Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM WYDANIU..

- Wyrażenia hasłowe
- Bezpieczne używanie wyrażeń hasłowych
- Dodatkowe informacje

Nowe oblicze hasła

Wprowadzenie

Haseł używamy na co dzień, począwszy od logowania się do kont poczty elektronicznej lub bankowości online, skończywszy na zakupach online czy odblokowywaniu swojego smartfona. Niestety hasła to także jedno z najsłabszych zabezpieczeń - w przypadku, gdy ktoś je pozna może ukraść naszą tożsamość (np. na portalu społecznościowym), przelać nasze pieniądze z konta bankowego lub uzyskać dostęp do poufnych informacji osobistych. Silne hasła to podstawa ochrony osobistej. W tym wydaniu magazynu OUCH! dowiesz się jak tworzyć silne i bardzo łatwe do zapamiętania hasła poprzez użycie tzw. wyrażeń hasłowych.

Redaktor gościnny

Guy Bruneau jest starszym konsultantem ds. bezpieczeństwa w IPSS Inc., instruktorem w Instytucie SANS oraz zajmuje się obsługą incydentów w ISC (Internet Storm Center). Ukończył program Cyber Guardian oraz jest certyfikowanym ekspertem ds. bezpieczeństwa (GSE). Można go znaleźć na Twitterze (**@GuyBruneau**) oraz na stronie **handlers.sans.org/gbruneau**.

Wyrażenia hasłowe

Cyberprzestępcy na potrzeby swoich działań wynajdują coraz bardziej wyszukane metody zgadywania lub łamania haseł i z każdą chwilą stają się w tym coraz lepsi. Oznacza to, że jeżeli hasło jest zbyt proste lub łatwe do odgadnięcia, to może szybko stać się ich łupem. Ważnym elementem ochrony osobistej jest używanie silnych haseł. Niestety, długie i skomplikowane hasła mogą być trudne do zapamiętania. Alternatywą dla ich używania są tzw. wyrażenia hasłowe. Są to proste zwroty lub zdania, które są bardzo łatwe do zapamiętania ale bardzo trudne do złamania przez narzędzia używane przez przestępców. Poniżej prezentujemy przykład:

Gdzie jest król Julian?

To wyrażenie hasłowe jest przykładem silnego hasła z kilku względów - jest długie, bo zawiera aż 23 znaki (wliczając spacje) oraz używa wielkich liter oraz znaków specjalnych (spacje oraz znak "?"). Możesz łatwo sprawić, żeby było jeszcze silniejsze poprzez zamianę niektórych liter na odpowiadające im inne symbole, np. zamianę liter "a" na znak "@" lub liter "o" na cyfrę "0". W przypadku, gdy strona internetowa lub program którego używasz ograniczają długość możliwego do użycia hasła, zawsze staraj się wykorzystać ten limit i wykorzystać wszystkie możliwe znaki.

Bezpieczne używanie wyrażeń hasłowych

Pomimo tego, że zastąpisz swoje hasła wyrażeniami hasłowymi, musisz nadal pozostać czujny i nie dopuścić do tego, aby Twoje nowe hasło zostało skradzione. Poniżej prezentujemy kilka porad bezpiecznego używania haseł.

Nowe oblicze hasła

1. Zawsze staraj się używać różnych wyrażeń hasłowych dla różnych kont i urządzeń, które posiadasz. Nigdy nie używaj tego samego hasła do komputera w pracy lub konta bankowego i do innych kont jak np. na portalach społecznościowych jak Facebook, YouTube czy Twitter. Zapewni to, że jeżeli nawet któreś z kont padnie łupem przestępców, pozostałe nadal będą bezpieczne. Jeśli masz zbyt wiele kont i nie jesteś w stanie zapamiętać wszystkich wyrażeń hasłowych do nich, zacznij używać menadżera haseł. Jest to oprogramowanie specjalnie zaprojektowane do bezpiecznego przechowywania wielu haseł. Dzięki niemu będziesz musiał zapamiętać tylko dwa hasła: jedno do zalogowania się na komputerze oraz drugie do menadżera haseł.

2. NIGDY nie dziel się z NIKIM swoim wyrażeniem hasłowym lub metodą jakiej używasz do ich tworzenia. Zapamiętaj jedno, Twoje hasło to sekret - jeżeli ktoś je pozna, nie jest już nadal bezpieczne. Jeśli przypadkiem podasz komuś swoje wyrażenie hasłowe lub masz podejrzenia, że mogło zostać wykradzione, natychmiast zmień je na inne.

Używanie wyrażeń hasłowych to jeden z najbardziej skutecznych kroków jakie możesz podjąć, aby ochronić siebie i swoje dane.

3. Podobnie jak dla haseł, unikaj tworzenia wyrażeń hasłowych, które są proste do odgadnięcia lub powszechnie używane. Np. wyrażenie hasłowe “Kwiecień plecień, bo przeplata trochę zimy, trochę lata” nie powinno być używane, ponieważ jest znanym przysłowiem.

4. Nie używaj publicznie dostępnych komputerów, np. w hotelach lub bibliotekach, do logowania się na konta bankowe lub służbowe. Takie komputery, ze względu na to, że każdy ma do nich dostęp, mogą być zainfekowane złośliwym oprogramowaniem, które zapamiętuje wszystko, co zostanie wpisane na klawiaturze. Loguj się na swoje konta wyłącznie na komputerach i urządzeniach przenośnych, którym ufasz.

5. Uważaj na strony internetowe, które wymagają, abyś odpowiadał na osobiste pytania. Są one potem wykorzystywane w procedurze odzyskiwania hasła w przypadku, gdy go zapomnisz. Częsty problem z tego typu pytaniami polega na tym, że odpowiedzi na nie da się łatwo znaleźć w Internecie, np. na profilu Facebook. Upewnij się, że jeśli podajesz odpowiedzi na tego typu pytania, to używasz informacji, które nie są publicznie dostępne lub zmyślone. Programy do zarządzania hasłami, o których wspomnieliśmy wcześniej, mogą Ci pomóc w bezpiecznym przechowywaniu takich informacji.

6. Wiele z portali internetowych oferuje sposób logowania się oparty na tzw. dwustopniowym uwierzytelnieniu. Polega on na tym, że do uzyskania dostępu do konta potrzebne jest nie tylko hasło, ale także kod jednorazowy otrzymywany

Nowe oblicze hasła

SMSem. Korzystanie z takiej opcji jest o wiele bezpieczniejsze niż użycie tylko samego hasła. Jeśli portal, z którego korzystasz umożliwia włączenie takiej opcji, koniecznie jej używaj.

7. Urządzenia przenośne często wymagają podania kodu PIN w celu ich odblokowania. Pamiętaj, że ten kod to tylko inna forma hasła. Zatem im dłuższy jest PIN tym jest bardziej bezpieczny. Wiele z nowoczesnych smartfonów pozwala na użycie prawdziwych haseł zamiast zwykłych kodów PIN.

8. W końcu, jeśli nie używasz już swoich kont, postaraj się je wyłączyć, usunąć lub zdezaktywować.

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

Dwustopniowe uwierzytelnianie:	http://www.securingthehuman.org/ouch/2013#august2013
Systemy zarządzania hasłami:	http://www.securingthehuman.org/ouch/2013#october2013
Socjotechnika:	http://www.securingthehuman.org/ouch/2014#november2014
Słownik pojęć (j.ang.):	http://www.securingthehuman.org/resources/security-terms

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