieważ tym sposobem nie tylko omija się lub eliminuje wiele punktów kontroli bezpieczeństwa wbudowanych w urządzenie przenośne, ale także często powoduje to utratę gwarancji oraz wygasniecie umów wsparcia producenta.

Uprawnienia

Po zainstalowaniu aplikacji mobilnej z zaufanego źródła należy upewnić się, że jest ona bezpiecznie skonfigurowana i że chroni naszą prywatność. Instalacja i/lub konfiguracja aplikacji mobilnych często wymaga udzielenia jej pewnych uprawnień. Zawsze zastanów się zanim nadasz aplikacji uprawnienia i pomyśl czy ta aplikacja naprawdę potrzebuje wszystkich uprawnień, których żąda do wykonania swoich funkcji? Na przykład: niektóre aplikacje korzystają z geolokalizacji. Jeśli pozwolisz, aby aplikacja znała Twoją lokalizację, umożliwisz twórcy tej aplikacji śledzenie Twojego położenia, a on z kolei może nawet sprzedać te informacje innym osobom. Jeśli nie chcesz przyznać uprawnień, o które dana aplikacja prosi, rozejrzyj się za inną, która spełnia Twoje wymagania. Pamiętaj, że na rynku aplikacji masz bardzo szeroki wybór. Urządzenia Apple pozwalają na konfigurację niektórych uprawnień aplikacji, takich jak dostęp do informacji o geolokalizacji. Można je zmienić w ustawieniach lub podczas uruchomienia danej funkcji. W urządzeniach mobilnych Windows i Android wygląda to inaczej, bo obowiązuje podejście “wszystko albo nic”. Jeśli nie udzieli się wszystkich określonych uprawnień, nie będzie można zainstalować aplikacji.

Bezpieczne aplikacje mobilne

Aktualizacja aplikacji

Aplikacje mobilne, tak jak te na komputerze i jak system operacyjny każdego urzadzenia, muszą być aktualizowane, aby być na bieżąco z coraz nowszymi zagrożeniami. Przestępcy bezustannie poszukują słabych punktów w aplikacjach. Następnie wymyślają sposoby, aby wykorzystać te słabości. Programiści, którzy stworzyli aplikację starają się regularnie publikować aktualizacje, aby naprawić te słabości i chronić urządzenie. Im częściej sprawdzasz i instalujesz aktualizacje, tym lepiej. Większość platform pozwala skonfigurować system tak, aby automatycznie aktualizował aplikacje mobilne. Gorąco zalecamy włączenie takich ustawień. Jeśli nie jest to możliwe, należy sprawdzić co najmniej raz na dwa tygodnie aktualizacje dla zainstalowanych na urządzeniu aplikacji mobilnych. Gdy Twoje aplikacje będą aktualizowane, zawsze sprawdź nowe uprawnienia, których mogą przy tej okazji wymagać.

Dowiedz się więcej

Zasubskrybuj comiesięczny biuletyn o bezpieczeństwie komputerowym SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS dotyczące 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

Przydatne linki

Socjotechnika:	http://www.securingthehuman.org/ouch/2014#november2014
Pozbywanie się urządzeń mobilnych:	http://www.securingthehuman.org/ouch/2014#june2014
Zabezpiecz swój nowy tablet:	http://www.securingthehuman.org/ouch/2013#december2013
Słownik pojęć bezpieczeństwa (ang):	http://www.securingthehuman.org/resources/security-terms
SEC575: Kurs - bezpieczeństwo urządzeń mobilnych (ang):	http://www.sans.org/sec575

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak, Paweł Jacewicz, Łukasz Siewierski

