



Username

Password

LOGIN

Biuletyn Bezpieczeństwa Komputerowego

Tworzenie haseł w prostszy sposób

Wstęp

Mówi się, że hasła są kluczem do ochrony kont internetowych i aplikacji, co oczywiście jest prawdą. Niestety często występuje problem zapamiętywania haseł oraz tworzenia ich, w taki sposób aby dawały maksymalny poziom bezpieczeństwa. Poniżej przedstawimy trzy proste kroki upraszczające tworzenie haseł, oraz zapewnienie bezpieczeństwa. Omówimy dodatkowy sposób na zwiększenie ochrony kont i aplikacji.

Hasła wielowyrazowe

Czasy szalonych i skomplikowanych haseł dobiegają końca. Hasła tego typu są trudne do zapamiętania, ciężkie do wpisywania, a przy dzisiejszych możliwościach obliczeniowych komputerów, również coraz łatwiejsze do złamania. Kluczem do tworzenia bezpiecznych haseł jest ich długość. Z im większej liczby znaków składa się hasło, tym lepiej. Dobrą alternatywą przy tworzeniu silnych haseł są hasła zbudowane na frazach. Są to proste zwroty lub zdania, które są łatwe do zapamiętania. Poniżej przedstawiamy dwa przykłady:



*Kot Marleny lubi się wspinać po drzewach
codziennie-rano-wstaje-o-godzinie-6.15*

Oba przykłady haseł składają się z ponad dwudziestu znaków. Są łatwe do zapamiętania i wpisywania, jednakże są trudne do złamania przez cyberprzestępców. Różne strony internetowe bądź serwisy, podczas tworzenia konta, wymagają dodania znaków specjalnych do hasła (cyfra, wielka litera bądź symbol). Należy mieć na uwadze, że ważnym aspektem przy posiadaniu bezpiecznego hasła, jest jego długość.

Menedżer haseł

Nigdy nie powinno się używać jednego hasła do wielu usług, jest to bardzo niebezpieczne. Cyberprzestępcy, uzyskując dostęp do strony internetowej i wykradając hasła użytkowników, będą w stanie użyć tych haseł aby zalogować się nimi na inne konta. Z takim scenariuszem możemy się spotkać bardzo często. Polecamy zapoznać się ze stroną internetową www.haveibeenpwned.com, gdzie prezentowane są serwisy internetowe, na których w przeszłości doszło do wycieku bazy haseł. Jeżeli masz problem z zapamiętaniem haseł, sugerujemy skorzystanie z menedżera haseł.

Menedżery haseł to programy komputerowe, które przechowują hasła w zaszyfrowanej formie. Dostęp do programu wymaga zapamiętania zaledwie jednego hasła. Podczas logowania się na konto lub do aplikacji, potrzebne hasło może być automatycznie pobierane z menedżera. Nie musisz nawet znać ani pamiętać haseł, z których korzystasz. Na rynku istnieje wiele menadżerów haseł. Wiele z nich poza przechowywaniem haseł, posiada funkcje zapisania pytań pomocniczych

służących do zresetowania hasła, jak i również ostrzegania przed wygaśnięciem hasła. Przydatną funkcją menedżerów jest wbudowany generator haseł, który tworzy za nas silne, bezpieczne hasła. Większość tych programów potrafi synchronizować się pomiędzy różnymi urządzeniami oraz systemami operacyjnymi, więc niezależnie z jakiego urządzenia będziesz korzystał, zawsze będziesz miał pod ręką swoje hasła.

Dodatkowo, sugerujemy zapisać hasło dostępowe do menedżera haseł i trzymać je w bezpiecznym miejscu. Istnieją wersje menedżerów pozwalające na zrobienie kopii haseł poprzez wydruk. Tym sposobem zabezpieczysz się przed przypadkowym zapomnieniem głównego hasła do menedżera. Jeśli zachorujesz bądź przydarzy Ci się nieplanowany pobyt w szpitalu, Twoja rodzina w razie potrzeby będzie w stanie uzyskać dostęp do Twoich kont.

Uwierzytelnianie dwuskładnikowe

Uwierzytelnianie dwuskładnikowe często nazywane jest uwierzytelnianiem dwuczynnikowym bądź wieloetapowym. Sprawia, że dostęp do kont staje się jeszcze bezpieczniejszy. Podczas logowania na konta lub do aplikacji, poza hasłem dostępowym, użytkownik musi wprowadzić dodatkowy kod autoryzujący, który jest przesyłany SMS'em lub generowany przez aplikację. Proces ten zapewnia, że nawet jeśli cyberprzestępca pozyska hasło, nadal nie będzie mógł się dostać do konta. Weryfikacja dwuetapowa jest prosta w konfiguracji i nie przysparza wielu problemów podczas używania. Zazwyczaj dodatkowy kod wymagany jest podczas pierwszego logowania na konto z nowego komputera lub urządzenia. Uwierzytelnianie dwuetapowe warto włączyć wszędzie gdzie jest to możliwe, zwłaszcza przy logowaniu do konta bankowego lub poczty. Jeśli korzystasz z menedżera haseł, zalecamy ustanowienie silnego, niepowtarzalnego hasła oraz włączenie opcji uwierzytelnienia dwuskładnikowego.

Trzy przedstawione przez nas kroki może brzmiać mało poważnie, ale uwierz, że jeśli będziesz się do nich stosował, przyczynia się do zwiększenia ochrony Twoich finansów, reputacji oraz własności intelektualnej.

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](https://twitter.com/CERT_Polska)

Facebook: <http://facebook.com/CERT.Polska>

Redaktor wydania

Justin Henderson ([@SecurityMapper](https://twitter.com/SecurityMapper)) jest założycielem firmy H&A Security Solutions. Jest certyfikowanym instruktorem instytutu SANS oraz autorem kursów SANS Cyber Defense i SIEM. Interesuje się wszystkimi rzeczami związanymi z cyberbezpieczeństwem, oraz doradza w tej dziedzinie od 15 lat.



Źródła

Have I Been Pwned:

<https://haveibeenpwned.com/>

Uwierzytelnianie dwuskładnikowe:

<https://twofactorauth.org/>

Wytyczne NIST SP800-63B dotyczące tożsamości cyfrowej:

<https://pages.nist.gov/800-63-3/sp800-63b.html>

Plakat: Jesteś celem ataków:

<https://www.sans.org/u/OGi>

Biuletyn OUCH! powstaje w ramach programu „Security Awareness” Instytutu SANS i jest wydawany na licencji [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/). Powielanie treści biuletynu jest dozwolone jedynie w celach niekomercyjnych oraz pod warunkiem zachowania informacji o źródle pochodzenia kopiowanych treści oraz nienaruszania zawartości samego biuletynu. Informacje kontaktowe: www.sans.org/security-awareness/ouch-newsletter. Editorial Board: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Polski przekład (NASK/CERT Polska): Bartłomiej Wnuk, Konrad Purzycki, Janusz Urbanowicz