Bezpieczeństwo urządzeń mobilnych

Wstęp

Urządzenia mobilne to łatwy sposób komunikowania się ze znajomymi, robienia zakupów lub korzystania z usług bankowych, oglądania filmów, grania w gry i wykonywania wielu innych czynności. Urządzenia mobilne są ważną częścią życia i ważne jest, aby zapewnić ich bezpieczne korzystanie.

Zabezpiecz swoje urządzenia

Może to wydawać się dziwne, ale największym zagrożeniem dla Twojego urządzenia mobilnego najprawdopodobniej nie są cyberprzestępcy, lecz Ty sam. Bardziej prawdopodobne jest, że zgubisz urządzenie mobilne, niż to, że ktoś się do niego włamie. Najważniejszą rzeczą, którą powinieneś zrobić, aby chronić swoje urządzenie, jest włączenie automatycznego blokowania ekranu, gdy urządzenie jest bezczynne. Oznacza to, że aby korzystać z urządzenia, musisz odblokować ekran silnym hasłem, swoją twarzą lub odciskiem palca. Dzięki temu osoby trzecie będą miały znacznie trudniejszy dostęp do informacji, jeśli urządzenie zostanie zgubione lub skradzione. Dodatkowo, w przypadku większości urządzeń mobilnych, włączenie blokady ekranu umożliwia również szyfrowanie, co jest dodatkową ochroną w przechowywaniu informacji na urządzeniu.

Kilka wskazówek, które pomogą chronić Twoje urządzenia:

1. **Aktualizacja**: Włącz automatyczne aktualizacje na swoich urządzeniach, aby zawsze korzystały z najnowszej wersji systemu operacyjnego i aplikacji. Atakujący cały czas szukają nowych luk w oprogramowaniu, a dostawcy stale publikują aktualizacje i łatki, aby je naprawić. Aktualizowanie urządzeń sprawia, że są one znacznie trudniejsze do zhakowania. Wybierając nowe urządzenie z Androidem, spójrz na zobowiązanie dostawcy do aktualizacji urządzenia. Urządzenia Apple są aktualizowane przez samą firmę, podczas gdy urządzenia mobilne z Androidem są aktualizowane przez dostawcę, który sprzedał dane urządzenie, a nie wszyscy dostawcy systematycznie aktualizują swoje urządzenia. Jeśli używasz starego urządzenia, które nie jest już wspierane lub nie można go zaktualizować, zastanów się, czy nie kupić nowego urządzenia, które jest w pełni wspierane.

2. **Śledzenie**: Zainstaluj oprogramowanie do zdalnego śledzenia urządzenia mobilnego przez Internet. W ten sposób możesz połączyć się z nim przez Internet i sprawdzić jego lokalizację w przypadku zgubienia lub kradzieży urządzenia lub zdalnie wyczyścić wszystkie informacje.

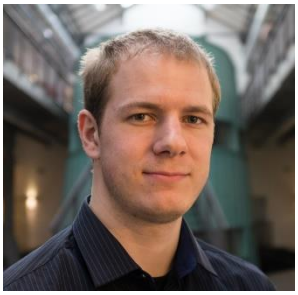
3. **Zaufane aplikacje mobilne**: Instaluj tylko potrzebne aplikacje z pewnych źródeł. W przypadku urządzeń Apple, takich jak iPady lub iPhone'y jest to App Store firmy Apple. W przypadku urządzeń z systemem Android użyj Google Play, natomiast w przypadku tabletów Amazon skorzystaj z Amazon App Store. Oczywiście możesz instalować aplikacje z innych witryn, ale musisz mieć na uwadze, że nie są one sprawdzane i znacznie częściej są zainfekowane, co może narażać Twoją prywatność. Przed jej pobraniem aplikacji upewnij się, czy ma ona pozytywne oceny i jest aktywnie aktualizowana przez dostawcę. Trzymaj się z dala od zupełnie nowych aplikacji, aplikacji z niewielką liczbą ocen lub aplikacji, które są rzadko aktualizowane.

4. **Opcje prywatności**: Urządzenia mobilne zbierają obszerne informacje, zwłaszcza jeśli zabierasz je wszędzie ze sobą. Dokładnie przejrzyj ustawienia prywatności urządzenia, w tym śledzenie lokalizacji, i upewnij się, że poufne powiadomienia (takie jak kody weryfikacyjne) nie pojawiają się na ekranie, gdy urządzenie jest zablokowane.

5. **Praca**: Upewnij się, że każde urządzenie mobilne, którego używasz do pracy, jest dopuszczone do użytku służbowego. W pracy zachowaj szczególną ostrożność i nigdy nie rób zdjęć ani filmów, które mogą przypadkowo zawierać poufne informacje.

Twoje urządzenia mobilne to potężne narzędzie. Wystarczy wykonać kilka prostych kroków, aby zapewnić bezpieczeństwo Tobie i Twoim urządzeniom mobilnym.

Redaktor gościnny



Jeroen Beckers jest ekspertem ds. bezpieczeństwa mobilnego w NVISO, współautorem OWASP MASVS i MSTG, instruktorem instytutu SANS i autorem SEC575: Kurs dotyczący bezpieczeństwa urządzeń mobilnych i etycznego hakowania. Możesz znaleźć Jeroena przez LinkedIn https://www.linkedin.com/in/beckersjeroen/.

Źródła

Moc aktualizacji: https://www.sans.org/newsletters/ouch/the-power-of-updating
Bezpieczne korzystanie z aplikacji mobilnych: https://www.sans.org/newsletters/ouch/securely-using-mobile-apps/
Oszustwa bazujące na wiadomościach tekstowych: https://www.sans.org/newsletters/ouch/messaging-smishing-attacks/
Tworzenie haseł w prostszy sposób: https://www.sans.org/newsletters/ouch/making-passwords-simple/
Ataki i oszustwa telefoniczne: https://www.sans.org/newsletters/ouch/vishing/

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz