Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu

Co robić kiedy stracisz smartfon lub tablet

REDAKTOR GOŚCINNY

Heather Mahalik jest redaktorką tego wydania. Jest certyfikowaną instruktorką SANS z Waszyngtonu i zajmuje się śledztwami w zakresie technologii mobilnych. Heather jest aktywna na Twitterze pod nickiem @heathermahalik.

WSTĘP

Urządzenia mobilne są używane do komunikacji oraz do uzyskiwania informacji. W rezultacie często zawierają poufne informacje, między innymi wiadomości e-mail, smsy, wiadomości poczty głosowej, kalendarze, informacje o lokalizacji, zdjęcia i filmy. Jeśli urządzenie zostanie zgubione lub skradzione, każdy kto ma do niego fizyczny dostęp, może potencjalnie uzyskać dostęp do wszystkich tych informacji i narazić Ciebie, osoby z Twoich kontaktów i Twojego pracodawcę na poważne ryzyko. W tym biuletynie omawiamy kroki jakie można podjąć, aby chronić informacje zapisane w urządzeniu w przypadku jego zagubienia lub kradzieży.

Uwaga: Większość z opisanych w biuletynie porad dotyczy urządzeń osobistych. Jeśli urządzenie mobilne zostało Ci udostępnione przez pracodawcę i zawiera wewnętrzne dane organizacji, upewnij się, aby postępować zgodnie z wewnętrzną polityką firmy dotyczącą zabezpieczania urządzeń mobilnych oraz zgłaszania ich utraty lub kradzieży.

ŚRODKI OSTROŻNOŚCI

Jednym z najbardziej skutecznych sposobów, w jaki można chronić swoje dane, jest zabezpieczenie urządzenia póki jeszcze jest się w jego posiadaniu. Najlepiej jest zacząć od aktywowania ochrony dostępu do urządzenia, takiej jak blokada PIN, hasło lub blokada ekranu oparta o wzór graficzny. Dzięki temu tylko autoryzowani użytkownicy mogą korzystać i mieć dostęp do informacji znajdujących się na urządzeniu.

- **PIN**: PIN (Personal Identification Number) to numer który należy wpisać aby uzyskać dostęp do urządzenia mobilnego.
- **Hasło**: Hasło na urządzeniach przenośnych działa tak samo, jak hasło w komputerze lub na dowolnym koncie internetowym. Każdorazowe pytanie o hasło to opcja jaką można włączyć na większości smartfonów. Silne hasło daje większe bezpieczeństwo niż zabezpieczenie kodem PIN.
- **Wzór graficzny blokujący ekran**: To niepowtarzalny wzór, który można narysować na ekranie aby odblokować dostęp do urządzenia.

Zdecydowanie warto rozważyć włączenie opcji całkowitego usunięcia wszystkich danych z urządzenia po określonej liczbie nieudanych prób uzyskania dostępu. To może ochronić urządzenie, jeśli wpadnie ono

Co robić kiedy stracisz smartfon lub tablet

w niepowołane ręce. Jednak włączając tę funkcję należy uważać na ciekawskie dzieci. Niezależnie od używanego mechanizmu uwierzytelniania, upewnij się, że nie ujawniłeś swojego kodu PIN, hasła lub wzoru blokady nikomu i że jest ono trudne do odgadnięcia.

- **Zdalny Tracking & Kasowanie:** Większość urządzeń mobilnych wspiera oprogramowanie, które może zdalnie zlokalizować i/lub zdalnie wykasować dane z utraconego urządzenia. Najprawdopodobniej konieczne będzie zainstalowanie i skonfigurowanie specjalnie do tego przeznaczonego oprogramowania, kiedy jeszcze posiadamy urządzenie. iPhone i iPad posiadają tę funkcję pod nazwą "Find My iPhone" i włącza się ją przy użyciu Apple ID. Urządzenia BlackBerry muszą być powiązane z serwerem BES (BlackBerry Enterprise Server) lub podobnym rozwiązaniem aby zostać zdanie wyczyszczone. Urządzenia z systemem Android muszą mieć zainstalowane specjalne oprogramowanie do zdalnego lokalizowania i czyszczenia urządzenia.
- **Szyfrowanie:** Jeśli ktoś ma fizyczny dostęp do urządzenia mobilnego, może skorzystać z zaawansowanych rozwiązań i próbować pominąć hasło lub kod PIN, aby uzyskać dostęp do przechowywanych danych. Szyfrowanie chroni dane przed bardziej zaawansowanymi typami ataków. Niektóre urządzenia przenośne posiadają wbudowane szyfrowanie, podczas gdy inne wymagają włączenia takiej funkcji lub zainstalowania oprogramowania szyfrującego. iPhone i iPad zapewniają wbudowane szyfrowanie sprzętowe, które jest domyślnie włączone. Tym sposobem bez użycia hasła, dane są chronione. Android ma wbudowane szyfrowanie, które może być aktywowane w menu Ustawienia -> Osobiste -> Zabezpieczenia -> Szyfrowanie -> Zaszyfruj telefon.
- **Kopia zapasowa (backup)**: Backup pozwala szybko odzyskać informacje, które znajdowały się na zgubionym lub skradzionym urządzeniu. Kopie zapasowe powinny być wykonywane regularnie i mogą zostać wykonane przy użyciu jednej z następujących metod:
  - Archiwizacja bezpośrednio na komputerze.
  - Cloud jest dostępny jako bezpłatna usługa dla wszystkich użytkowników iPhone'ów, iPad'ów i iPod'ów. Użytkownik może wykonać kopię zapasową swoich kontaktów, wiadomości e-mail, kalendarza, zdjęć, muzyki i innych plików przesyłając ją jednocześnie na konto iCloud.
  - Google Cloud to bezpłatna usługa tworzenia kopii zapasowych dla urządzeń z systemem Android. Funkcje Google Cloud są podobne do iCloud.

Podejmując kilka prostych kroków możesz skutecznie ochronić się na wypadek utraty swojego smartfona lub tabletu.

Co robić kiedy stracisz smartfon lub tablet

CO ROBIĆ W WYPADKU UTRATY URZĄDZENIA MOBILNEGO

Wykonaj te kroki, aby chronić dane osobowe w przypadku, jeśli urządzenie zostanie zgubione lub skradzione.

- Jeśli urządzenie zostało wydane przez pracodawcę lub zawiera dane związane z pracą, natychmiast zgłoś utratę urządzenia do działu help desk lub zespołu bezpieczeństwa w Twojej organizacji i postępuj zgodnie z ich instrukcjami.
- Jeśli uprzednio zainstalowano oprogramowanie do śledzenia na urządzeniu przenośnym, najprawdopodobniej istnieje możliwość zdalnego kasowania danych. Wyczyszczenie urządzenia spowoduje skasowanie z niego wszystkich informacji osobistych i wyeliminowania ryzyka dostępu do danych. Jeśli urządzenie zostało skradzione, możesz skontaktować się z policją przed zdalnym kasowaniem danych i powiadomić ich, że masz włączone śledzenie lokalizacji urządzenia. Jeśli urządzenie zostało skradzione, nie należy próbować odzyskiwać go samodzielnie.
- Skontaktuj się z dostawcą sieci lub usługi telefonicznej w celu ostrzeżenia ich, że Twój telefon komórkowy został zgubiony lub skradziony. Dostawcy mogą być w stanie wprowadzić blokadę na numer telefonu zapewniając że nikt nie może używać urządzenia do prowadzenia rozmów telefonicznych, do czasu aż zostanie ono wymienione
- Po zakupie zastępczego urządzenia można użyć kopii zapasowych, aby odzyskać swoje dane.

ŹRÓDŁA

W celu poprawy czytelności tekstu niektóre odnośniki w biuletynie zostały skrócone przy użyciu usługi TinyURL. Dla zachowania bezpieczeństwa, OUCH! używa funkcji podglądu TinyURL, która pozwala podejrzeć docelowy adres odnośnika oraz pyta o pozwolenie przed wejściem na stronę o docelowym adresie.

20 aplikacji bezpieczeństwa dla Androida:
http://preview.tinyurl.com/27qbb6w

10 aplikacji bezpieczeństwa dla iOS:
http://preview.tinyurl.com/bumb8vv

Google Cloud:
http://preview.tinyurl.com/cy49ntb

iCloud:
https://www.icloud.com/#find

Słownik pojęć bezpieczeństwa (j.ang):
http://preview.tinyurl.com/6wkpae5

Porada dnia SANS Security (j.ang):
http://preview.tinyurl.com/6s2wrkp

DOWIEDZ SIĘ WIĘCEJ

Zasubskrybuj comiesięczny Biuletyn Bezpieczeństwa Komputerowego – SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS z zakresu 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

Redakcja: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak, Paweł Jacewicz