Komunikat IOD-y

2022 / 06 / 10

Czy warto zapisywać hasła w przeglądarce?

Czy zdarzyło Ci się zapisać hasło do konta na witrynie internetowej w pamięci przeglądarki? Niektórzy robią z przekonaniem, że jest to bezpieczne ułatwienie logowania. Inni świadomi są zagrożeń, jakie pociąga za sobą tego typu działanie, ale przez chwilę nieuwagi mogą nieświadomie skorzystać z tej możliwości. Zapisane w przeglądarce hasło może zostać wykorzystane do zalogowania się przez inną osobą, która będzie korzystać z tego samego urządzenia.

Nawet jeżeli dany sprzęt jest użytkowany tylko przez jednego użytkownika i nigdy nie ma dostępu do niego żadna inna osoba, to wciąż zapisywanie haseł nie jest dobry rozwiązaniem. Mało kto jest świadomy faktu, że dane zapisane w pamięci przeglądarki internetowej mogą być wykradzione przez cyberprzestępców.

W JAKI SPOSÓB ZAPISANE HASŁA MOGĄ ZOSTAĆ WYKRADZIONE?

Jeżeli na stronie internetowej wypełniamy formularz logowania, to przeglądarka automatycznie pyta, czy ma zapamiętać login i hasło. Jeżeli zostanie wybrana ta opcja, dane do logowania są przechowywane najczęściej w pliku SQLLite, pod nazwą „Login Data”. Znajduje się on w różnych miejscach na dysku, co uzależnione jest od używanej przeglądarki oraz od systemu operacyjnego.

Niestety oprócz domowników lub innych użytkowników sprzętu dostęp do zapisanych haseł mogą mieć również cyberprzestępcy. W tym celu korzystają oni z oprogramowania do wykradania haseł, które sprzedawane jest w Darknecie (ukrytej części Internetu, do której dostęp możliwy jest dzięki specjalnemu oprogramowaniu). Co więcej, zaobserwowano i opisano skuteczne ataki z jego użyciem. Tego typu programy są dostępne w sprzedaży od 2020 r. Co ważne, przy ich pomocy można nie wykraść tylko hasła, ale również dane kart płatniczych, pliki cookies, a także dane autouzupełniania przeglądarek. Najnowsze aplikacje umożliwiają również pozyskanie informacji z portfeli kryptowalut.

UDANY ATAK

Firma AhnLab opisała atak cyberprzestępców na pracownika podczas wykonywania pracy zdalnej. Przedsiębiorstwo świadczyło usługę VPN pracownikom świadczącym pracę z domu, co umożliwiało dostęp do sieci wewnętrznej firmy. Na swoim urządzeniu zaatakowany pracownik korzystał z funkcji zapamiętywania haseł w przeglądarce internetowej. Poprzez specjalne oprogramowanie cyberprzestępcy uzyskali dostęp do haseł ofiary, a następnie do konta jego VPN. Trzy miesiące później pozyskane konto VPN wykorzystano do włamania się do wewnętrznej sieci firmy.

W toku wyjaśnień odkryto, że komputer był użytkowany nie tylko przez pracownika, ale również przez całą jego rodzinę i nie był bezpiecznie zarządzany. Urządzenie już od dłuższego czasu było zainfekowane różnymi złośliwymi programami. Mimo, że na urządzeniu zainstalowano oprogramowanie antywirusowe, to nie wykryło ono zagrożenia. Da ataku wykorzystano program Redline Stealer. Jest to narzędzie, które pozyskuje dane uwierzytelniające zapisane w pamięci przeglądarki internetowej. Pojawiło się w 2020 r. i było rozpowszechniane przez m.in. wiadomości phishigowe, reklamy Google i programy do edycji zdjęć.

Przykładów udanych ataków nie trzeba szukać daleko. Nie tak dawno doszło do niego na naszej uczelni. Cyberprzestępcy przeprowadzili atak ransomware z użyciem danych logowania zapisanych w przeglądarce internetowej. Na szczęście dzięki szybkiej reakcji udało się udaremnić atak.

MENEDŻER HASEŁ

Tworzenie jednego hasła do wielu serwisów nie jest dobrym rozwiązaniem. Należy kierować się zasadą „jedno hasło = jedna witryna". Jednak zapamiętanie wielu haseł jest trudne. Pomocne może być więc narzędzie do zarządzania hasłami. Menedżer haseł bezpiecznie przechowuje hasła i pozwala wpisać je w panelu logowania danego serwisu na żądanie użytkownika. Hasła są przechowywane w zaszyfrowanej bazie. Narzędzie takie dostępne jest w formie aplikacji lub jako moduł wbudowany w przeglądarkę internetową. Każda popularna przeglądarka ma dostępne różne wtyczki w postaci menedżerów haseł.

Dzięki menedżerowi haseł nie musimy również sami ich wymyślać, ponieważ generuje on losowe, unikatowe i dobrej jakości hasła oraz przechowuje je w swojej bazie. Wszystkie wygenerowane hasła są zabezpieczone hasłem głównym. Dzięki menedżerowi haseł będziemy musieli pamiętać tylko to jedno hasło, a reszta pozostanie zabezpieczona. Oczywiście, o ile hasło do menadżera nie będzie trywialne.

Coraz więcej menedżerów haseł powiadamia użytkowników o wycieku haseł i potrzebie ich zmiany. Możliwe jest to dzięki temu, że twórcy programów sprawdzają bazy danych pochodzące z różnych wycieków. Dzięki temu użytkownicy mogą szybko zareagować i uchronić się przed atakiem cyberprzestępców. Niektóre z menedżerów haseł umożliwiają zapamiętywanie nie tylko loginów i haseł, ale również innych informacji. Oferują one przyswojenie m.in. danych kart płatniczych, innych danych osobowych (np. PESEL, numer dowodu / paszportu) czy nawet kodów do domofonów.

WYŁĄCZ OPCJĘ ZAPISYWANIA HASEŁ

Samo zapisywanie haseł w przeglądarce (o ile jesteś jedynym użytkownikiem komputera) nie jest niebezpieczne. Jednak staje się ogromnym zagrożeniem po zainfekowaniu urządzenia, a na to niestety nie mamy większego wpływu. Jak mawiają specjaliści od cyberbezpieczeństwa, ludzie dzielą się na tych, którzy zostali zhackowani i na tych, którzy o tym nie wiedzą. Dane do logowania wyciekają również bezpośrednio z serwisów internetowych. Można to sprawdzić na stronie https://haveibeenpwned.com/. Cyberprzestępcy wciąż rozwijają metody cyberataków, dlatego zdecydowanie lepszym rozwiązaniem jest korzystanie z menadżera haseł.

Może dojść także do sytuacji, w której przez przypadek zgodzimy się na propozycję przeglądarki, która oferuje zapamiętanie hasła. Aby się przed tym uchronić warto wyłączyć opcję proponowania zapisywania haseł. Opcja taka znajduje się w ustawieniach każdej popularnej przeglądarki.