Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM NUMERZE..

Dwustopniowe uwierzytelnianie

Kim jesteś?

Proces udowodniania kim jesteś (zwany uwierzytelnianiem) jest kluczowym krokiem do ochrony Twoich informacji w Internecie. Jeśli chcesz być pewny, że tylko Ty masz dostęp do swoich prywatnych informacji, potrzebujesz bezpiecznej metody aby potwierdzić kim jesteś - na przykład podczas sprawdzania poczty e-mail, zakupów online czy uzyskując dostęp do swoich kont bankowych. Możesz udowodnić swoją tożsamość na trzy różne sposoby: podając coś co wiesz (np. hasło), coś co masz (np. paszport) lub kim jesteś (np. odcisk palca). Każda z tych metod ma swoje wady i zalety. Najbardziej popularną metodą uwierzytelniania jest podanie czegoś co wiesz: hasła.

Redaktor gościnny

James Tarala jest prelegentem, autorem i starszym wykładowcą Instytutu SANS. Jest głównym konsultantem w Enclave Security, współpracuje przy tworzeniu Critical Security Controls i **AuditScripts.com**. Możesz śledzić Jamesa na Twitterze **@isaudit** lub spotkać się z nim osobiście na jednym z jego najbliższych kursów.

Hasła

Najprawdopodobniej używasz haseł prawie codziennie. Hasło służy do udowodnienia, że jesteś tym za kogo się podajesz. Jest to dobry przykład czegoś co wiesz. Niebezpieczeństwem wiążącym się z hasłami jest to, że jeśli ktoś odgadnie lub uzyska dostęp do Twojego hasła, może łatwo podać się za Ciebie i uzyskać dostęp do wszystkich informacji, które są nim zabezpieczone. To dlatego uczy się użytkowników aby dobrze chronili swoje hasła, poprzez stosowanie tzw. silnych haseł, które są trudne do odgadnięcia dla atakujących. Problemem z hasłami jest to, że szybko stają się przestarzałe. Wraz z rozwojem nowych technologii coraz łatwiejsze dla atakujących staje się testowanie popularnych haseł i w rezultacie ich odgadnięcie lub masowe wykradnięcie przy użyciu takich technik jak rejestrowanie naciśnięć klawiszy na klawiaturze użytkownika. Do silnego uwierzytelnienia jest potrzebne prostsze niż zapamiętywanie bardzo skomplikowanych haseł i do tego bardziej bezpieczne rozwiązanie. Na szczęście takie rozwiązanie staje się coraz bardziej powszechne i nazywa się dwustopniowym uwierzytelnianiem (lub weryfikacją). Aby się zabezpieczyć, zalecamy korzystać z tej opcji w miarę możliwości.

Dwustopniowe uwierzytelnianie

Dwustopniowe uwierzytelnianie (czasami też nazywane dwuskładnikowym) jest bardziej bezpiecznym sposobem, aby potwierdzić Twoją tożsamość. Zamiast wymaganego tylko jednego kroku do uwierzytelnienia, takiego jak podanie hasła (czyli czegoś co coś wiesz), wymagane są dwa kroki. Korzystanie z karty do bankomatu jest

Dwustopniowe uwierzytelnianie

dobrym przykładem takiego uwierzytelniania. Kiedy wypłacasz pieniądze z bankomatu korzystasz właśnie z dwuetapowej weryfikacji. Aby udowodnić kim jesteś kiedy próbujesz otrzymać dostęp do swoich pieniędzy, potrzebne są dwie rzeczy: karta do bankomatu (coś co masz) i numer PIN (coś co wiesz). W przypadku utraty karty bankomatowej Twoje pieniądze są nadal bezpieczne, bo każdy, kto znajdzie kartę nie może ich wypłacić jeśli nie zna Twojego kodu PIN (oczywiście jeśli nie napisałeś swojego kodu PIN na swojej karcie, co jest bardzo złym pomysłem). Podobnie działa to jeśli ktoś zdobył tylko Twój PIN ale nie posiada karty. Atakujący musi być w posiadaniu obu tych rzeczy aby dostać się do Twoich pieniędzy. To właśnie sprawia, że dwuetapowa weryfikacja jest dużo bardziej bezpieczna: składa się z dwóch warstw zabezpieczeń.

Używaj dwuetapowego uwierzytelniania, kiedy tylko to możliwe, ponieważ jest to dużo bezpieczniejsze niż używanie tylko hasła.

Jak korzystać z dwustopniowego uwierzytelniania

Jednym z liderów w internetowym dwuetapowym uwierzytelnianiu jest Google. Wraz z szeroką ofertą bezpłatnych usług online, takich jak Gmail, Google potrzebowało zapewnić rozwiązanie bardziej bezpiecznego uwierzytelniania dla milionów użytkowników. I tak Google wprowadziło dwuetapową weryfikację dla większości swoich usług online. Ale nie tylko Google zapewnia bezpłatną usługę dwuetapowej weryfikacji dla każdego użytkownika. Inne serwisy też wykorzystują podobną technologię w swoich usługach: np. Dropbox, Facebook, LinkedIn i Twitter. Przez zrozumienie w jaki sposób działa dwuetapowe uwierzytelnianie Google, zrozumiesz, jak działa wiele innych usług wykorzystujących dwuskładnikowe uwierzytelnianie.

Dwuskładnikowe uwierzytelnianie Google działa w następujący sposób. Po pierwsze, potrzebna jest nazwa użytkownika i hasło, tak jak zazwyczaj. Ale jest to tylko pierwszy czynnik, czyli coś co wiesz. Jednak potem Google wymaga drugiego czynnika, czyli czegoś coś masz, a konkretnie - Twojego smartfona. Istnieją dwa różne sposoby w jakie można używać smartfona jako części procesu logowania. Pierwszym jest zarejestrowanie swojego numeru telefonu w Google. Podczas próby uwierzytelnienia się przy użyciu nazwy użytkownika i hasła, Google wyśle do Ciebie w wiadomości SMS nowy, unikalny kod. Wtedy trzeba wpisać ten numer podczas logowania. Drugim sposobem jest zainstalowanie oprogramowania uwierzytelniającego od Google w smartfonie. Wtedy to oprogramowanie generuje unikalny kod. Zaletą drugiego rozwiązania jest to, że nie musisz być podłączony do sieci operatora ponieważ to telefon generuje kod dla Ciebie.

Dwustopniowe uwierzytelnianie

Dwuskładnikowe uwierzytelnianie zazwyczaj nie jest włączone domyślnie i musisz włączyć je sam. Ponadto, większość aplikacji nie wspiera logowania z wykorzystaniem dwuetapowego uwierzytelniania do usług online. Dla każdej z tych aplikacji zazwyczaj trzeba użyć oddzielnego, dedykowanego hasła, które można wygenerować po uaktywnieniu dwuetapowego uwierzytelniania dla danej usługi. Ponadto masz możliwość utworzenia kluczy odzyskiwania w przypadku utraty smartfona. Zalecamy ich wydrukowanie i przechowywanie w bezpiecznym, zamykanym na klucz miejscu.

Gorąco zalecamy w miarę możliwości korzystanie z dwuskładnikowego uwierzytelniania, zwłaszcza dla krytycznych usług takich jak e-mail lub przechowywanie plików. Dwustopniowa weryfikacja znacznie lepiej chroni Twoje informacje, i jednocześnie przestępcy muszą pracować znacznie ciężej, aby skompromitować Twoje konto.

Dowiedz się więcej

Zasubskrybuj comiesięczny Biuletyn Bezpieczeństwa Komputerowego – 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

Gdzie możesz skorzystać z dwustopniowego uwierzytelniania:
http://lifehacker.com/5938565/heres-everywhere-you-should-enable-two+factor-authentication-right-now

Weryfikacja dwuetapowa Google:
http://www.google.com/landing/2step/

Słownik pojęcia bezpieczeństwa SANS (angielski):
http://www.securingthehuman.org/resources/security-terms

Porada dnia SANS Security (angielski):
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, Łukasz Siewierski