OUCH! | Grudzień 2013

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM NUMERZE..

- Jak zabezpieczyć tablet
- Co zrobić żeby tablet pozostał bezpieczny na dłużej

Zabezpiecz swój nowy tablet

Twój nowy tablet

Gratulacje, kupiłeś nowy tablet! Ta technologia jest potężnym i wygodnym sposobem komunikowania się z innymi, robienia zakupów online, czytania, słuchania muzyki, grania i wykonywania mnóstwa innych czynności. Ponieważ to nowe urządzenie może stać się tak ważną częścią codziennego życia, gorąco zachęcamy do podjęcia kilku prostych kroków, aby było ono właściwie zabezpieczone.

Redaktor gościnny

Chad Tilbury jest redaktorem gościnnym tego wydania. Posiada bogate doświadczenie w prowadzeniu śledztw związanych z przestępczością komputerową i jest współautorem kursów FOR408 (Windows Forensics) i FOR508 (Advanced Forensics and Incident Response) w SANS Institute. Można go znaleźć na Twitterze jako **@chadtilbury**, lub na jego blogu **http://forensicmethods.com**.

Jak zabezpieczyć tablet

Pierwszym krokiem jest ustawienie hasła dostępu lub innego mechanizmu blokującego ekran. Tablet z łatwością można wszędzie ze sobą zabrać, ale to też oznacza, że równie łatwo można go zgubić lub stracić w wyniku kradzieży. Aby zapobiec dostaniu się Twoich danych w niepowołane ręce upewnij się, że ekran tabletu jest blokowany trudnym do odgadnięcia numerem PIN, hasłem, lub wzorem graficznym. W nowszych urządzeniach można znaleźć niektóre rodzaje uwierzytelniania biometrycznego, np. czytnik linii papilarnych. Użyj najsilniejszej metody blokady jaką obsługuje Twój tablet i pamiętaj aby ustawić tablet tak, aby ekran blokował się automatycznie po krótkim czasie bezczynności.

W kolejnym kroku należy zaktualizować system operacyjny tabletu do najnowszej wersji. Działający w internecie przestępcy ciągle wynajdują nowe słabe punkty w oprogramowaniu, a sprzedawcy oprogramowania wydają aktualizacje i poprawki, aby je naprawić. Korzystając z najnowszego systemu operacyjnego, możesz skutecznie utrudnić komuś włamanie się do tabletu.

Bardzo dokładnie skonfiguruj swój tablet po raz pierwszy. Najważniejsze opcje konfiguracyjne to opcje prywatności i opcje korzystania z chmury. Opcje prywatności dotyczą ochrony Twoich danych osobowych. Jednym z największych problemów związanych z ochroną prywatności w tablecie jest jego zdolność do poznania i śledzenia lokalizacji. Zalecamy przejście do funkcji ochrony prywatności i zupełne wyłączenie śledzenia lokalizacji, a następnie jej włączenie tylko dla wybranych aplikacji. Dla działania niektórych aplikacji śledzenie położenia jest kluczowe (np. mapy lub wyszukiwarka restauracji w pobliżu), ale większość aplikacji nie potrzebuje informacji o lokalizacji w czasie rzeczywistym.

Zabezpiecz swój nowy tablet

Najlepszym sposobem aby zabezpieczyć tablet jest stosowanie blokady ekranu, posiadanie najnowszej wersji systemu operacyjnego oraz świadomość opcji prywatności i opcji danych w chmurze.

Innym ważnym aspektem konfiguracji są kwestie przechowywania danych w chmurze. Usługi w chmurze, takie jak Apple iCloud, Microsoft SkyDrive, Dropbox czy Google Drive pozwalają na przechowywanie danych na swoich serwerach. Większość tabletów ma wbudowane opcje automatycznego zapisywania danych w chmurze, w tym dokumentów, zdjęć i filmów. Pomyśl o tym jak wrażliwe są Twoje dane i sam zdecyduj, czy należy je przechowywać w chmurze. Upewnij się, że wiesz, jak te dane będą chronione (np. hasłem) oraz w jaki sposób można kontrolować kto będzie miał do nich dostęp. Z pewnością ostatnią rzeczą o jakiej marzysz to Twoje świeżo zrobione prywatne zdjęcia zamieszczone w Internecie wraz z dokładną informacją o geolokalizacji, a wszystko to bez Twojej wiedzy.

Bądź świadomy tego, że tablety coraz częściej synchronizują dane z Twoich aplikacji z innymi urządzeniami, takimi jak smartfony czy laptopy. Jest to popularne wśród wielu aplikacji, takich jak Google Chrome, w Windows 8, i jest jedną z najczęściej używanych funkcji iCloud. Synchronizacja urządzenia może być świetną cechą, ale kiedy ją włączysz nie należy się dziwić, że strony które odwiedziłeś i Twoje zakładki, które stworzyłeś na tablecie pojawią się w Twojej przeglądarce w pracy.

Co zrobić żeby tablet pozostał bezpieczny na dłużej

Kiedy Twój tablet będzie już zabezpieczony, chcesz mieć pewność, że takim zostanie. Oto kilka prostych kroków, których wykonywanie warto rozważyć, podczas późniejszego korzystania z tabletu.

- Utrzymuj zawsze zaktualizowane do najnowszej wersji system operacyjny oraz wszystkie aplikacje. Wiele tabletów automatycznie aktualizuje zainstalowane aplikacje, zachęcamy aby włączyć tę funkcję.
- Nie rób jailbreaku ani nie hakuj swojego tabletu. To może spowodować ominięcie i uczynienie bezużytecznymi wszystkich punktów kontroli bezpieczeństwa oraz sprawi, że Twój tablet będzie znacznie bardziej narażony na ataki.
- Pobieraj tylko aplikacje, których naprawdę potrzebujesz i które pochodzą z zaufanych źródeł. Dla iPadów jest to bardzo proste, gdyż można je pobrać wyłącznie z iTunes. Te aplikacje są sprawdzane przez Apple zanim staną się dostępne dla użytkowników. W przypadku Google zalecamy ograniczyć źródła pobierania aplikacji tylko do Google Play. Mimo że jest możliwe

Zabezpiecz swój nowy tablet

pobranie aplikacji z innych stron, nie są one zazwyczaj odpowiednio weryfikowane i mogą zawierać złośliwą zawartość. Wreszcie, niezależnie od tego skąd masz swoją aplikację, kiedy nie jest Ci już potrzebna lub nie korzystasz z niej aktywnie zalecamy usunąć ją z tabletu.

- Po zainstalowaniu nowej aplikacji, upewnij się, że przejrzałeś i ustawiłeś dla niej opcje prywatności, tak jak przy początkowej konfiguracji nowego tabletu. Uważaj na to do jakich informacji dajesz dostęp aplikacji i co pozwalasz jej z nimi zrobić. Na przykład: czy właśnie pobrana aplikacja naprawdę potrzebuje dostępu do wszystkich kontaktów aby spełniać swoje funkcje?
- Upewnij się że masz zainstalowane i skonfigurowane oprogramowanie pozwalające zdalnie śledzić, zablokować lub usunąć wszystkie dane z tabletu w przypadku kiedy został on zgubiony lub skradziony.

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

Synchronizacja Chrome:
http://www.techrepublic.com/blog/google-in-the-enterprise/chrome-sync-configure-once-work-everywhere/
8 powodów dla których możesz obawiać się przechowywania danych w chmurze:
http://www.businessnewsdaily.com/5215-dangers-cloud-computing.html
Słownik pojęcia bezpieczeństwa SANS :
http://www.securingthehuman.org/resources/security-terms
Porada dnia SANS Security:
https://www.sans.org/tip_of_the_day.php

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