OUCH! | Sierpień 2014

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM NUMERZE..

Szyfrowanie

Czym jest szyfrowanie?

Mogłeś już wcześniej słyszeć słowo “szyfrowanie” i o tym, że powinieneś go używać do ochrony siebie i swoich informacji. Jednakże, pojęcie samo w sobie może czasami być niejasne lub mylące. W dodatku szyfrowania nie należy traktować jako remedium na wszystkie zagrożenia, ponieważ jego zastosowanie też ma swoje ograniczenia. W tym wydaniu biuletynu postaramy się wyjaśnić w prostych słowach czym jest szyfrowanie, dlaczego powinieneś go używać oraz w jaki sposób należy je poprawnie stosować.

Redaktor gościnny

Christopher Crowley (**@CCrowMontance**; **+ChrisCrowley**) jest konsultantem i na co dzień pracuje w mieście Washington D.C. Jest jednym z czołowych instruktorów kursu Instytutu SANS dotyczącego bezpieczeństwa urządzeń przenośnych oraz etycznego hackingu (SEC575) oraz autorem kursu poświęconego zarządzaniu zespołem reakcji na incydenty (MGT535).

Twoje urządzenia przechowują olbrzymią ilość wrażliwych informacji, takich jak dokumenty finansowe, zdjęcia, adresy email czy nawet dane medyczne. Gdybyś zgubił jedno z takich urządzeń lub zostałoby ono skradzione, wtedy do wszystkich tych danych ktoś mógłby uzyskać dostęp. Z całą pewnością też korzystasz z bankowości online lub robisz zakupy przez Internet. Gdybyś stał się celem przestępcy internetowego, który monitorowałby Twoją aktywność w sieci, mógłby on wykraść informacje o numerach Twoich kart kredytowych lub uzyskać dostęp do konta bankowego. Szyfrowanie pomaga chronić Cię w takich sytuacjach zapewniając, że nieupoważnione osoby nie mogą zdobyć ani zmodyfikować Twoich danych.

Informacja, która nie jest zaszyfrowana jest określana jako “czysty tekst” (ang. plaintext). Oznacza to, że każdy może w prosty sposób ją odczytać. Szyfrowanie zmienia ją do postaci nieczytelnej zwanej szyfrogramem (ang. ciphertext). Operacja szyfrowania używa skomplikowanych operacji matematycznych oraz unikatowego klucza w celu zamiany informacji z postaci czytelnej dla każdego do postaci zaszyfrowanej. Unikatowy klucz działa podobnie jak klucz do zamka w drzwiach - tylko on daje dostęp do oryginalnej informacji. Przykładem takiego klucza jest hasło. Tylko posiadacz hasła może odszyfrować dane i je odczytać. Aby chronić zaszyfrowane dane musisz chronić swój klucz.
Szyfrowanie może być stosowane głównie w dwóch przypadkach: do zabezpieczania danych na dyskach twardych (np. pliki) oraz do zabezpieczania danych przesyłanych w sieci (np. transakcje bankowe).

Szyfrowanie plików

Podstawowym celem szyfrowania plików jest zabezpieczenie informacji przed niepowołanym dostępem, najczęściej w przypadku gdy urządzenie na którym są zapisane zostanie skradzione lub zagubione (np. smartfon). Kilkanaście lat temu nie było potrzeby, aby używać szyfrowania w tym celu, gdyż większość komputerów była czasami zbyt duża żeby nawet je przenieść. Dziś przeciętny laptop waży 2-3 kg, a smartfon zwykle nie więcej niż 200g. Przechowują one ogromne

Szyfrowanie

ilości prywatnych danych, a ze względu na małe wymiary można je łatwo stracić. Jeśli prywatne dane są zapisywane na przenośnych pamięciach, takich jak pendrive'y czy dyski CD, one także powinny być zabezpieczone. Najpopularniejszą techniką szyfrowania jest wykonanie pełnego szyfrowania dysku (z ang. FDE). Oznacza to, że wszystko co jest zapisywane na tak zabezpieczonym urządzeniu jest automatycznie szyfrowane i użytkownik nie musi się martwić co szyfrować a co nie. Większość najnowszych systemów operacyjnych dostarcza takich mechanizmów i jedyne co musi zrobić użytkownik to włączenie odpowiedniej opcji. Na przykład w systemie Mac OS X pełne szyfrowanie dysku nazywa się FileVault, a w niektórych wersjach systemu Windows odpowiada za to Bitlocker. Jeśli masz możliwość uruchomienia takiej funkcji, zalecamy abyś to zrobił. Także większość smartfonów może wykorzystywać taką funkcjonalność. Na przykład w urządzeniach przenośnych marki Apple jest ona uruchamiana automatycznie gdy użytkownik ustawi hasło dostępu do urządzenia. Sprawdź czy Twój sprzęt wspiera FDE. W przypadku urządzeń służbowych zapytaj wsparcia technicznego Twojej firmy, a w przypadku prywatnego sprzętu skontaktuj się z producentem lub sprawdź w dokumentacji.

Szyfrowanie to potężne narzędzie do ochrony Twoich informacji, ale jest tylko tak silne jak klucz, którego użyjesz.

Szyfrowanie komunikacji

Dane są także zagrożone w momencie ich transmisji przez sieć i mogą zostać przechwycone jeśli nie są zaszyfrowane. Z tego powodu musisz zapewnić, że cała wrażliwa komunikacja internetowa, taka jak bankowość online, poczta elektroniczna, czy nawet dostęp do portali społecznościowych odbywa się z wykorzystaniem szyfrowania. Najpopularniejszym typem szyfrowania online jest wykorzystanie protokołu HTTPS. Jego użycie gwarantuje, że cała komunikacja pomiędzy Twoją przeglądarką internetową a serwerem WWW jest szyfrowana. Różne przeglądarki w różny sposób informują o użyciu HTTPS i szyfrowania: jawnie poprzez oznaczenie protokołu w adresie internetowym strony WWW (szukaj ciągu https:// na samym początku adresu), poprzez znak kłódki lub oznaczenie paska adresu na zielono. W zależności od przeglądarki, może się zdarzyć, że zobaczysz wszystkie z wymienionych oznaczeń. Dodatkowo, za każdym razem gdy logujesz się do publicznej sieci WiFi koniecznie używaj szyfrowania komunikacji. Podobnie w przypadku używania poczty elektronicznej upewnij się, że Twój klient pocztowy używa szyfrowania gdy wysyła lub odbiera pocztę. Sprawdź dokumentację swojego programu pocztowego lub zadzwoń do dostawcy usługi email i dowiedz się jak włączyć taką opcję na swoim koncie.

Prawidłowe używanie szyfrowania

Szyfrowanie może być wykorzystane do wielu celów, ale w każdym użyciu należy pamiętać o pewnym wspólnym zbiorze zaleceń, który pomoże prawidłowo je zastosować:

Szyfrowanie

- Siła szyfrowania w dużej mierze zależy od siły Twojego klucza. Jeśli komuś uda się go odgadnąć lub wykraść, uzyska tym dostęp do Twoich danych. Musisz chronić swój klucz!
- Jeśli Twój klucz to hasło, upewnij się, że jest mocne i wystarczająco długie. Przechowuj je w bezpiecznym miejscu, gdyż jeśli je zgubisz to utracisz bezpowrotnie dostęp do swoich danych.
- Zabezpieczenie danych w postaci szyfrowania działa tylko jeśli Twoje urządzenie nie jest zainfekowane złośliwym oprogramowaniem. Musisz zadbać o bezpieczeństwo komputera i urządzeń przenośnych poprzez częste aktualizacje i instalację oprogramowania antywirusowego.
- Jeśli masz kilka opcji do wyboru w momencie gdy masz zamiar uruchomić szyfrowanie, zawsze wybierz najmocniejszą z nich. Jeśli nie wiesz, którą powinieneś wybrać, poproś o pomoc specjalistę.

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

Mac OS X Filevault:	http://support.apple.com/kb/HT4790?viewlocale=pl_PL
Szyfrowanie w Apple iOS:	http://support.apple.com/kb/HT4175?viewlocale=pl_PL
Szyfrowanie w Androidzie:	https://support.google.com/nexus/answer/2844831?hl=pl
Windows Encryption:	http://windows.microsoft.com/pl-pl/windows/protect-files-bitlocker-drive-encryption
Bezpieczny komputer w 7 krokach:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201212_po.pdf
Systemy zarządzania hasłami:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201310_po.pdf

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

