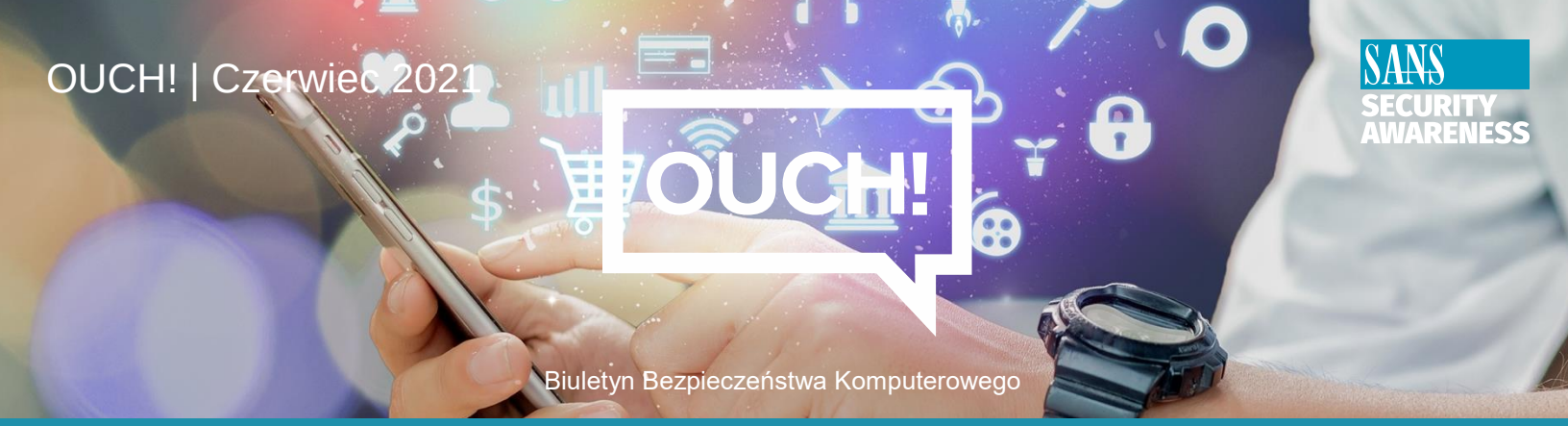

Biuletyn Bezpieczeństwa Komputerowego

Bezpieczne korzystanie z aplikacji mobilnych

Wstęp

Urządzenia mobilne takie jak tablety, smartfony i smartwatche, stały się jedną z podstawowych technologii, z których korzystamy zarówno w życiu prywatnym jak i zawodowym. To co czyni te urządzenia tak przydatnymi i potężnymi, to setki tysięcy dostępnych aplikacji, z których możemy wybierać. Aplikacje te pozwalają nam być bardziej produktywnymi, szybko i skutecznie komunikować się z przyjaciółmi i rodziną, dzielić się materiałami z innymi oraz wykorzystywać je do nauki jak i zabawy. W tym wydaniu biuletynu przedstawimy niebezpieczeństwa związane z aplikacjami w urządzeniach mobilnych oraz sposoby na bezpieczną instalację oraz ich użytkowanie.

Instalowanie aplikacji mobilnych

Cyberprzestępcy opanowali umiejętność tworzenia i rozpowszechniania szkodliwych aplikacji, których wygląd bardzo przypomina te prawdziwe. Jeśli zainstalujesz jedną z tych aplikacji, przestępcy będą mogli przejąć kontrolę nad urządzeniem włączając w to czytanie wiadomości e-mail, dostęp do listy kontaktów oraz podsłuchiwanie rozmów. Pobierając aplikację tylko ze znanych, zaufanych źródeł zmniejszasz ryzyko instalacji niebezpiecznej aplikacji. Pamiętaj, że marka urządzenia mobilnego, którego używasz determinuje sposób instalacji aplikacji.

W przypadku urządzeń marki Apple, należy pobrać aplikacje mobilne wyłącznie ze sklepu Apple App Store. Zaletą takiego rozwiązania jest to, że Apple sprawdza wszystkie aplikacje mobilne pod kątem bezpieczeństwa przed ich publikacją w serwisie. Pomimo, że Apple nie jest w stanie wykryć wszystkich szkodliwych aplikacji, to zastosowanie takiego rozwiązania znacznie zmniejsza ryzyko zainstalowania podejrzanej aplikacji. Ponadto, jeśli Apple znajdzie w swoim sklepie aplikację, którą uzna za niebezpieczną, szybko ją usunie z serwisu.

W przypadki urządzeń z systemem operacyjnym Android, aplikacje należy pobierać tylko ze sklepu z aplikacjami Google Play, który jest prowadzony przez firmę Google. Podobnie jak Apple, Google sprawdza wszystkie aplikacje pod kątem bezpieczeństwa przed udostępnieniem ich klientom. Różnica w przypadku urządzeń z systemem operacyjnym Android polega na tym, że system po włączeniu odpowiedniej opcji pozwala na zainstalowanie aplikacji spoza oficjalnego sklepu Google. Zdecydowanie odradzamy instalowanie aplikacji z nieznanego źródła. Cyberprzestępcy z łatwością mogą stworzyć i rozpowszechniać szkodliwe aplikacje mobilne, które w podstępny sposób mogą zainfekować urządzenie mobilne.
Bez względu z jakiej marki urządzenia korzystasz, sprawdź aplikację przed jej zainstalowaniem. Sprawdź jak długo aplikacja jest dostępna, ile osób z niej korzysta oraz kto jest jej wydawcą.

Im dłużej aplikacja jest dostępna w sklepie i im ma więcej pozytywnych komentarzy, tym bardziej prawdopodobne, że można z niej bezpiecznie korzystać. Ponadto instaluj tylko te, których potrzebujesz i które naprawdę wykorzystujesz. Zadaj sobie pytanie: "Czy naprawdę potrzebuję tej aplikacji?" Każda pojedyncza aplikacja może posiadać luki bezpieczeństwa, a także naruszać kwestie prywatności. Kiedy nie korzystasz już z danej aplikacji, po prostu ją usuń. Zawsze możesz ją zainstalować ponownie, jeśli zajdzie taka potrzeba.

Prywatność i uprawnienia

Po zainstalowaniu aplikacji mobilnej z zaufanego źródła należy upewnić się, że jest skonfigurowana w odpowiedni sposób i chroni naszą prywatność. Zastanów się czy aplikacja mobilna naprawdę musi znać lokalizację lub mieć dostęp do kontaktów? Na przykład, niektóre aplikacje korzystają z geolokalizacji. Jeśli pozwolisz, aby aplikacja znała Twoją lokalizację, umożliwisz twórcom tej aplikacji śledzenie Twojego położenia, a on z kolei może sprzedać te informacje innym osobom czy firmom. Jeśli nie chcesz przyznać uprawnień, o które dana aplikacja prosi, rozejrzyj się za inną, która spełni Twoje oczekiwania. Pamiętaj, że na rynku aplikacji masz bardzo szeroki wybór.

Aktualizacje

Aplikacje mobile, podobnie jak system operacyjny każdego urządzenia, muszą być nieustannie aktualizowane, aby być na bieżąco z coraz nowszymi zagrożeniami. Przestępcy nieustannie poszukują słabych punktów w aplikacjach i wymyślają sposoby, aby wykorzystać te podatności. Twórcy aplikacji starają się regularnie publikować aktualizacje, aby naprawić te podatności i ochronić urządzenie. Im częściej sprawdzasz i instalujesz aktualizacje, tym lepiej. Większość platform pozwala skonfigurować system tak, aby automatycznie wykonywał aktualizacje. Zalecamy włączenie takich funkcjonalności.

Mobilne aplikacje pozwalają wykorzystać w pełni potencjał urządzeń mobilnych. Pamiętaj jedynie, aby uważać na aplikacje, które wybierasz oraz upewnij się, że korzystasz z nich w sposób bezpieczny i pewny.

Redaktor gościnny

Domenica Crognale jest inżynierem ds. zapewnienia jakości oraz certyfikowanym instruktorem w Instytucie SANS. Jest współautorką projektu FOR585: Smartphone Analysis In-Depth. Znajdź Domenica on Twitter @domenicacrognal.

Źródła

Moc aktualizacji: https://www.sans.org/security-awareness-training/resources/power-updating
Prywatność - chroń swoje cyfrowe życie: https://www.sans.org/newsletters/ouch/privacy/
Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz