Mesečni bilten bezbednosnih saveta za korisnike računara

OUCH!

U OVOM IZDANJU...

Menadžeri lozinki

Uvod

Jadna od najbitnijih mera koju možete da preduzmete u cilju zaštite svojih podataka je da koristite jedinstvenu i jaku lozinku za svaki od svojih naloga. Nažalost, većina od nas ima toliko mnogo naloga da je prosto nemoguće zapamtiti sve svoje lozinke. Jednostavno rešenje predstavlja korišćenje menadžera lozinki, ili drugim imenom trezor lozinki. To su specijalizovane aplikacije dizajnirane za bezbedno čuvanje akreditiva za prijavljivanje (korisničkih imena i lozinki). Štaviše, takođe mogu da pojednostave prijavljivanje na vebsajtove, mobilne ili konvencionalne aplikacije.

Gost urednik

Lenny Zeltser je fokusiran na zaštitu IT operacija klijenata u NCR Corp i obuku profesionalaca za bezbednosti informacija pri SANS institutu. Lenny je aktivan na Twitter-u kao **@lennyzeltser** I objavljuje publikacije na **zeltser.com**.

Kako funkcionišu menadžeri lozinki

Menadžeri lozinki funkcionišu kao digitalni sef, bezbedno čuvaju i skladište vaša korisnička imena, lozinke i druge osetljive informacije. Kada neki vebsajt zahteva vaše akreditive za prijavljivanje, menadžer lozinki može da automatski unese odgovarajuće podatke i da vas bezbedno prijavi na odgovarajući vebsajt. Na takav način je jednostavno imati na stotine jedinstvenih, jakih lozinki, pošto ne morate da ih sami pamtite.

Menadžeri lozinki čuvaju detalje u bazi podataka koja se ponekad naziva trezor. Sadržaj trezora je enkriptovan (šifriran) i zaštićen glavnom lozinkom koja je poznata samo vlasniku. Kada je potrebno da se koriste neki akreditiv za prijavljivanje, na primer da se prijavite na svoj on-line bankovni račun, potrebno je samo da unesete svoju glavnu lozinku u svoj menadžer lozinki da bi ste otključali trezor.

Neki menadžeri lozinki čuvaju trezor na lokalnom sistemu ili pametnom telefonu, dok drugi za to koriste specijalizovan vebsajt koji je održavan od strane samog proizvođača menadžera lozinki. Osim toga, većina menadžera lozinki uključuje mogućnost automatske sinhronizacije sadržaja trezora između više uređaja odobrenih od strane vlasnika. Na takav način svaki put kada ažurirate lozinku na svom laptopu, promene će biti sinhronizovane sa vašim pametnim telefonom, tabletom

Menadžeri lozinki

ili drugim računarima koje koristite. Bez obzira na to gde se čuva baza podataka, da bi se menadžer lozinki koristio, aplikacija menadžera lozinki mora biti instalirana na sistemu ili uređaju koji se koristi.

Kada prvi put podešavate menadžer lozinki, potrebno je da ručno uneste ili uvezete svoja korisnička imena i lozinke. Nakon toga, menadžer lozinki sam može da detektuje kada pokušate da se registrujete na novi on-line nalog ili ažurirate lozinku za postojeći i na osnovu toga ažurira trezor. To je moguće zato što se većina menadžera lozinki integriše sa Internet pretraživačima, a ta integracija i omogućava automatsko prijavljivanje na vebsajtove.

Menadžeri lozinki predstavljaju jednostavan način da bezbedno čuvate i koristite sve svoje različite lozinke.

Menadžeri lozinki su dizajnirani da bezbedno čuvaju osetljive podatke. Međutim, od izuzetne važnosti je da glavna lozinka koja se koristi za zaštitu sadržaja trezora bude jaka i veoma teška za druge da je pogode. U stvari preporučljivo je da za glavnu lozinku koristite propusnu frazu, možda i najjači tip lozinke koji postoji. Ako menadžer lozinki podržava verifikaciju iz dva koraka, obavezno je koristite za svoju glavnu lozinku. Na kraju budite sigurni da svoju glavnu lozinku ne koristite za bilo koji drugi sistem ili nalog. Na takav način, čak i ako hakeri uspeju da kopiraju vaš trezor, neće biti u mogućnosti da pogode lozinku i pristupe sadržaju. Konačno, budite sigurni da ste dobro zapamtili svoju glavnu lozinku, pošto u slučaju da je zaboravite, nećete moći da pristupite svim ostalim lozinkama.

Kako izabrati odgovarajući menadžer lozinki

Na tržištu postoji veliki izbor besplatnih i komercijalnih menadžera lozinki. Kada budete odlučivali koji od njih je najbolji izbor za vas, imajte sledeće na umu:

- Proverite da li će menadžer lozinki raditi na svim uređajima koje ćete koristiti za pristup trezoru, i da sinhronizacija funkcioniše na svim uređajima.
- Koristite samo renomirane i pouzdane menadžere lozinki. Budite obazrivi prema proizvodima koji su novi na tržištu, ili imaju malo ili nemaju komentara korisnika. Kao što postoje lažni antivirus programi, tako je moguće i napraviti menadžere lozinki koji će da kradu podatke korisnika.

Menadžeri lozinki

- Rešenje koje izaberete treba da bude jednostavno za korišćenje. Ako mislite da je previše složeno, bolje je da nađete alternativu, koja više odgovara vašem stilu i veštinama.
- Ma koje rešenje da odaberete, budite sigurni da se redovno ažurira i da koristite najnoviju verziju.
- Menadžer lozinki bi trebalo da omogući lak izbor jakih lozinki za različite naloge, uključujući i automatsko generisanje jakih lozinki, kao i procenu kompleksnosti/jačine izabrane lozinke.
- Menadžer lozinki bi trebalo da omogući čuvanje drugih osetljivih podataka, kao što su odgovori na tajna bezbednosna pitanja ili kreditne kartice.
- Budite oprezni ako menadžer lozinki za enkripciju trezora koristi nekonvencionalne ili nepoznate tehnike enkripcije, umesto industrijskih standarda. Izbegavajte proizvode gde proizvođač tvrdi da su sami razvili rešenje za enkripciju.
- Izbegavajte bilo koji menadžer lozinki gde proizvođač tvrdi da mogu da povrate vašu glavnu lozinku u slučaju da ste je zaboravili. To znači da oni znaju vašu glavnu lozinku, a samim tim i da je rizik kojem se izlažete dosta veći.

Menadžeri lozinki su veoma moćno rešenje za bezbedno čuvanje svih vaših lozinki i drugih osetljivih podataka. Međutim, pošto se koriste za čuvanje izuzetno važnih podataka, budite sigurni da koristite jaku glavnu lozinku koja nije samo teška za nekog da je pogodi, već i laka za vas da je zapamtite.

Saznaj Više

Prijavi se na OUCH! mesečni bilten bezbednosnih saveta za korisnike računara, pristupi prethodnim OUCH! izdanjima i saznaj više o SANS rešenjima u vezi svesnosti bezbednosti informacija na našoj internet prezentaciji http://www.securingthehuman.org/.

Dodatne informacije

Propusne fraze:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_se.pdf
Verifikacija iz dva koraka:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201509_se.pdf
5 vodećih menadžera lozinki:	http://lifehacker.com/5529133/five-best-password-managers
SANS tip dana:	http://www.sans.org/tip_of_the_day.php

Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Preveo: Nenad Varinac