SANS SECURITY AWARENESS

OUCH!

Biuletyn Bezpieczeństwa Komputerowego

Zabezpieczanie urządzenia mobilnego

Wstęp

Urządzenia mobline są obecnie bardzo wszechstronne, można za ich pomocą zarówno komunikować się z przyjaciółmi, robić zakupy, korzystać z bankowości elektronicznej, oglądać filmy czy grać w gry. To jedynie kilka przykładów, jednak zdecydowanie urządzenia mobilne stały się nieodłączną częścią życia znacznej części społeczeństwa. W tym wydaniu przedstawiamy kilka prostych porad, które pomogą bezpiecznie korzystać z urządzenia mobilnego oraz odpowiednio je zabezpieczyć.

Zabezpieczanie urządzenia

Być może to zaskakujące, jednak największym zagrożeniem dla bezpieczeństwa twojego urządzenia nie są hakerzy, a działania podejmowane przez ciebie. O wiele bardziej prawdopodobne jest, że zgubisz lub zapomnisz o swoim urządzeniu niż to, że ktoś przełamie jego zabezpieczenia. Pierwszą czynnością, którą powinieneś wykonać jest włączenie automatycznej blokady ekranu. Ochrona urządzenia złożonym kodem lub odciskiem palca da ci pewność, że gdy zostawisz urządzenie na chwilę bez opieki, nie skończy się to wysłaniem z twojego telefonu do działu HR wiadomości o odejściu z pracy. Poniżej znajdziesz inne wskazówki, które również mogą być pomocne:

Aktualizacje

Włącz funkcję automatycznej aktualizacji, dzięki temu urządzenie będzie zawsze działać w najnowszej wersji systemu operacyjnego oraz zainstalowanych aplikacji. Przestępcy stale poszukują nowych podatności w oprogramowaniu, a jeśli posiadasz zainstalowane wszystkie dostępne poprawki bezpieczeństwa o wiele trudniej będzie im się włamać się do twojego urządzenia.

Geolokalizacja

Zainstaluj lub uruchom oprogramowanie, które umożliwi zdalne śledzenie położenia telefonu. Gdy zgubisz urządzenie lub zostanie ono skradzione będziesz mógł się z nim połączyć przez internet, określić jego lokalizację, a w najgorszym przypadku usunąć z niego zdalnie wszystkie informacje.

Zaufane aplikacje

Potrzebne aplikacje instaluj jedynie z zaufanych źródeł. Dla iPada czy iPhone jest to sklep Apple App Store, dla urządzeń opartych o system Android - sklep Google Play, zaś dla tabletów Amazon - Amazon App Store. Oczywiście, możliwe jest pobieranie aplikacji z innych stron, jednak nie są one zazwyczaj weryfikowane i ryzyko wystąpienia aplikacji zawierającej szkodliwe oprogramowanie jest o wiele wyższe. Dobrą praktyką jest również sprawdzenie jakie opinie posiada aplikacja

i czy jest aktualizowana przez producenta. Omijaj szerokim łukiem zupełnie nowe aplikacje posiadające małą liczbę opinii. Przede wszystkim, niezależnie skąd pochodzi oprogramowanie, jeśli nie jest ci już potrzebne, sugerujemy jego odinstalowanie z urządzenia.

Ustawienia prywatności

Za każdym razem kiedy instalujesz nową aplikację sprawdź jej ustawienia prywatności. Sprawdź, czy rzeczywiście oprogramowanie potrzebuje dostępu do listy twoich znajomych i listy kontaktów? Rekomendujemy domyślne wyłączenie ustawień geolokalizacyjnych dla wszystkich aplikacji, a następnie udostępnienie lokalizacji tylko tym aplikacjom, co do których masz pewność, że jej wymagają.

Kopie Zapasowe

Regularnie twórz kopie zapasowe! Urządzenia mobilne często posiadają usługi automatycznego tworzenia kopii zapasowych zdjęć oraz wiadomości. Takie kopie zapasowe często zapisują również informacje o konfiguracji aplikacji oraz innych informacji o urządzeniu, dzięki czemu o wiele prościej można przenieść dane do nowego urządzenia po zgubieniu lub zniszczeniu starego.

Praca

W pracy zachowaj szczególną ostrożność. Nie wykonuj zdjęć i nie nagrywaj filmów mogących zawierać wrażliwe informacje takie jak zdjęcia zapisanych haseł dostępowych czy tablic z poufnymi danymi.

Urządzenie mobilne to obecnie wielozadaniowe narzędzia, z których na pewno chciałbyś jak najdłużej korzystać i się nimi cieszyć. Wskazówki zawarte w tym biuletynie na pewno pomogą poprawić jego bezpieczeństwo.

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

Bezpieczne hasła:	https://www.sans.org/u/A3E
Kopie zapasowe / Przywracanie systemu:	https://www.sans.org/u/A3z
Bezpieczna utylizacja urządzenia mobilnego:	https://www.sans.org/u/A3u
Bezpieczne użycie aplikacji mobilnych:	https://www.sans.org/u/A3p
Wskazówka dnia SANS:	https://www.sans.org/tip_of_the_day.php

Licencja

Editorial Board: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Polski przekład (NASK/CERT Polska): Sebastian Kondraszuk, Michał Strzelczyk, Jacek Sikorski