OUCH! I Maj 2013

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM NUMERZE..

Hasła

Czym są hasła?

Hasła są jednym z podstawowych sposobów, w jaki możemy udowodnić, kim jesteśmy. Używając ich logujemy się do poczty elektronicznej, bankowości on-line, dokonujemy zakupów w sieci i uzyskujemy dostęp do urządzeń, takich jak laptop lub smartfon. Można powiedzieć, że w wielu przypadkach hasła są niczym klucze do naszego królestwa. W związku z tym, jeśli ktoś byłby w posiadaniu Twojego hasła, mógłby dokonać kradzieży Twojej tożsamości, transferu Twoich pieniędzy lub uzyskać dostęp do wszystkich Twoich prywatnych danych. Używanie silnych haseł jest niezbędne aby chronić swoją tożsamość i swoje informacje. Dowiedzmy się, co sprawia, że hasło jest silne i jak bezpiecznie je stosować.

Redaktor gościnny

Raul Siles jest redaktorem gościnnym tego wydania OUCH! Raul jest założycielem i starszym analitykiem bezpieczeństwa w Taddong, a także autorem SANS, instruktorem i pasjonatem bezpieczeństwa. Możesz śledzić Raula na Twitterze na **@taddong** i na jego blogu **blog.taddong.com**.

Silne hasła

Cyberprzestępcy opracowali wyspecjalizowane programy, które coraz lepiej potrafią odgadnąć, a mówiąc inaczej "złamać", hasła. To oznacza, że mogą oni wykraść Twoje hasła jeśli są one słabe albo łatwe do odgadnięcia. Nigdy nie należy używać łatwo dostępnych informacji tworząc hasła. Do takich informacji należą na przykład data urodzenia, imię zwierzątka lub cokolwiek, co można łatwo znaleźć na portalach społecznościowych lub wyszukać w Google. Zamiast tego, najlepszym sposobem na stworzenie silnego hasła jest użycie długiego hasła, które im więcej znaków zawiera, tym lepiej. Najlepiej zamiast używać jednego słowa, używać wielu słów, a nawet pełnych zdań. Tego typu hasło nazywa się z angielskiego passphrase i jest jednym z najsilniejszych jakich można użyć. Oto przykład jednego z nich:

stoi na stacji lokomotywa

To wszystko czego potrzebujesz. Jeśli jest to wymagane, możesz sprawić że Twoje hasło stanie się jeszcze silniejsze dodając do niego symbole, wielkie litery lub cyfry, tak jak w przykładzie poniżej. Jest to szczególnie ważne, jeśli korzystasz z portali nie pozwalających używać wielu słów lub pełnych zdań jako hasła:

Stoi na stacji l0komotywa!

Zwróć uwagę, jak w przykładzie została użyta wielka litera. Możesz również zastąpić niektóre litery cyframi lub symbolami, na przykład zastępując literę "a" symbolem "@", literę "o" zerem, albo dodać znaki przestankowe, takie jak znak zapytania, kropkę czy nawet spację. Jeśli portal lub program ogranicza liczbę znaków w haśle, użyj maksymalnej dozwolonej liczby znaków.

Hasła

Bezpieczne korzystanie z haseł

Poza używaniem mocnych haseł, należy również ostrożnie się z nimi obchodzić. Posiadanie mocnego hasła nie pomoże, jeśli będzie można je łatwo wykraść lub skopiować.

Używaj silnych haseł, najlepiej złożonych z wielu słów i upewnij się, że korzystasz z nich bezpiecznie!

1. Upewnij się że używasz różnych haseł do różnych kont. Na przykład, nigdy nie używaj tych samych haseł do usług w pracy czy do konta w banku co do haseł do kont osobistych, takich jak Facebook, YouTube czy Twitter. W ten sposób, jeśli jedno z haseł zostanie skompromitowane, pozostałe konta pozostaną nadal bezpieczne. Jeśli masz zbyt wiele haseł do zapamiętania, rozważ użycie menedżera haseł. Jest to specjalny program, który działa na komputerze lub urządzeniu przenośnym, który bezpiecznie przechowuje wszystkie Twoje hasła. Jedyne hasło, które trzeba zapamiętać to hasło do komputera i programu do zarządzania hasłami. Jeśli chcesz zastosować taki program do haseł używanych w pracy, skontaktuj się ze swoim przełożonym lub pomocą techniczną aby upewnić się czy korzystanie z menedżera haseł jest dozwolone w Twojej organizacji.

2. Nigdy nie udostępniaj swojego hasła innym osobom, także współpracownikom. Pamiętaj, że hasło jest tajemnicą, a jeśli ktoś je pozna, nie jest już bezpieczne. Jeżeli przypadkowo podzieliłeś się hasłem z kimś innym lub domyślasz się, że mogło być ono zostać złamane lub wykradzione, należy je natychmiast zmienić.

3. Nie należy korzystać z publicznych komputerów, takich jak te w hotelach lub w bibliotekach, aby logować się na konto do pracy lub do banku. Ponieważ każdy może korzystać z tych komputerów, mogą one być zainfekowane złośliwym oprogramowaniem, które przechwytuje wszystkie naciśnięcia klawiszy. Do kont w swojej pracy lub rachunków bankowych loguj się tylko z zaufanych komputerów lub urządzeń mobilnych, nad którymi masz kontrolę.

4. Uważaj na strony internetowe, które wymagają odpowiedzi na osobiste pytania. Pytania te są używane, jeśli zapomnisz hasła i trzeba będzie je zresetować. Sęk w tym, że odpowiedzi na te pytania można często znaleźć w Internecie czy nawet na Facebooku. Upewnij się, że jeśli odpowiadasz na osobiste pytania używasz tylko informacji, które nie są dostępne publicznie lub są to fikcyjne dane, celowo przez Ciebie zmyślone. Programy do zarządzania hasłami mogą pomóc także w trzymaniu bezpiecznie takich odpowiedzi, gdyż wiele z nich pozwala na przechowywanie dodatkowych informacji o kontach.

Hasła

5. Wiele kont internetowych oferuje coś, co jest nazywane “dwuskładnikowym uwierzytelnianiem” lub “dwuetapową weryfikacją”. Jest to stosowane kiedy do logowania potrzebne jest więcej niż tylko jedno hasło, np. dodatkowo żądany jest kod przesyłany na smartfon. Użycie tej metody jest o wiele bardziej bezpieczne niż użycie samego hasła. Jeśli tylko jest to możliwe, należy zawsze korzystać z tych silniejszych metod uwierzytelniania.

6. Urządzenia mobilne często wymagają podania kodu PIN w celu ochrony dostępu do nich. Pamiętaj, że PIN jest niczym innym tylko kolejnym hasłem. Im Twój PIN jest dłuższy, tym jest bardziej bezpieczny. Niektóre urządzenia mobilne (np. iPhone) pozwolą Ci zmienić numer PIN na zwykłe literowe hasło.

7. I na koniec, zapamiętaj: jeśli przestajesz korzystać z konta, należy je zamknąć, usunąć lub wyłączyć.

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

Weryfikacja dwuetapowa:	http://www.google.com/landing/2step
Programy do zarządzania hasłami:	http://www.freepasswordmanager.com
Siła hasła:	https://xkcd.com/936
Słownik pojęć bezpieczeństwa (ang.):	http://preview.tinyurl.com/6wkpae5
Porada dnia SANS (ang.):	http://preview.tinyurl.com/6s2wrkp

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