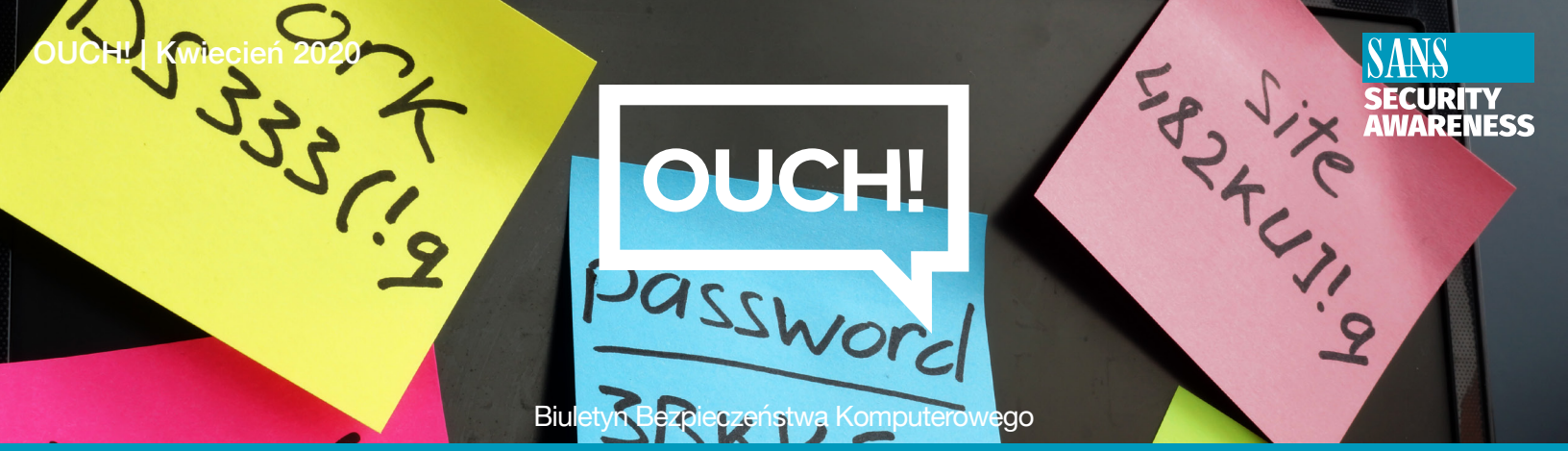

Biuletyn Bezpieczeństwa Komputerowego

Menedżer haseł

Wstęp

Jednym z najważniejszych kroków, które powinieneś podjąć w celu ochrony swojej aktywności w sieci, jest wykorzystywanie niepowtarzalnego i silnego hasła dla każdego konta oraz aplikacji, z których korzystasz. Niestety samodzielne zapamiętanie wielu unikalnych haseł może być nie lada gratką. Ponadto zdajemy sobie sprawę z tego, że ciągłe wpisywanie haseł na różnych stronach internetowych jest czasochłonne. Uciążliwe jest również wymyślanie bezpiecznych haseł czy zapamiętywanie haseł pomocniczych służących do odzyskania kont. Z pomocą przychodzą nam aplikacje/programy, które zrobią to za nas, zwane są menedżerami haseł.

Czym są menedżery haseł i jak działają

Menedżery haseł funkcjonują przechowując wszystkie hasła w bazie danych, czasami nazywanej skarbcem. Aplikacja szyfruje zawartość całej 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. W momencie logowania, menedżery haseł w sposób automatyczny i bezpieczny mogą przekazać login i hasło do konta, w którym chcesz się zalogować. Nigdy więcej nie będziesz musiał zaprzątać sobie głowy dziesiątkami haseł.

Większość menedżerów haseł ma funkcję automatycznego synchronizowania zawartości sejfu pomiędzy wieloma urządzeniami. W ten sposób po aktualizacji hasła, np. na laptopie, zmiany są synchronizowane do wszystkich urządzeń, z których korzystasz. Menedżer wykrywa, kiedy próbujesz założyć nowe konto internetowe lub zaktualizować hasło dla istniejącego konta i automatyczne aktualizuje dane w sejfie.

Menedżery haseł są przeznaczone do bezpiecznego przechowywania poufnych danych. 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 uwierzytelnianie dwuskładnikowe, zalecamy użyć jej dla hasła głównego. Upewnij się, że zapamiętałeś hasło główne. Jeśli go zapomnisz, nie będziesz w stanie uzyskać dostępu do swoich innych haseł.

Wybór menedżera haseł

Istnieje wiele menedżerów haseł na rynku. W sekcji "Źródła" udostępniamy link do strony zawierającej przegląd oprogramowania tego typu. Tymczasem, próbując znaleźć rozwiązanie dopasowane do Twoich potrzeb, miej na uwadze następujące rzeczy:

Aplikacja powinna być prosta w użyciu. Jeśli trafisz na taką, która jest zbyt skomplikowana, przetestuj inną i znajdź taką, która Ci odpowiada.

Menedżer haseł powinien współpracować ze wszystkimi Twoimi urządzeniami, z których korzystasz. Powinien także umożliwiać w prosty sposób synchronizację haseł z resztą urządzeń.

Używaj tylko znany i popularnych menedżerów haseł. Uważaj na aplikacje, które nie były aktualizowane od dłuższego czasu lub mają niewiele lub żadnych opinii użytkowników. Cyber przestępcy mogą tworzyć fałszywe menedżery haseł w celu kradzieży Twoich informacji. Bądź podejrzliwy do menedżerów haseł, w których producenci zastosowali własną lub nieznaną dotąd technikę szyfrowania.

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.

Upewnij się, że bez względu na wybrane rozwiązanie będzie ono na bieżąco aktualizowane i poprawiane, oraz że używasz zawsze najnowszej wersji.

Menedżer haseł powinien dawać możliwość przechowywania innych poufnych danych, takich jak odpowiedzi na pytania pomocnicze w przypadku odzyskiwania konta, numery kart kredytowych itp.

Zabezpieczając się na wypadek zapomnienia hasła głównego do menedżera haseł, zastanów się nad zapisaniem go na kartce i przechowywaniu go w miejscu tylko Tobie znanym np. w zamkniętej szufladzie czy sejfie.

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.

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

Redaktor gościnny

***Russell Eubanks** jest liderem w dziedzinie bezpieczeństwa informacji w Atlancie posiadającym ponad 20 lat doświadczenia, w swoim dorobku ma wiele certyfikatów bezpieczeństwa. Współpracuje z SANS Internet Storm Center i bierze udział w CIS (Critical Security Controls). Russell można znaleźć na Twitterze jako @russelleubanks lub https://www.securityeverafter.com.*

Źródła

Tworzenie haseł w prostszy sposób: http://www.sans.org/u/10Uz
Cyfrowa spuścizna: http://www.sans.org/u/10Uz
Przegląd najlepszych menedżerów haseł: https://www.wired.com/story/best-password-managers/