OUCH! Grudzień 2022

Biuletyn Bezpieczeństwa Komputerowego

Utylizacja urządzeń mobilnych

Wstęp

Urządzenia mobilne takie jak smartfony, smart watche i tablety rozwijają się w zdumiewającym tempie. W rezultacie często się zdarza, że urządzenia są zmieniane na nowe raz w roku. Niestety, możesz nawet nie zdawać sobie sprawy z tego jak wiele prywatnych danych jest przechowywanych na takim urządzeniu - zdecydowanie więcej niż na komputerze. Poniżej przyjrzymy się różnym typom danych, które są przechowywane na Twoich urządzeniach mobilnych oraz temu jak je bezpiecznie usunąć przed wyrzuceniem lub zamianą urządzenia. Jeśli urządzenie, którego chcesz się pozbyć zostało Ci udostępnione przez pracodawcę, należy postępować według firmowych procedur.

Twoje dane

Urządzenia mobilne zbierają więcej wrażliwych danych niż Ci się wydaje, włączając w to dane na temat:

Miejsca zamieszkania i pracy, oraz codziennych podróży.
Szczegółów kontaktów zapisanych w książce telefonicznej, w tym dane rodziny, przyjaciół oraz współpracowników.
Historii połączeń - przychodzących, wychodzących, połączeń nieodebranych oraz wiadomości nagranych na pocztę głosową.
Wiadomości sms lub rozmów tekstowych wykorzystujących czaty w grach lub social mediach.
Prywatnych zdjęć, filmów i nagrań audio.
Zapisanych haseł i informacji o kontach, na których jesteś zalogowany na urządzeniu mobilnym, takich jak Twój bank, konta na portalach społecznościowych oraz skrzynki poczty elektronicznej.
Twojego wieku oraz warunków zdrowotnych.
Wykonywanych operacji finansowych, metod płatności oraz danych kart płatniczych.

Wymazywanie danych z urządzenia

Bez względu na to w jaki sposób pozbywasz się urządzenia, czy wymieniasz urządzenie na nowe, oddajesz stare urządzenie znajomemu, sprzedajesz je lub oddajesz do punktu utylizacji, najpierw należy usunąć z niego wszystkie wrażliwe informacje. Nie można zakładać, że kolejny właściciel urządzenia postąpi właściwie i wyczyści dane. Pierwszym krokiem powinno być wykonanie kopii zapasowej, dzięki niej bez problemu będziesz mógł przenieść wszystkie swoje dane oraz ustawienia na nowe urządzenie. Kiedy już wykonasz kopię zapasową, należy wykonać tak zwany twardy reset. Procedura ta usuwa wszystkie dane z urządzenia i przywraca je do ustawień fabrycznych. W czasie procesu resetowania urządzenia możesz zostać poproszony o podanie hasła do wykorzystywanych rozwiązań chmurowych, takich jak na przykład Google Drive lub iCloud, dzięki temu urządzenie zostanie odłączone od tych rozwiązań. Poniżej przedstawione procesy przywracania urządzeń do ustawień fabrycznych dotyczą dwóch najpopularniejszych urządzeń - Apple i Android.

Urządzenia z systemem Apple iOS: Ustawienia | Ogólne | Przenieś zawartość lub wyzeruj | Wymaż zawartość i ustawienia.

Urządzenia z systemem Android: Ustawienia | System | Opcje resetowania | Wymaż wszystkie dane (te opcje mogą być różne w zależności od producenta Twojego urządzenia).

SIM & Karty Zewnętrzne

Dodatkowo podczas resetowania urządzenia, warto rozważyć co zrobić z kartą SIM (Subscriber Identity Module). Ta mała karta wydawana przez operatorów telefonii komórkowej służy do identyfikacji Twojego urządzenia i pozwala na wykonywanie połączeń oraz korzystanie z danych mobilnych. Kiedy usuwasz dane z urządzenia, karta SIM zachowuje dane o Twoim koncie i jest z Tobą powiązana. Jeśli zachowujesz ten sam numer telefonu i tylko zmieniasz urządzenie, najlepiej porozmawiać z operatorem telekomunikacyjnym o możliwościach przeniesienia karty SIM do nowego urządzenia. Jeśli nie jest to możliwe, należy zachować starą kartę SIM, a następnie ją zniszczyć. Coraz więcej najnowszych smartfonów w dzisiejszych czasach korzysta z kart eSIM, są to wirtualne karty SIM i są przeciwieństwem zwykłych fizycznych kart SIM. Dane z kart eSIM są wymazywane podczas procesu resetowania urządzenia.

Na koniec należy wspomnieć również o tym, że niektóre urządzenia z systemem Android pozwalają na korzystanie z przenośnych kart SD (Secure Digital) zapewniających dodatkową pamięć. Przed utylizacją należy je wyjąć z urządzenia. Karty te często mogą zostać wykorzystane w nowych urządzeniach. Posiadając odpowiedni adapter można używać ich również jak jako pamięć masową (pendrive) do przechowywania danych z komputera. Jeśli nie jest możliwe ponowne wykorzystanie karty, należy postąpić z nią tak jak ze starą kartą SIM, zalecamy jej fizyczne zniszczenie.

Jeśli nie jesteś pewny co do kroków opisanych powyżej lub opcje resetowania Twojego urządzenia są inne, wystarczy zabrać urządzenie do sklepu, w którym zostało ono kupione lub do operatora telefonii komórkowej. Dodatkowo, jeśli planujesz wyrzucić urządzenie, warto rozważyć oddanie go do punktu utylizacji urządzeń elektronicznych lub do organizacji charytatywnej. Istnieje wiele wspaniałych organizacji charytatywnych, które przyjmują używane urządzenia mobilne oraz wiele punktów utylizacji, które poddają urządzenia recyklingowi.

Redaktor gościnny

Heather Mahalik (@HeatherMahalik) Jest starszym Dyrektorem ds. Cyfrowej Inteligencji w Cellebrite i Kierownik Programu Nauczania SANS DFIR, FOR585 Autor i wykładowca wydziałowy w SANS. Heather's career has been based upon forensic research and 20 years of case work. Bloguje na www.smarterforensics.com/blog.

Źródła

Bezpieczne korzystanie z aplikacji mobilnych:
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltfdc5d4a5c4b09c58/60b66cffdbcf2a08eed7a795/ouch!_polish_june_2021_securely_using_mobile_apps.pdf
Bezpieczeństwo urządzeń mobilnych:
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltf4e23f61005c39a7/60e8b43fb1bfa71471c7c3a0/ouch!_july_2021_securing_your_mobile_device_pl.pdf
Przekaż swój telefon komórkowy https://www.makeuseof.com/best-places-to-donate-your-old-phone/
SANS Course: Advanced Smartphone Forensics Course: https://sans.org/for58

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz