SANS SECURITY AWARENESS
CERT.PL
OUCH! | Grudzień 2017
Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu..

- **Hasła**
- **Czym jest dwuskładnikowe uwierzytelnianie**
- **Jak to działa**

Bezpieczne Logowanie

Wstęp

Proces uwierzytelniania stanowiący weryfikację naszej tożsamości, jest kluczowy przy okazji zabezpieczania dostępu do Twoich danych, takich jak poczta elektroniczna, media społecznościowe czy bankowość internetowa. Możesz nie zdawać sobie z tego sprawy, ale istnieją trzy sposoby, dzięki którym możesz potwierdzić własną tożsamość; coś co wiesz - na przykład znane Tobie hasło, coś co posiadasz – na przykład prawo jazdy, w końcu coś co jest częścią Ciebie – na przykład Twój odcisk palca. Każda z wyżej wymienionych metod ma swoje zalety i wady. Najbardziej powszechnym sposobem uzyskania dostępu, jest jak pewnie wiesz podanie hasła. Niestety, używanie haseł samych w sobie wydaje się stawać coraz mniej bezpieczne. W niniejszym wydaniu pokażemy, jak zwiększyć bezpieczeństwo logowania za pomocą środków idących znacznie dalej, niż samo stosowanie haseł, opowiemy o tzw. dwuskładnikowym uwierzytelnianiu.

Redaktor gościnny

Tiffany Schoenike jest dyrektorem ds. kampanii i inicjatyw w National Cyber Security Alliance (**@staysafeonline**). W 2016 roku Pani Schoenike współpracowała z Białym Domem, rządem oraz sektorem przemysłowym przy rozwijaniu i uruchamianiu kampanii Lock Down Your Login, inicjatywy promującej dwuskładnikowe uwierzytelnianie wchodzącej w skład STOP. THINK. CONNECT.™.

Same hasła już nie wystarczają

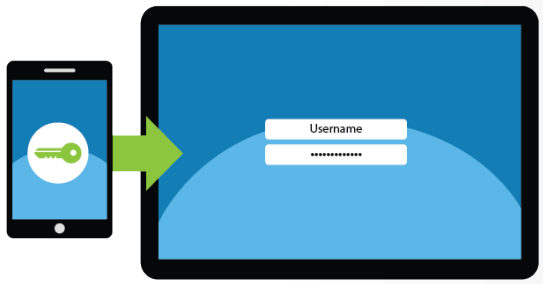
Hasła potwierdzają Twoją tożsamość bazując na tym, co wiesz. Jeżeli jednak ktoś odgadnie, lub w inny sposób pozna Twoje hasło, będzie mógł podszywając się pod Ciebie, uzyskać dostęp do informacji jakie posiadasz. Skompromitowane hasła stały się jedną z głównych przyczyn uzyskiwania nieautoryzowanych dostępów do danych. Właśnie dlatego jesteś zachęcany do korzystania z haseł odpowiednio złożonych, trudnych do odgadnięcia przez osoby postronne. Istotne jest także, aby nie używać tych samych haseł w przypadku logowania się do różnych serwisów, jak również nie udostępniać ich innym osobom. Podczas gdy powyższe zalecenia wciąż pozostają aktualne, hasła same w sobie nie chronią nas już tak skutecznie jak kiedyś. Istnieje na szczęście pewien prosty i szybki sposób, dający kontrolę i wpływający na poprawę bezpieczeństwa Twoich prywatnych danych, nazywamy go uwierzytelnianiem dwuskładnikowym.

Czym jest dwuskładnikowe uwierzytelnianie?

Uwierzytelnianie dwuskładnikowe (nazywane czasami podwójną weryfikacją, autentykacją wieloskładnikową lub 2FA) jest o wiele pewniejsze, niż zabezpieczenie dostępu do danych tylko za pomocą hasła. Funkcjonuje ono opierając się nie na jednym, ale dwóch różnych sposobach udowodnienia, że jesteś osobą za którą się podajesz. Dobrym przykładem

Bezpieczne Logowanie

może być tutaj karta bankomatowa. Wypłacając pieniądze z bankomatu korzystasz z uwierzytelniania dwuskładnikowego. Aby uzyskać dostęp do zgromadzonych na koncie środków potrzebujesz dwóch rzeczy: Twojej karty bankomatowej (coś, co posiadasz) i Twojego kodu PIN (coś, co wiesz). W momencie gdy Twoja karta bankomatowa zaginie lub zostanie skradziona, niepowołane osoby nie będą w stanie wypłacić pieniędzy bez znajomości kodu PIN.Aby dokonać wypłaty, złodziej musiałby mieć dostęp do dwóch składników: Twojej karty oraz Twojego PIN'u. Dwuskładnikowe uwierzytelnianie opiera się na tej właśnie zasadzie.



Uczyń swój proces logowania bezpieczniejszym wykorzystując dwustopniowe uwierzytelnianie wszędzie tam gdzie jest to możliwe, stanowi to jeden z najważniejszych kroków jakie możesz podjąć w celu poprawy swojego bezpieczeństwa w sieci.

Jak to działa

Dwuskładnikowe uwierzytelnianie jest szeroko dostępne dla większości wiodących serwisów związanych z obsługą bankowości internetowej, poczty elektronicznej, mediów społecznościowych, czy innych portali. Dodatkowo, wiele serwisów tego typu oferuje proste, prowadzące krok po kroku poradniki, w których wytłumaczone jest, jak aktywować metodę podwójnego uwierzytelniania (jeżeli chcesz uzyskać więcej informacji, zapoznaj się z sekcją *przydatne zasoby* na końcu biuletynu). Kiedy już dokonasz aktywacji opisywanej funkcjonalności, będziesz musiał zalogować się do swojego konta za pomocą nazwy użytkownika i hasła, tak jak odbywało się to dotychczas. To pierwszy z dwóch składników – coś, co wiesz. Następnie otrzymasz unikatowy kod, najczęściej w formie wiadomości tekstowej dostarczanej na Twój telefon komórkowy. Powyższy kod będziesz musiał przepisać na ekranie logowania. Oto drugi z dwóch składników – musisz mieć przy sobie Twój telefon, aby odebrać generowany kod. Dostęp do Twojego konta został dodatkowo zabezpieczony. Nawet jeżeli cyberprzestępcy odkryją Twoje hasło, nie będą mogli zalogować się do konta, musieliby w tym celu przejąć także Twój telefon.

Alternatywną metodą do odbierania unikatowych kodów przesyłanych w formie wiadomości SMS, może być zainstalowanie na smartfonie specjalnej aplikacji uwierzytelniającej. W momencie kiedy będziesz chciał zalogować się do konta, wygeneruje ona unikatowy ciąg znaków. Zaletą korzystania z tego typu aplikacji jest jeszcze wyższy poziom bezpieczeństwa. Wynika to z faktu, że kod generowany będzie w aplikacji, co pozwoli uniknąć przesyłania go poprzez SMS. O dodatkowej wygodzie stanowić będzie brak potrzeby utrzymywania łączności z usługą umożliwiającą otrzymanie klucza. Aplikacja generuje je w sposób ciągły, umożliwiając ich wykorzystanie w czasie logowania.

Bezpieczne Logowanie

Podczas gdy dwuskładnikowe uwierzytelnianie może w pierwszej chwili wydawać się pracochłonne, to jednak Twoje prywatne dane zostaną dzięki niemu znacznie lepiej zabezpieczone. Nie czekaj, aż Twoje konta zostaną zaatakowane przez hakerów, zadbaj o bezpieczeństwo procesu logowania, aktywując podwójne uwierzytelnianie w kluczowych serwisach, takich jak konto poczty elektroniczej, bankowość internetowa, czy portale społecznościowe i ciesz się poprawą Twojego poziomiu bezpieczeństwa.

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

Silne hasła:	https://securingthehuman.sans.org/ouch/2017#april2017
Strony wspierające dwuskładnikowe uwierzytelnianie:	https://twofactorauth.org
Stop|Think|Connect:	https://www.lockdownyourlogin.org
Dwustopniowa weryfikacja Google:	http://www.google.com/landing/2step/

Editorial Board: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Polski przekład (NASK/CERT Polska): Sebastian Kondraszuk, Michał Strzelczyk, Jacek Sikorski

