OUCH! | czerwiec 2014

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM NUMERZE..

Pozbywanie się urządzeń mobilnych

Informacje ogólne

Urządzenia mobilne, jak smartfony czy tablety, wciąż rozwijają się w bardzo szybkim tempie. Wynikiem tego jest dosyć krótki okres życia tych urządzeń - większość z nas wymienia je co 18 miesięcy. Niestety dużo osób pozbywa się urządzeń mobilnych nie zważając na osobiste dane, które mogą znajdować się na tych urządzeniach. W tym biuletynie zwrócimy uwagę na dane, które mogą się znajdować na urządzeniach mobilnych i wskażemy jak bezpiecznie się ich 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 tutaj kroki.

Redaktor gościnny

Christopher Crowley (**@CCrowMontance**; **+ChrisCrowley**) jest konsultantem z Waszyngtonu. Jest również głownym instruktorem kursu Mobile Device Secutiry and Ethical Hacking (SEC575) i autorem kursu Incident Response Team Management (MGT535) organizowanych przez SANS Institute.

Twoje dane

Urządzenia mobilne przechowują bardzo dużo prywatnych danych, możliwe nawet, że więcej niż komputer. Przykłady takich danych są podane poniżej.

- Twoje miejsce zamieszkania, pracy oraz miejsca, które najczęsciej odwiedzasz.
- Informacje kontaktowe Twoich współpracowników, znajomych, rodziny i przyjaciół.
- Historia rozmów, zarówno przychodzących jak i wychodzących oraz nieodebranych.
- Wiadomośći SMS / MMS oraz głosowe.
- Rozmowy prowadzone przez aplikacje takie jak gry czy serwisy społecznościowe.
- Położenie w oparciu o dane GPS albo stacji bazowych GSM.
- Historia przeglądanych stron, ciasteczka czy zapamiętane strony internetowe.
- Osobiste zdjęcia, filmy, nagrania dźwiękowe czy 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, puls czy ciśnienie krwi.

Pozbywanie się urządzeń mobilnych

Usuwanie danych z urządzenia

Jak można wywnioskować z listy powyżej, na Twoim urządzeniu mobilnym jest bardzo wiele prywatnych, wrażliwych informacji. Nieważne czy oddajesz urządzenie komuś znajomemu, czy nawet członkowi rodziny, albo je odsprzedajesz czy oddajesz do utylizacji, powinieneś usunąć z niego wszystkie informacje. Powinieneś to zrobić także gdy oddajesz telefon do serwisu, aby wymienić go na nowy, albo po prostu do naprawy. Jeśli tego nie zrobisz, każdy, kto będzie miał dostęp do telefonu może uzyskać także dostęp do Twoich prywatnych danych. Pamiętaj także, aby przed usunięciem danych wykonać ich kopię. Po usunięciu będzie już za późno i nie będziesz mógł odzyskać zdjęć czy filmów.

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

Gdy już wykonałeś kopię danych, możesz je bezpiecznie usunąć. Zwyczajne usunięcie plików czy zdjęć nie jest wystarczające. Takie dane można łatwo odzyskać za pomocą darmowych narzędzi dostępnych w internecie. Zamiast tego należy dane usunąć bezpiecznie, co nazywa się z angielskiego “wiping” (od słowa “wipe” - wycierać, zmazywać, kasować). Najłatwiejszą metodą osiągnięcia tego 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 zależny od urządzenia, którego używasz. Poniżej znajdują się opisy dla trzech najpopularniejszych typów urządzeń.

- Apple iOS: Ustawienia | Ogólne | Wyzeruj | Wymaż zawartość i ustawienia
- Android: Ustawienia | Kopie i kasowanie danych | Ustawienia fabryczne
- Windows Phones: Ustawienia | Informacje | Zresetuj telefon

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 oraz 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 nawiązania połaczeń głosowych oraz połączeń danych. Kiedy przeprowadzasz przywrócenie telefonu 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.

Pozbywanie się urządzeń mobilnych

Niektóre urządzenia trzymają również dane na osobnych karta 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 (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 komórkowe.

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 http://www.securingthehuman.org 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

OUCH! Backup i przywracanie osobistych danych:
http://www.securingthehuman.org/ouch/2013#september2013
PC World “Jak przygotować sprzęt do sprzedaży”:
http://www.pcworld.pl/artykuly/393783/Jak.przygotowac.sprzet.do.sprzedazy.html

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak, Paweł Jacewicz, Łukasz Siewierski