SANS SECURITY AWARENESS

OUCH!

Biuletyn Bezpieczeństwa Komputerowego

Utylizacja urządzenia mobilnego

Informacje ogólne

Urządzenia mobilne, takie jak smartfony, smartwatche i tablety, rozwijają się w zawrotnym tempie. W rezultacie, okres ich użytkowania staje się krótszy, a użytkownicy częściej je wymieniają. Niestety, bardzo często nie zdają sobie sprawy, jak wiele cennych danych znajduje się na urządzeniach. Poniżej omówimy, jakie informacje mogą znajdować się na urządzeniu mobilnym i w jaki sposób możemy się ich pozbyć, tak aby informacje nie trafiły w niepowołane ręce. Jeżeli telefon należy do Twojego pracodawcy, lub posiadasz zapisane na nim dane służbowe, skonsultuj się najpierw ze swoim przełożonym. Uzyskasz w ten sposób informacje o procedurach tworzenia kopii zapasowych i utylizacji urządzenia.

Twoje dane

Nasze urządzenia mobilne często przechowują więcej prywatnych informacji niż komputery. Oto przykłady niektórych z nich:

⚠

- **Adres zamieszkania, miejsce pracy, odwiedzane lokalizacje**
- **Dane kontaktowe wszystkich osób znajdujących się w książce adresowej, w tym rodziny, przyjaciół i współpracowników**
- **Historia połączeń telefonicznych, w tym połączeń przychodzących, wychodzących, poczty głosowej i połączeń nieodebranych**
- **Wiadomości SMS oraz rozmowy prowadzone przez komunikatory, gry, czy aplikacje społecznościowe**
- **Historia przeglądania stron internetowych, historia wyszukiwania, pliki cookie i strony w pamięci podręcznej**
- **Prywatne zdjęcia, nagrania wideo i pliki audio**
- **Hasła i inne dane dostępowe do kont, takich jak bankowość elektroniczna, media społecznościowe, czy poczta elektroniczna**
- **Informacje dotyczące zdrowia, w tym wieku, pulsu serca, przebiegu ćwiczeń, ciśnienia krwi itp.**

Wymazanie danych z urządzenia

Niezależnie od sposobu w jaki pozbywasz się urządzenia mobilnego, czy to oddając je komuś, wymieniając na nowe, przekazując komuś z rodziny, odsprzedając, czy wyrzucając - musisz być pewny, że usunąłeś z niego wszystkie cenne informacje. Samo skasowanie danych nie wystarczy, powinieneś mieć pewność, że usunąłeś je w sposób bezpieczny. Najprostszym sposobem jest przywrócenie urządzenia do ustawień fabrycznych. Położenie opisywanej funkcji różni się w zależności od posiadanego sprzętu i wersji zainstalowanego oprogramowania. Poniżej przedstawiamy czynności przywracania ustawień fabrycznych dla dwóch najpopularniejszych systemów urządzeń mobilnych. Dodatkowym krokiem jest upewnienie się, że na urządzeniu jest włączone szyfrowanie zawartości pamięci. Ważne informacje są przechowywane w

zaszyfrowanej postaci, a ich odszyfrowanie następuje za każdym razem gdy użytkownik wprowadzi kod PIN, aby odblokować telefon. Zalecamy również utworzenie kopii zapasowej urządzenia przed jego przywróceniem do ustawień fabrycznych.

- **Urządzenia Apple z systemem iOS: Ustawienia | Ogólne | Wyzeruj | Wymaż zawartość i ustawienia**
- **Urządzenia z systemem Android: Ustawienia | Prywatność | Ustawienia fabryczne**

Karty SIM i karty pamięci

Oprócz samego urządzenia, należy również rozważyć, co zrobić z kartą SIM (Subscriber Identity Module). To właśnie dzięki karcie SIM telefon nawiązuje połączenia telefoniczne oraz transmisję danych. Trzeba mieć na uwadze, że przywracając telefon do ustawień fabrycznych, żadne informacje z karty SIM nie są usuwane. Porozmawiaj ze swoim operatorem na temat przeniesienia karty SIM do nowego telefonu. Jeśli nie ma takiej możliwości po prostu ją zniszcz. Takie działanie ma na celu uniemożliwić jej ponowne wykorzystanie, w celu podszycia się pod Ciebie i uzyskania dostępu do Twoich kont lub danych. Niektóre urządzenia z systemem Android przechowują dane na osobnych kartach pamięci SD (Secure Digital). Pamiętaj, aby ją usunąć z telefonu zanim się go pozbędziesz. Karty te mogą być często ponownie używane w nowych urządzeniach przenośnych lub mogą służyć jako pamięć masowa w komputerze za pomocą adaptera USB. Jeśli ponowne użycie karty SD nie jest możliwe, zalecamy jej fizyczne zniszczenie, tak jak w przypadku starej karty SIM.

Jeśli nie jesteś pewny co do któregoś z opisanych tutaj kroków lub jeśli nie potrafisz znaleźć opcji resetowania urządzenia, udaj się do miejsca, w którym zakupiłeś telefon lub zabierz go do serwisu, gdzie pomocy udzieli Ci profesjonalista. Niemniej jednak, jeśli zamierzasz po prostu wyrzucić telefon do śmieci, rozważ oddanie go jednej z organizacji charytatywnych lub wrzucenie go do odpowiednich pojemników na elektronikę, znajdujących się w różnych sklepach i salonach sieci komórkowych.

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

Redaktor Gościnny

Christopher Crowley *(@CcrowMontance) jest niezależnym konsultantem pracującym w Waszyngtonie, zajmującym się cyberbezpieczeństwem. Okazjonalnie publikuje tweety i artykuły na blogach. Wkrótce wyda książkę poświęconą działalności zespołów SOC (Security Operations Centers). Jest starszym wykładowcą w Instytucie SANS.*

Źródła

SANS Course: Pen Testing Mobile Devices:	https://sans.org/sec575
SANS Course: Advanced Smartphone Forensics Course:	https://sans.org/for585
Porady FTC dotyczące utylizacji urządzenia mobilnego:	https://www.consumer.ftc.gov/articles/0200-disposing-your-mobile-device