OUCH! | Czerwiec 2016

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu..

- Czym jest szyfrowanie?
- Co możesz zaszyfrować?
- Dobre praktyki i zalecenia

Szyfrowanie

Czym jest szyfrowanie?

Mogłeś już wcześniej słyszeć słowo “szyfrowanie” i to, 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

Redaktorem gościnnym tego numeru jest Francesca Bosco (**@francibosco**). Zawodowo jest badaczem i kierownikiem projektów. Zarządza głównie projektami związanymi z cyberprzestępczością cyberbezpieczeństwem i niewłaściwym używaniem technologii. Pracuje w United Nations Interregional Crime and Justice Research Institute i jest założycielem Centrum Techniki i Prawa.

Na pewno posiadasz ogromne ilości poufnych danych, takich jak dokumenty osobiste, zdjęcia czy e-maile, zapisane na różnych nośnikach. 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.

Szyfrowanie towarzyszy nam już od tysięcy lat. Dziś, proces szyfrowania jest dużo bardziej wyrafinowany jednak w rzeczywistości ma ten sam cel - przesłanie sekretnej wiadomości z jednego miejsca w drugie, gwarantując, że tylko uprawniona osoba będzie w stanie ją przeczytać. 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). Współcześnie, operacja szyfrowania używa skomplikowanych działań matematycznych oraz unikatowego klucza w celu zamiany informacji z postaci czytelnej dla każdego do postaci zaszyfrowanej. Tylko przy pomocy tego klucza będziesz w stanie zaszyfrować/odszyfrować informację. W większości przypadków ten klucz jest zwykłym hasłem alfanumerycznym.

Co możesz zaszyfrować?

Generalnie istnieją dwa rodzaje danych, które można zaszyfrować - dane w spoczynku (te przechowywane na dysku lub urządzeniu przenośnym) i dane w ruchu (pobierane wiadomości e-mail czy dane z komunikatorów).

Szyfrowanie

Szyfrowanie danych na nośnikach pamięci jest niezbędne w przypadku gdy komputer lub urządzenie mobilne zostanie skradzione lub zgubione. Obecnie, urządzenia są niesamowicie szybkie i wydajne a tym samym przechowują ogromne ilości informacji, która może zostać skradzione. Także inne urządzenia mogą zawierać wrażliwe dane - pendrive'y, dyski CD oraz inne zewnętrzne nośniki. 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 włączyć odpowiednią opcję. Na przykład w systemie Mac OS X pełne szyfrowanie dysku nazywa się FileVault, a w niektórych wersjach systemu Windows odpowiada za to Bitlocker lub Device Encryption. Aktualnie większość smartfonów wspiera FDE. Na przykład w urządzeniach przenośnych marki Apple jest ono uruchamiania automatycznie gdy użytkownik ustawi hasło dostępu do urządzenia. Począwszy od Androida w wersji 6.0 (Marshmallow), Google wymaga od użytkownika włączenia FDE zawsze gdy tylko sprzęt spełnia minimalne standardy.

Szyfrowanie to doskonałe narzędzie ochrony danych. Jednak jego efektywność mocno zależy od siły naszych kluczy.

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. Innym przykładem jest wysyłanie i otrzymywanie emaili. Większość klientów poczty pozwala na szyfrowanie które możesz włączyć. Kolejnym przykładem jest szyfrowanie danych które są wymieniane poprzez komunikatory, takie jak iMessage, Wickr, Signal, WhatsApp czy Telegram. Aplikacje tego typu używają szyfrowania typu end-to-end, które uniemożliwia osobom trzecim dostęp do konwersacji. Oznacza to tyle, że tylko ty i osoba z którą czatujesz może przeczytać wiadomości.

Dobre praktyki i zalecenia:

Aby być pewnym, że dobrze używasz szyfrowania, musisz to robić poprawnie.

- Twój szyfr jest tak silny, jak Twój klucz. Jeśli klucz zostanie skompromitowany, to samo stanie się z Twoimi danymi.

Szyfrowanie

Jeśli używasz haseł do ochrony Twoich kluczy, upewnij się, że są to silne hasła i że są dobrze chronione. Im dłuższego hasła używasz, tym trudniej dla atakującego będzie je zgadnąć lub złamać. Nie zapomnij swojego hasła, bez niego klucz nie będzie w stanie odszyfrować informacji. Jeżeli masz trudności z zapamiętywaniem haseł, użyj specjalnego menadżera do ich przechowywania.

- Twój szyf jest tak silny jak zabezpieczenia Twojego komputera. Jeśli Twój komputer jest zainfekowany, intruzi mogą skompromitować Twój szyfr. Dlatego tak ważne jest aby dobrze chronić swoje urządzenia. Używaj oprogramowania antywirusowego, silnych haseł i nie zapominaj o aktualizacjach systemu.
- Wiele aplikacji mobilnych i programów komputerowych oferuje szyfrowanie aby chronić Twoje dane i komunikację. Jeżeli aplikacja której zamierzasz użyć nie wspiera szyfrowania, zastanów się nad jakąś alternatywą.

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 securingthehuman.sans.org/ouch/archives 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

Więcej o szyfrowaniu:	http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/
Nowe oblicze hasła:	https://securingthehuman.sans.org/ouch/2015#april2015
Menadżery haseł:	https://securingthehuman.sans.org/ouch/2015#october2015
Czym jest złośliwe oprogramowanie:	https://securingthehuman.sans.org/ouch/2016#march2016
Zabezpiecz swój nowy tablet:	https://securingthehuman.sans.org/ouch/2016#january2016

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

