OUCH! | Styczeń 2016

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM WYDANIU..

- **Jak zabezpieczyć swój tablet**
- **Bezpieczny tablet na dłużej**

Zabezpiecz swój nowy tablet

Wstęp

Gratulujemy zakupu nowego tabletu! Jest to potężne i wygodne narzędzie, które może być wykorzystane do komunikacji, robienia zakupów w sieci, oglądania filmów, grania oraz całej masy innych aktywności. Tablet może stać się bardzo ważną częścią Twojej codzienności, a możliwe, że nawet zastąpi Twój komputer. W tym wydaniu OUCH! przedstawiamy kroki, które w pełni pomogą zabezpieczyć urządzenie oraz przechowywane na nim informacje.

Redaktor gościnny

Lori Rosenberg ma duże doświadczenie w tworzeniu materiałów edukacyjnych dotyczących bezpieczeństwa komputerowego dla klientów oraz pracowników przedsiębiorstw. Pasjonuje się poszukiwaniem nowych metod przekazywania wiedzy. Możesz znaleźć ją na Twiterze jako **@InfoSecLori**.

Jak zabezpieczyć swój tablet

Może być to dla Ciebie zaskoczeniem, ale największym zagrożeniem dla Twojego tabletu nie są hakerzy, ale Ty sam. Dużo bardziej prawdopodobne jest to, że zgubisz swój tablet, zapomnisz o nim, lub że zostanie Ci skradziony i potem ktoś się do niego włamie. Pierwszym i podstawowym zabezpieczeniem jakie powinno być włączone jest automatyczna blokada ekranu, którą można odblokować np. za pomocą silnego hasła, złożonego symbolu lub używając odcisku palca. Zapewni to, że w przypadku gdy Twój tablet zostanie skradziony lub zgubiony, nikt nie będzie mógł w prosty sposób dostać się do Twoich danych. Chronisz tym samym swoje prywatne pliki, aplikacje mobilne i wszystko inne co na nim masz. Gdy już włączysz automatyczną blokadę ekranu, postaraj się też wdrożyć pozostałe wskazówki, które prezentujemy poniżej:

1. Zainstaluj lub aktywuj oprogramowanie do zdalnego śledzenia Twojego tabletu przez Internet. W przypadku, gdy zgubisz swój tablet lub jeśli zostanie Ci on skradziony, taka funkcja najprawdopodobniej pomoże Ci go odnaleźć lub, w najgorszym wypadku, zdalnie skasować wszystkie Twoje prywatne dane.
2. Włącz automatyczne aktualizacje na swoim tablecie, lub jeśli nie jest to możliwe, aktualizuj go ręcznie do najnowszej wersji systemu operacyjnego i oprogramowania. Przestępcy ciągle szukają nowych dziur w oprogramowaniu, a jego twórcy ciągle je łatają i wypuszczają aktualizacje. Mając najnowsze wersje systemu i oprogramowania znacząco utrudniasz przestępcom możliwość włamania się.
3. Zwracaj szczególną uwagę na opcje prywatności, które są możliwe do skonfigurowania na Twoim tablecie, a zwłaszcza takie,

Zabezpiecz swój nowy tablet

które dotyczą śledzenia Twojej lokalizacji. Zalecamy, aby wyłączyć możliwość śledzenia Twojej lokalizacji we wszystkich aplikacjach, a później selektywnie włączać ją tylko w tych, które naprawdę tego potrzebują, jak np. mapy. Większość aplikacji nie potrzebuje mieć ciągłego dostępu do informacji o Twoim położeniu i dla nich taka opcja powinna być wyłączona.

4. Większość tabletów i aplikacji na nich zainstalowanych przechowuje swoje dane w chmurze. W takim wypadku, upewnij się, że wiesz gdzie dokładnie znajdują się Twoje pliki i jak są zabezpieczone. Ostatnią rzeczą jaką chcesz jest to, aby cały świat zobaczył Twoje prywatne zdjęcia wraz z lokalizacją gdzie były zrobione. Najlepiej będzie, jeśli zupełnie wyłączysz opcje automatycznego udostępniania jakichkolwiek danych do chmury, a następnie będziesz z tej możliwości korzystać tylko wtedy, gdy na pewno będziesz chcieć coś do niej wysłać.

Najlepszą metodą na zabezpieczenie tabletu jest włączenie blokady ekranu, sprawdzenie ustawień prywatności i częste aktualizacje oprogramowania.

5. Aplikacje zainstalowane na tabletach, np. przeglądarki internetowe bardzo często umożliwiają synchronizację danych pomiędzy innymi urządzeniami z których korzystasz, np. komputerami czy smartfonem. Jest to bardzo przydatna funkcja, ale może nieść za sobą pewne zagrożenie. Upewnij się, że wiesz, które aplikacje używają takich funkcji i nie daj się zaskoczyć sytuacją, gdy odwiedzone przez Ciebie strony na tablecie pojawią się w historii przeglądanych stron na komputerze w pracy.

Bezpieczny tablet na dłużej

Gdy już zabezpieczyłeś swój tablet, na pewno chciałbyś, aby taki pozostał na dłużej. Poniżej znajdziesz kilka kluczowych porad jak tego dokonać:

- Nigdy nie wykonuj jailbreaku (z ang. zdjęcie zabezpieczeń twórcy sprzętu) swoich urządzeń. Spowoduje to usunięcie lub ominięcie specjalnych zabezpieczeń i może znacząco ułatwić włamanie przestępcom na urządzenie.
- Ściągaj i instaluj aplikacje tylko z zaufanych źródeł. Dla iPadów, pobieraj aplikacje z oficjalnego sklepu Apple - są one sprawdzane przez Apple zanim staną się dostępne dla użytkowników. Dla tabletów z Androidem używaj tylko sklepów Google Play lub Amazon. Aplikacje dostępne w pozostałych sklepach często nie są w żaden sposób sprawdzane i mogą być zainfekowane wirusami. Pamiętaj, że jeśli nie używasz jakiejś aplikacji i nie jest Ci ona dłużej potrzebna, to najlepiej ją odinstalować.

Zabezpiecz swój nowy tablet

- Gdy instalujesz nową aplikację, zweryfikuj ustawienia prywatności, które są w niej dostępne - podobnie jak miało to miejsce w czasie wcześniejszej konfiguracji tabletu. Uważaj na co pozwalasz instalowanemu programowi. Np. czy aplikacja naprawdę musi mieć dostęp do całej listy Twoich znajomych wraz z informacjami kontaktowymi? Jeśli czujesz się niepewnie w stosunku do uprawnień jakich żąda, postaraj się znaleźć inną. Dodatkowo, regularnie sprawdzaj uprawnienia nadawane aplikacjom i upewnij się, że nie uległy zmianie.

Twój tablet to potężne narzędzie - takie z którego powinieneś się cieszyć i korzystać z przyjemnością. Zapamiętanie tych kilku prostych wskazówek pozwoli Ci zabezpieczyć na długo zarówno siebie jak i tablet.

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

Źródła

Bezpieczne aplikacje mobilne:	https://www.securingthehuman.org/ouch/2015#january2015
Nowe oblicze hasła:	https://www.securingthehuman.org/ouch/2015#april2015
Bezpieczne korzystanie z chmury:	https://www.securingthehuman.org/ouch/2014#september2014
Pozbywanie się urządzeń mobilnych:	https://www.securingthehuman.org/ouch/2014#june2014
Wskazówka dnia od SANS Security (w j. ang.):	https://www.securingthehuman.org/resources/security-terms

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