OUCH! | Październik 2015

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM WYDANIU..

- Zarys problemu
- Jak działają menedżery haseł
- Wybór menedżera haseł

Menedżery haseł

Zarys problemu

Jedną z pierwszych zasad jakie poznajemy gdy uczymy się chronić naszą cyfrową tożsamość to potrzeba tworzenia i używania silnych haseł. Niestety, większość z nas ma tak wiele kont, że jest to prawie niemożliwe, aby zapamiętać wszystkie hasła. Prostym rozwiązaniem jest użycie menedżera haseł, czasami nazywanego sejfem na hasła. Aplikacje te są przeznaczone do bezpiecznego przechowywania danych do logowania się. Co więcej, sprawiają one, że o wiele łatwiej można się zalogować do stron internetowych, aplikacji mobilnych i aplikacji zainstalowanych na komputerze.

Redaktor gościnny

Lenny Zeltser pracuje nad zabezpieczeniem operacji informatycznych klientów w NCR Corp oraz szkoli specjalistów bezpieczeństwa w SANS Institute. Lenny jest aktywny na Twitterze, jako **@lennyzeltser** i publikuje artykuły na **zeltser.com**.

Jak działają menedżery haseł

Menedżer haseł działa jak cyfrowy sejf - bezpiecznie przechowuje loginy, hasła i inne poufne informacje. Kiedy strona wymaga, aby zalogować się na konto, menedżer haseł może automatycznie odnaleźć hasło i bezpiecznie zalogować Cię na stronie internetowej. To sprawia, że w prosty sposób możesz posiadać setki unikalnych silnych haseł i nie musieć ich zapamiętywać.

Menedżery haseł przechowują Twoje dane w bazie danych, która jest czasami nazywana sejfem. Szyfrują one zawartość sejfu i chronią ją hasłem głównym, które tylko Ty znasz. Kiedy trzeba pobrać dane do logowania, np. w celu zalogowania się się do swoich kont bankowych lub pocztowych, wystarczy wpisać hasło główne do swojego menedżera haseł, aby odblokować sejf.

Niektóre menedżery haseł przechowują sejf w systemie lokalnym lub w smartfonie, podczas gdy inne przechowują go na zdalnym serwerze prowadzonym przez firmę, która zbudowała menedżer haseł. Ponadto, większość menedżerów haseł ma funkcję automatycznego synchronizowania zawartości sejfu na wielu urządzeniach, które zautoryzujesz. W ten sposób po aktualizacji hasła, np. na laptopie, zmiany są synchronizowane do smartfonu, tabletu lub innych komputerów, z których korzystasz. Niezależnie od tego, gdzie jest przechowywana baza danych, należy zainstalować menedżera haseł na urządzeniu, na którym mamy zamiar go używać.

Podczas pierwszej konfiguracji menedżera haseł, należy ręcznie wprowadzić lub zaimportować loginy i hasła. Następnie menedżer wykrywa, kiedy próbujesz założyć nowe konto internetowe lub zaktualizować hasło dla istniejącego konta i automatyczne aktualizuje dane w sejfie. Jest to możliwe, ponieważ większość menedżerów haseł

Menedżery haseł

ma zaimplementowaną współpracę z przeglądarkami internetowymi. Integracja ta pozwala na automatyczne logowanie się na strony internetowe.

Menedżery haseł są przeznaczone do bezpiecznego przechowywania poufnych danych. Jednak bardzo ważne jest, żeby główne hasło używane do ochrony zawartości sejfu było silne i bardzo trudne do odgadnięcia dla innych. W rzeczywistości zalecamy, aby hasło główne było wyrażeniem hasłowym - jedną z metod tworzenia najsilniejszych rodzajów haseł. Jeśli menedżer haseł obsługuje weryfikację dwuetapową, zalecamy użyć jej dla hasła głównego. Na koniec upewnij się, że nie korzystasz z hasła głównego do jakiegokolwiek innego systemu lub konta. W ten sposób, nawet jeśli przestępcy uda się uzyskać kopię sejfu, nie będzie w stanie odgadnąć hasła i uzyskać dostępu do jego zawartości. Wreszcie, należy zapamiętać hasło główne. Jeżeli je zapomnisz, nie będziesz w stanie uzyskać dostępu do swoich innych haseł.

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

Wybór menedżera haseł

Istnieje wiele menedżerów haseł, zarówno darmowych jak i komercyjnych. Gdy próbujesz znaleźć ten, który jest najlepszy dla Ciebie, pamiętaj o następujących kwestiach:

- Oprogramowanie powinno działać na wszystkich typach urządzeń jakie posiadasz, także tych przenośnych, jak smartfony i tablety. Wybrane rozwiązanie powinno również umożliwiać synchronizację zawartości sejfu na wszystkich urządzeniach.
- Należy używać tylko dobrze znanych i zaufanych menedżerów haseł. Uważaj na produkty, które nie były aktualizowane od dłuższego czasu lub mają niewiele lub żadnych opinii użytkowników. Podobnie jak fałszywe oprogramowanie antywirusowe, cyber przestępcy mogą tworzyć fałszywe menedżery haseł w celu kradzieży Twoich informacji.
- Twój menedżer haseł powinien być prosty w użyciu. Jeśli znajdziesz rozwiązanie zbyt skomplikowane, aby je zrozumieć, poszukaj alternatywy, która lepiej odpowiada Twoim nawykom i doświadczeniu.
- Upewnij się, że bez względu na wybrane rozwiązanie będzie ono na bieżąco aktualizowane i poprawiane, oraz że używasz zawsze najnowszej wersji.
- Menedżer haseł powinien ułatwiać wybór silnego hasła do różnych kont, w tym dawać możliwość automatycznego generowania silnych haseł i pokazać siłę haseł już wybranych.
- Menedżer haseł powinien dawać możliwość przechowywania innych poufnych danych, takich jak odpowiedzi na swoje tajne pytanie bezpieczeństwa, numery kart kredytowych itp.
- Uważaj na menedżery haseł, które używają własnych lub nieznanych technik szyfrowania, zamiast metod zgodnych

Menedżery haseł

ze standardami branżowymi. Jeżeli producent menedżera haseł chwali własne rozwiązania szyfrowania, trzymaj się z dala od takiego oprogramowania.

- Unikaj jakiegokolwiek menedżera haseł, który twierdzi, że jest w stanie odzyskać hasło główne. Oznacza to, że twórcy oprogramowania w jakiś sposób znają Twoje hasło główne, co naraża Cię na znacznie większe ryzyko.

Menedżery haseł są doskonałym rozwiązaniem na bezpieczne przechowywanie wszystkich haseł i innych poufnych danych. Jednakże, ponieważ chronią tak ważne informacje, upewnij się, że używasz silnego hasła głównego, które jest trudno odgadnąć, ale jednocześnie pozostaje łatwe do zapamiętania.

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

Nowe oblicze hasła:	http://www.securingthehuman.org/ouch/2015#april2015
Dwuskładnikowe uwierzytelnianie:	https://www.securingthehuman.org/ouch/2015#september2015
O zarządzaniu hasłami:	https://www.technologie.org.pl/artykuly/jedno-za-wszystkie-o-zarzadzaniu-haslami

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