

OUCH!

W TYM NUMERZE..

- Zarys problemu
- Proponowane rozwiązanie
- Sposób działania menadżera haseł
- Wybierz jeden dla siebie

Systemy zarządzania hasłami

Zarys problemu

Jedną z pierwszych zasad jakie poznajemy gdy uczymy się chronić naszą cyfrową tożsamość to potrzeba tworzenia i używania silnych haseł. Z lektury poprzednich wydań magazynu OUCH! wiemy już, że silne hasło to nie tylko takie, które nie da się łatwo odgadnąć, czyli nie jest stworzone na bazie naszych urodzin czy imienia psa, ale także takie, którego nie da się łatwo złamać z użyciem ogólnie dostępnych narzędzi. Prosta zasada jaką można się kierować przy tworzeniu hasła to "im dłuższe i bardziej skomplikowane hasło - tym lepiej". Niestety pojawia się problem, że takie długie hasło nie jest łatwo zapamiętać. Prowadzi to do sytuacji, że często tworzymy jedno skomplikowane hasło i używamy we wszystkich serwisach internetowych i aplikacjach. Czasami nawet, co jest groźnym naruszeniem norm bezpieczeństwa, używamy tego samego hasła zarówno dla kont prywatnych jak i związanych z pracą. To co chcemy osiągnąć, to przypisanie indywidualnego, mocnego hasła do każdego z kont. Wtedy, nawet w przypadku gdy jedno z kont padnie ofiarą cyberwłamywacza, pozostałe będą bezpieczne. Niestety, zapamiętanie tak dużej liczby haseł jest niemożliwe.

Redaktor gościnnie

Październikowe wydanie biuletynu OUCH! powstało dzięki pomocy George'a Bakosa, Dyrektora Technicznego departamentu Intelligence & Response firmy Northrop Grumman. Od roku 2001 George jest certyfikowanym instruktorem w Instytucie SANS, a w listopadzie tego roku będzie prowadził w Londynie szkolenie poświęcone ochronie sieci - Security 502.

Proponowane rozwiązanie

Jednym z rozwiązań (ale odradzonym!) jest zapisywanie haseł w notesie. Grozi to tym, że jeśli go stracimy, to razem z nim także dostęp do naszych kont. A osoba, która go znajdzie (lub ukradnie) będzie mogła uzyskać do nich dostęp. Jeszcze gorszym rozwiązaniem jest zapisywanie haseł na karteczkach i przyklejanie ich na monitorze lub biurku - jeden rzut oka na miejsce pracy osoby, która tak robi i wszystkie jej dane są zagrożone. Wyjściem z tej sytuacji jest użycie oprogramowania, które będzie w bezpieczny sposób przechowywać nasze hasła w miejscu, do którego mamy zawsze dostęp. Jeszcze lepiej by było, gdyby taki program był łatwy w użyciu i integrował się z przeglądarką internetową oraz innymi aplikacjami. Dodatkowo, powinien pozwalać na generowanie silnych haseł oraz pozwalać na przechowywanie innych wrażliwych danych, np. numerów kart kredytowych. Na szczęście takie programy już istnieją. Nazywamy je menadżerami haseł lub systemami zarządzania hasłami.

Systemy zarządzania hasłami

Sposób działania menadżera haseł

System zarządzania hasłami działa trochę jak wirtualny sejf. Po zainstalowaniu na komputerze lub urządzeniu przenośnym, umieszczasz w nim wszystkie swoje dane do logowania się w serwisach oraz poufne informacje, a on zapisuje je w bazie danych, którą następnie szyfruje. Zaszzyfrowana baza może być przechowywana tylko na danym urządzeniu lub synchronizowana z wieloma urządzeniami, np. za pomocą serwisów umieszczonych w chmurze (jak Dropbox). Dostęp do takiej bazy jest chroniony za pomocą hasła, ale jest to jedyne hasło jakie musisz zapamiętać - wszystkie inne będą udostępnione Ci przez program. Pozwala to na używanie unikatowych silnych haseł dla każdego z kont, nawet jeśli masz ich setki. Hasło, które daje dostęp do bazy wirtualnego sejfu, powinno być bardzo silne i takie, którego nie zapomnisz!



Systemy zarządzania hasłami to prosta metoda na bezpieczne przechowywanie wszystkich Twoich haseł.

Wiele z dostępnych systemów zarządzania hasłami integruje się z przeglądarkami internetowymi, w sposób, który pozwala na automatyczne lub prawie automatyczne logowanie się do portali i serwisów, w których mamy założone konta. Jeśli zmienisz hasło w takim serwisie, to zostanie ono także zmienione w menadżerze haseł, który dba o to, aby mieć aktualną bazę. Część z menadżerów haseł ma swoje odpowiedniki na urządzenia mobilne. Niestety nie integrują się tak dobrze z mobilnymi aplikacjami jak w wersji na komputery stacjonarne, a jedynie współpracują z mobilnymi przeglądarkami.

Wybierz jeden dla siebie

Istnieje wiele płatnych oraz darmowych systemów zarządzania hasłami. Powinniśmy wybrać jeden z nich uwzględniając następujące kwestie:

- Używaj tylko sprawdzonych i potwierdzonych rozwiązań, które zapewniają wsparcie producenta lub społeczności użytkowników. Trzymaj się z daleka od mało znanych programów, gdyż mogą być próbą wyłudzenia Twoich danych.
- Zwróć uwagę na to, czy oprogramowanie jest często aktualizowane i czy zawsze używasz najnowszej wersji.
- Program powinien być łatwy w obsłudze. Trudny lub mało intuicyjny program może powodować, że będziesz popełniać błędy w czasie jego używania lub zwyczajnie się do niego zniechęcis.

Systemy zarządzania hasłami

- Dane jakie przechowujesz w takim wirtualnym sejfie powinny być zaszyfrowane z użyciem znanych, otwartych i potwierdzonych standardów szyfrowania. Każde rozwiązanie, które chwali się, że ma swój własny, zamknięty algorytm szyfrowania powinno być natychmiast odrzucone z Twojej listy.
- Oprogramowanie powinno działać na wszystkich typach urządzeń jakie posiadasz, także tych przenośnych, jak smartfony i tablety.
- System powinien pozwalać na bezpieczną (szyfrowaną) synchronizację bazy danych haseł pomiędzy wszystkimi urządzeniami jakie posiadasz.
- System powinien dostarczać mechanizmów generowania silnych haseł oraz ułatwiać zarządzanie nimi (np. generować przypomnienia o zmianę hasła, jeśli ustawimy jego ważność).
- Program powinien pozwalać na określenie siły hasła, jeśli chcemy takie hasło wybrać sami.

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

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

Źródła

“O zarządzaniu hasłami”:

<https://www.technologie.org.pl/artykuly/jedno-za-wszystkie-o-zarządzaniu-hasłami>

Słownik pojęć bezpieczeństwa SANS (j. angielski):

<http://www.securingthehuman.org/resources/security-terms>

Biuletyn OUCH! powstaje w ramach programu „Securing The Human” Instytutu SANS i jest wydawany na licencji [Creative Commons BY-NC-ND 3.0](https://creativecommons.org/licenses/by-nc-nd/3.0/). 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: ouch@securingthehuman.org

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