OUCH! | Grudzień 2016

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu..

- **Twoje dane**
- **Usuwanie danych z urządzenia**
- **Karty SIM i karty pamięci**

Bezpieczne pozbywanie się urządzeń mobilnych

Informacje ogólne

Urządzenia mobilne, takie jak smartfony, smartwatche czy tablety, wciąż rozwijają się w zawrotnym tempie. Wynikiem tego jest dość krótki okres ich używania - często są wymieniane co rok. Niestety, dużo osób pozbywa się takich urządzeń nie zważając na osobiste dane, które mogą się znajdować na tych urządzeniach. W tym biuletynie zwrócimy uwagę na Twoje dane, które mogą się znajdować na urządzeniach mobilnych oraz wskażemy jak się ich bezpiecznie pozbyć. Jeśli telefon należy do Twojego pracodawcy, lub służył Ci do pracy, skontaktuj się z przełożonym, aby się dowiedzieć jak powinieneś postępować zanim wykonasz opisane poniżej kroki.

Redaktor gościnny

Heather Mahalik (**@HeatherMahalik**; **+HMahalik**) jest głównym badaczem śledczym w ManTech CARD. Heather jest współautorką i prowadzącą kurs w Instytucie SANS Advanced Smartphone Forensics (FOR585) i instruktorem Windows Forensic Analysis (FOR408). Prowadzi bloga **smarterforensics.com**.

Twoje dane

Urządzenia mobilne przechowują bardzo dużo prywatnych danych, często więcej niż komputer. Przykładami takich danych są:

- Twoje miejsce zamieszkania, pracy oraz miejsca, które najczęściej odwiedzasz,
- Informacje kontaktowe Twoich współpracowników, znajomych, rodziny i przyjaciół,
- Historia rozmów, zarówno przychodzących, wychodzących jak i nieodebranych,
- Wiadomości SMS, MMS oraz głosowe,
- Rozmowy prowadzone przez aplikacje takie jak szyfrowane komunikatory, gry czy serwisy społecznościowe,
- Położenie w oparciu o dane GPS lub stacji bazowych GSM,
- Historia przeglądanych stron, ciasteczka i zapamiętane strony internetowe,
- Osobiste zdjęcia, filmy, nagrania dźwiękowe i wiadomości email,
- Hasła wraz z danymi dostępowymi do kont w serwisach online takich jak bankowość elektroniczna czy skrzynka email,
- Zdjęcia, pliki i informacje trzymane w chmurze,
- Informacje dotyczące Twojego zdrowia, na przykład dieta, tętno czy ciśnienie krwi.

Skuteczne usuwanie danych z urządzenia

Jak można wywnioskować z listy powyżej, ma Twoim urządzeniu mobilnym jest bardzo wiele prywatnych, wrażliwych informacji.

Bezpieczne pozbywanie się urządzeń mobilnych

Nieważne czy oddajesz urządzenie komuś znajomemu, czy nawet członkowi rodziny, albo je odsprzedajesz czy oddajesz do utylizacji, powinieneś usunąć z niego te wszystkie informacje. Możesz nie być tego świadomy, ale zwyczajne usunięcie plików czy zdjęć nie jest wystarczające. Takie dane można łatwo odzyskać przy użyciu darmowych narzędzi dostępnych w Internecie. Zamiast tego należy dane usunąć bezpiecznie, co nazywa się z języka angielskiego “wiping” (od słowa “wipe” - wycierać, zmazywać, kasować). Zanim wymażesz dane ze swojego urządzenia pamiętaj o zrobieniu kopii danych, z której będziesz mógł przywrócić dane w nowym urządzeniu.

Kiedy pozbywasz się urządzenia mobilnego, pamiętaj aby wykonać przywrócenie do ustawień fabrycznych, usunąć kartę SIM oraz SD, jeśli Twoje urządzenie posiada takie karty.

Najłatwiejszą metodą bezpiecznego usunięcia danych jest użycie opcji przywracania do ustawień fabrycznych. To sprawi, że telefon będzie w takim samym stanie, w jakim go kupiłeś - przynajmniej pod względem danych na nim zamieszczonych. Jest to jedna z najbezpieczniejszych metod usuwania danych. Sposób wykonania tego kroku jest zależy od urządzenia, którego używasz. Poniżej znajdują się opisy dla dwóch najpopularniejszych typów urządzeń:

- Apple iOS: Ustawienia | Ogólne | Wyzeruj | Wymaż zawartość i ustawienia
- Android: Ustawienia | Kopie i kasowanie danych | Ustawienia fabryczne

Niestety, usuwanie danych osobistych z urządzeń z Windows Phone nie jest tak proste jak przywracanie ustawień fabrycznych. Wymagane jest głębsze sprawdzenie, czy osobiste dane zostały wymazane z urządzenia. Jeśli wciąż masz pytania dotyczące przywracania telefonu do ustawień fabrycznych sprawdź instrukcję użytkownika albo stronę internetową producenta. Pamiętaj, zwyczajne usunięcie danych w większości przypadków nie wystarcza.

Karty SIM i karty pamięci

Oprócz danych umieszczonych na urządzeniu, musisz też zwrócić uwagę na dane, które znajdują się na karcie SIM (z angielskiego Subscriber Identity Module). Karta SIM zawiera informacje, które służą do nawiązywania połączeń głosowych oraz połączeń danych. Kiedy przywracasz telefon do ustawień fabrycznych, żadne informacje nie są usuwane z karty SIM. Porozmawiaj ze sprzedawcą na temat przeniesienia danych z karty SIM do nowego telefonu. Jeśli nie ma takiej możliwości po prostu zniszcz kartę SIM w taki sposób, aby nikt inny nie mógł jej użyć.

Niektóre urządzenia trzymają również dane na osobnych kartach pamięci SD (z angielskiego Secure Digital). Te karty zawierają aplikacje, zdjęcia i inne prywatne dane. Pamiętaj, aby usunąć kartę SD z telefonu zanim się go pozbędziesz

Bezpieczne pozbywanie się urządzeń mobilnych

(czasami wymaga to zajrzenia pod baterię telefonu). Karty SD mogą zostać użyte ponownie z nowym urządzeniem, albo jako dodatkowy nośnik pamięci za pomocą specjalnej przejściówki na USB. Jeśli z jakiś powodów nie możesz ponownie użyć karty SD zalecamy jej zniszczenie, podobnie jak kartę SIM.

Jeśli nie jesteś pewny co do któregoś z opisanych tutaj kroków, zabierz telefon do serwisu, gdzie pomocy udzieli Ci profesjonalista. Na koniec, jeśli zamierzasz po prostu wyrzucić swój telefon do śmieci rozważ oddanie go jednej z organizacji charytatywnych, które akceptują używane telefony.

Dowiedz się więcej

Zasubskrybuj comiesięczny biuletyn o bezpieczeństwie komputerowym SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS dotyczące bezpieczeństwa komputerowego i osobowego.
Odwiedź securingthehuman.sans.org/ouch/archives i dowiedz się więcej.

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

Zabezpiecz swój nowy tablet:	https://securingthehuman.sans.org/ouch/2016#january2016
Backup i odzyskiwanie danych:	https://securingthehuman.sans.org/ouch/2015#august2015
Kurs Advanced Smartphone Forensics:	https://sans.org/for585
Archiwalne biuletyny OUCH:	https://securingthehuman.sans.org/ouch/archives

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Polski przekład (NASK/CERT Polska): Małgorzata Dębska, Przemysław Zielony, Sebastian Kondraszuk