OUCH! | Marzec, 2017

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu..

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 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

Joshua Wright zajmuje stanowisko dyrektora technicznego w Counter Hack oraz prowadzi szkolenia we współpracy z SANS Institute. Jest autorem takich pozycji jak SEC575: Mobile Device Security and Ethical Hacking, oraz Hacking Exposed: Wireless. Na Twitterze można go znaleźć jako **@joswr1ght**.

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 ją pobiera. Cyberprzestępcy doskonale opanowali umiejętność tworzenia i dystrybuowania złośliwych aplikacji, podszywających się pod te legalnie dystrybuowane. Jeśli zainstalujesz jedną z nich przestępcy mogą przejąć kontrolę nad urządzeniem mobilnym włączając w to czytanie wiadomości e-mail, podsłuchiwanie rozmów i dostęp do listy kontaktów. Pobierając aplikacje tylko ze znanych, zaufanych źródeł zmniejszasz ryzyko zainstalowania niebezpiecznej aplikacji. Pamiętaj, że marka urządzenia mobilnego, którego używasz determinuje sposób instalowania aplikacji.

Na urządzenia Apple, takie jak iPad czy iPhone, można pobrać aplikacje mobilne tylko z zarządzanego przez Apple środowiska - App Store. Zaletą tego rozwiązania jest to, że zarządzający dokonuje tam weryfikacji aplikacji przed jej oficjalną publikacją . Pomimo, że Apple nie jest w stanie wykryć wszystkich złośliwych aplikacji, to zastosowanie takiego środowiska znacznie zmniejsza ryzyko zainstalowania przez użytkownika takiej aplikacji. Ponadto, jeśli Apple znajdzie w swoim sklepie aplikację, którą uzna za niebezpieczną, 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

Bezpieczne aplikacje mobilne

odpowiedzialności za to jakie aplikacje mobilne się pobiera i instaluje, ponieważ nie wszystkie z nich są poddawane weryfikacji. 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 mobilne dla urządzeń z systemem Android tylko z Google Play. Należy unikać pobierania aplikacji na Androida z innych źródeł, ponieważ każdy, w tym cyberprzestępcy, mogą łatwo stworzyć i rozpowszechniać złośliwe aplikacje mobilne, nakłaniając użytkownika do zainfekowania swojego urządzenia. Jako dodatkową ochronę, warto rozważyć zainstalowanie antywirusa.

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

Bez względu na system Twojego urządzenia powinieneś unikać 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, których potrzebujesz i które naprawdę wykorzystujesz. Zadaj sobie pytanie: “Czy naprawdę potrzebuję tej aplikacji?”. Każda pojedyncza aplikacja może posiadać luki, a także naruszać kwestie prywatności. Kiedy nie korzystasz już więcej z danej aplikacji, po prostu ją usuń. Zawsze można zainstalować ją ponownie, jeśli zajdzie taka potrzeba.

Możesz także ulec pokusie, aby wykonać jailbreak lub zrootować swoje urządzenie. Jest to proces podobny do włamywania się do własnego urządzenia i instalacji na nim niezaakceptowanych oficjalnie aplikacji lub modyfikacji 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 wygaśnięcie umów wsparcia producenta.

Uprawnienia

Po zainstalowaniu aplikacji mobilnej z zaufanego źródła upewnij się, że jest ona bezpiecznie skonfigurowana oraz że chroni Twoją prywatność. Instalacja i/lub konfiguracja aplikacji mobilnej często wymaga udzielenia jej pewnych uprawnień. Zawsze zastanów się zanim nadasz aplikacji uprawnienia i pomyśl czy ona naprawdę potrzebuje wszystkich 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 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.

Bezpieczne aplikacje mobilne

Aktualizacje

Aplikacje mobilne, podobnie jak system operacyjny każdego urządzenia, muszą być aktualizowane, aby być na bieżąco z coraz nowszymi zagrożeniami. Przestępcy bezustannie poszukują słabych punktów w aplikacjach. Następnie wymyślają sposoby, aby wykorzystać te podatności . 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. Zalecamy włączenie takich ustawień. Jeśli nie jest to możliwe, należy sprawdzić co najmniej raz na dwa tygodnie aktualizacje dla zainstalowanych na urządzeniu aplikacji mobilnych. Przy okazji aktualizacji zawsze weryfikuj nowe uprawnienia, których aplikacje mogą wtedy 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 securingthehuman.sans.org/ouch/archives 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

Źródła

Socjotechnika:	https://securingthehuman.sans.org/ouch/2017#january2017
Bezpieczne pozbywanie się urządzeń mobilnych:	https://securingthehuman.sans.org/ouch/2016#december2016
Zabezpiecz swój nowy tablet:	https://securingthehuman.sans.org/ouch/2016#january2016
Archiwum oraz tłumaczenia OUCH:	https://securingthehuman.sans.org/ouch/archives
Kurs - bezpieczeństwo urządzeń mobilnych:	https://sans.org/sec575

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Polski przekład (NASK/CERT Polska): Sebastian Kondraszuk, Michał Strzelczyk, Jacek Sikorski

