OUCH! | wrzesień, 2017

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu..

- Wprowadzenie
- Jak działają menedżery haseł
- Wybór aplikacji

Menedżery Haseł

Wprowadzenie

Jednym z najważniejszych kroków, które możesz podjąć w celu ochrony swojej aktywności w sieci, jest wykorzystywanie niepowtarzalnego i silnego hasła dla każdego konta oraz aplikacji. Niestety, samodzielne zapamiętanie unikatowych danych logowania do poszczególnych kont graniczy z niemożliwością. Prawdopodobnie właśnie to jest jednym z powodów, dla którego tak wiele osób wykorzystuje te same hasła w wielu miejscach. Niestety, to rozwiązanie wiąże się z pewnym niebezpieczeństwem – w przypadku kompromitacji hasła, osoba która znajdzie się w jego posiadaniu, uzyska dostęp do wszystkich kont, dla których jest ono przypisane. Prostym rozwiązaniem jest używanie menedżera haseł, czasami nazywanego skarbcem (ang. password vault). Menedżery haseł to aplikacje przechowujące w sposób bezpieczny wszystkie zgromadzone poświadczenia do odwiedzanych przez Ciebie miejsc, dzięki czemu posiadanie unikatowych danych logowania do różnych serwisów staje się proste. Zamiast zapamiętywania haseł do poszczególnych kont na które się logujesz, pozostaje Ci zapamiętanie głównego hasła umożliwiającego dostęp do menedżera.

Redaktor gościnny

Chris Christianson jest Konsultantem ds. Bezpieczeństwa Informacji w Kaliforni, posiada 20 letnie doświadczenie oraz liczne certyfikaty. Występował jako mówca na różnorodnych konferencjach, a także autor wielu artykułów branżowych. Kontakt z Chrisem możliwy jest przez Twittera **@cchristianson** oraz stronę **https://ismellpackets.com**.

Jak działają menedżery haseł

Menedżery haseł funkcjonują przechowując wszystkie hasła w bazie danych, czasami nazywanej skarbcem. Aplikacja szyfruje zawartość tej bazy i zabezpiecza ją za pomocą głównego hasła znanego tylko Tobie. W momencie potrzeby uzyskania dostępu do danych, np. w celu zalogowania się do banku lub poczty e-mail po prostu uruchamiasz aplikację przechowującą Twoje poświadczenia, wpisujesz hasło główne i zyskujesz możliwość wglądu do bazy. Tego typu narzędzia nierzadko są w stanie automatycznie pobrać hasło, którego poszukujesz i w bezpieczny sposób zalogować Cię do miejsca docelowego. Wszystko to sprawia, że posiadanie setek niepowtarzalnych, silnych poświadczeń do różnych kont przestaje być kłopotliwe, z uwagi na brak konieczności ich zapamiętywania.

Niektóre menedżery haseł przechowują bazę danych lokalnie na Twoim komputerze lub urządzeniu mobilnym, inne z kolei przechowują ją w chmurze. Dodatkowo, wiele aplikacji do zarządzania hasłami posiada zdolność automatycznej synchronizacji zapisanych danych z innymi urządzeniami, które do tego upoważnisz. W ten sposób, aktualizując wpis w menedżerze haseł np. na swoim laptopie, roześlesz go także do pozostałych upoważnionych urządzeń. Niezależnie od tego czy baza danych jest przechowywana lokalnie, czy w chmurze, aby korzystać z menedżera haseł, potrzebujesz zainstalować go na swoim urządzeniu lub w systemie.

Menedżery Haseł

Kiedy uruchomisz menedżera haseł po raz pierwszy, będziesz potrzebował zaimportować do niego swoje loginy i hasła lub wprowadzić je ręcznie. Następnie, aplikacja może próbować wykryć Twoją próbę założenia nowego konta w chmurze, lub automatycznie zaktualizować istniejąca bazę danych. Jest to możliwe, ponieważ spora część oprogramowania tego typu pracuje we współpracy z przeglądarką internetową. W oparciu o wyżej wspomnianą integrację możliwe jest automatyczne logowanie do witryn w sieci web.

Niezwykle istotne jest, aby główne hasło, które zabezpiecza dostęp do zawartości menedżera haseł cechowało się odpowiednią siłą i wysoką trudnością do odgadnięcia przez innych. Zalecamy, aby główne hasło stanowił odpowiednio długi ciąg znaków. Jeżeli Twój menedżer haseł umożliwia dwuskładnikowe uwierzytelnianie, korzystaj z tego rozwiązania razem z hasłem głównym. Na koniec upewnij się, że jesteś w stanie je zapamiętać. W przypadku zapomnienia, utracisz możliwość dostępu do bazy z pozostałymi hasłami.

Menedżery haseł to łatwy sposób na bezpieczne przechowywanie i korzystanie ze wszystkich unikalnych haseł, jakie posiadasz.

Wybór aplikacji

Jest wiele menedżerów haseł, z których możemy wybierać. W sekcji przydatne zasoby, udostępniamy link do strony zawierającej przegląd oprogramowania tego typu. Tymczasem, próbując znaleźć rozwiązanie dopasowane do Twoich potrzeb, miej na uwadze następujące rzeczy:

- Twoja aplikacja powinna być dla Ciebie prosta w użyciu. Jeżeli trafisz na rozwiązanie, które przerasta Cię stopniem skomplikowania, znajdź takie które pasuje do Twoich preferencji i doświadczenia.
- Menedżer haseł powinien poprawnie działać na wszystkich urządzeniach, na których będziesz korzystał z haseł. Powinien także w prosty sposób umożliwiać ich synchronizację z pozostałymi urządzeniami.
- Używaj tylko dobrze znanych i zaufanych menedżerów haseł. Uważaj na produkty, których nie było na rynku przez dłuższy czas oraz takie, które posiadają znikome opinie w środowisku technicznej społeczności, lub nie posiadają ich wcale. Cyberprzestępcy potrafią przygotować fałszywą aplikację, celem kradzieży Twoich danych. Powinieneś być bardzo podejrzliwy w przypadku producentów oprogramowania promujących wypracowane przez siebie rozwiązania szyfrujące.
- Unikaj wszelkich menedżerów haseł, które uważają że są w stanie odzyskać dla Ciebie hasło główne. Oznacza to, że jest ono komuś znane, co wystawia Cię na zbyt duże ryzyko.
- Niezależnie od wybranego rozwiązania, upewnij się, że producent wciąż je rozwija i oferuje aktualizacje. Pamiętaj, aby zawsze korzystać aktualnej wersji.

Menedżery Haseł

- Menedżer haseł powinien posiadać wbudowaną funkcjonalność automatycznego generowania dla Ciebie silnych haseł oraz wyświetlania siły już wygenerowanych.
- Aplikacje tego typu powinny oferować Ci możliwość przechowywania innego rodzaju danych wrażliwych, takich jak odpowiedzi na pytania umożliwiające resetowanie haseł, dane kart kredytowych czy numery rezerwacji lotniczych.

Menedżery haseł są świetnym rozwiązaniem do bezpiecznego przechowywania wszystkich Twoich poświadczeń i innych danych wrażliwych. Ponieważ jednak chronią tak ważne informacje, upewnij się, że używasz unikalnego, silnego hasła głównego, które jest nie tylko trudne do odgadnięcia przez atakujących, ale również łatwe do zapamiętania przez Ciebie.

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

Przegląd najlepszych menedżerów haseł w roku 2017: https://www.pcmag.com/article2/0,2817,2407168,00.asp
Dobre hasła:
https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201704_po.pdf
Dwuskładnikowe uwierzytelnianie:
https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201509_po.pdf
Kampania Lock Down Your Login: https://www.lockdownyourlogin.org/
SANS Security Tip of the Day: https://www.sans.org/tip-of-the-day

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

