OUCH! | Wrzesień 2015

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM WYDANIU..

- **Wstęp**
- **Hasła**
- **Dwuskładnikowe uwierzytelnianie**

Dwuskładnikowe uwierzytelnianie

Wstęp

Głównym procesem, który służy ochronie Twoich informacji jest uwierzytelnienie - udowodnienie, że jesteś tym za kogo się podajesz. Im pewniejsza metoda uwierzytelnienia tym trudniej jest dostać się do Twoich informacji, takich jak wiadomości email, zdjęcia czy konta bankowe. Istnieją trzy sposoby potwierdzenia Twojej tożsamości: coś co znasz - np. hasło, coś co masz - jak na przykład prawo jazdy, coś czym jesteś - np. odcisk palca. Każda z nich ma swoje mocne i słabe strony. Najpopularniejszą metodą uwierzytelniania są hasła, czyli coś, co wiesz. W tym wydaniu nauczymy Cię używać dwuskładnikowego uwierzytelnienia, które jest dużo skuteczniejsze niż same hasła, a wciąż dosyć łatwe w użyciu. Aby lepiej zrozumieć dwuskładnikowe uwierzytelnianie przyjrzyjmy się najpierw hasłom.

Redaktor gościnny

Keith Palmgren ma ponad 30 lat doświadczenia w bezpieczeństwie informacji. Jest cetryfikowanym instruktorem SANS Institute, autorem kursu SANS SEC301 - pięciodniowego wprowadzenia do bezpieczeństwa informacyjnego. Kiedy nie zajmuje się nauczaniem, poświęca swój czas na konsultacje i tworzenie projektów związanych z bezpieczeństwem. Możesz zasubskrybować Kietha na Twitterze pod nickiem **@kpalmgren**.

Hasła

Hasła służą udowodnieniu, że jesteś tym za kogo się podajesz, bo znasz jakiś sekret. Niebezpieczeństwem związanym z hasłami jest fakt, że są jedynym zabezpieczeniem przed nieautoryzowanym dostępem. Jeśli ktoś jest w stanie zgadnąć bądź zdobyć Twoje hasło, uzyskuje dostęp do wszystkich informacji nim chronionych. Dlatego właśnie uczy się nas, że hasła powinny być mocne, trudne do zgadnięcia, unikatowe i nigdy nie udostępniane innym. Mimo, że te wszystkie porady są wciąż aktualne to hasła nie są dzisiaj zbyt efektywną metodą ochrony informacji. Najnowsze technologie ułatwiają atakującym szybkie łamanie haseł. Musimy znaleźć nowoczesne, ale wciąż proste i bezpieczne, rozwiązanie zapewniające uwierzytelnienie. Takim właśnie rozwiązaniem jest dwuskładnikowe uwierzytelnienie.

Dwuskładnikowe uwierzytelnienie

Dwuskładnikowe uwierzytelnienie (czasem skracane z angielskiego do “2FA”) jest dużo bezpieczniejszym rozwiązaniem niż same hasła. Zasada działania jest prosta: zamiast wykorzystywania tylko jednej metody uwierzytelniania, używane są dwie. Kiedy wypłacasz pieniądze z bankomatu również używasz dwuskładnikowego uwierzytelniania. Aby uzyskać dostęp do swoich środków potrzebujesz dwóch rzeczy: karty bankomatowej (coś co masz) oraz PIN (coś co wiesz). Nikt kto posiada

Dwuskładnikowe uwierzytelnianie

Twoją kartę, a nie zna kodu PIN nie jest w stanie wypłacić pieniędzy z bankomatu. Podobnie, jeśli ktoś zna tylko numer PIN, a nie posiada Twojej karty, nie wypłaci środków. Atakujący musi posiadać obie rzeczy, aby uzyskać dostęp do Twojego konta. Dlatego właśnie takie rozwiązanie jest bezpieczniejsze - masz dwie warstwy zabezpieczenia.

Używaj dwuskładnikowego uwierzytelnienia gdzie to tylko możliwe, bo to jeden z najważniejszych kroków, które możesz podjąć dla ochrony swoich danych.

Używanie dwuskładnikowego uwierzytelniania

Dwuskładnikowe uwierzytelnianie trzeba aktywować osobno dla każdego z kont. Na szczęście wiele serwisów internetowych na to pozwala. Jednym z liderów w dziedzinie dwuskładnikowego uwierzytelniania jest Google. Konta Google są jednym z głównych celów dla cyberprzestępców, ponieważ oferują darmowe usługi dla milionów osób na świecie. Właśnie dlatego Google jako jedna z pierwszych firm zaoferowało dwuskładnikowe uwierzytelnianie dla wszystkich swoich użytkowników. Jeśli zrozumiesz jak działa dwuskładnikowe uwierzytelnianie w usługach Google, zrozumiesz także jak ono działa na większości stron takich jak Twitter, Facebook, Apple, Instagram czy stronach bankowości elektronicznej.

Żeby włączyć dwuskładnikowe uwierzytelnianie musisz najpierw powiązać swój numer telefonu z kontem Google. Wtedy dwuskładnikowe uwierzytelnianie zaczyna działać w sposób następujący. Tak jak przy normalnym logowaniu podajesz nazwę użytkownika i hasło. To pierwszy z dwóch składników - coś, co znasz. Następnie Google wysyła wiadomość tekstową na Twój telefon, która zawiera unikalny kod, złożony z sześciu cyfr. Następnie podajesz ten kod na stronie - dokładnie tak jak podawałeś swoje hasło. Zatem, aby się zalogować potrzebujesz zarówno znać swoje hasło jak i posiadać telefon, na który przyjdzie unikalny kod. Nawet jeśli ktoś pozna Twoje hasło, wciąż musi posiadać Twój telefon, aby dostać kod. Aby zapewnić większe bezpieczeństwo, Google za każdym logowaniem tworzy nowy, losowy kod.

Istnieje również inny sposób na dwuskładnikowe uwierzytelnianie, również na stronach Google. Zamiast otrzymywać kod w wiadomości tekstowej, wystarczy zainstalować specjalną aplikację. Taka aplikacja generuje losowy kod za każdym razem gdy chcesz się zalogować. Zaletą jest to, że nie musisz być w zasięgu sieci komórkowej, aby dostać swój unikatowy kod, Twój telefon po prostu go wygeneruje. Ponadto, tak wytworzonego kodu nie można podsłuchać podczas przesyłania - tak jak wiadomości tekstowej.

Dwuskładnikowe uwierzytelnianie

Pamiętaj, że dwuskładnikowe uwierzytelnianie nie jest domyślnie włączone - musisz zrobić to osobiście. Z początku może się wydawać, że wymaga to dużo pracy, ale zalecamy jego użycie wszędzie, a szczególnie w przypadku usług krytycznych dla Twojej tożsamości, tak jak konto e-mail, bankowość internetowa czy przechowywanie plików. Dwuskładnikowe uwierzytelnianie jest dużo bardziej bezpieczne niż zwykłe hasła.

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

Przydatne linki

Hasła:	http://www.securingthehuman.org/ouch/2015#april2015
Dwuskładnikowe uwierzytelnianie w usługach Google:	http://www.google.com/landing/2step/

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