SANS SECURING THE HUMAN Telekom Srbija

OUCH! | Septembar, 2017

Mesečni bilten za podizanje svesti o bezbednosti informacija

OUCH!

U OVOM BROJU...

Menadžeri lozinki

Uvod

Jedan od najvažnijih koraka koje možete preduzeti kako biste se zaštitili na Internetu je da koristite jedinstvenu i jaku lozinku za svaki vaš nalog i aplikaciju. Nažalost, skoro da je nemoguće da zapamtite sve vaše različite lozinke za sve naloge koje posedujete. Zbog toga mnogo ljudi koristi istu lozinku za više naloga. Nažalost, upotreba iste lozinke za različite naloge je opasna zato što kada neko otkrije vašu lozinku, onda on može pristupiti svim vašim nalozima koji koriste tu lozinku. Jednostavno rešenje je korišćenje menadžera lozinki, koji se ponekad nazivaju i sefovi za lozinke (eng. password vault). To su programi koji bezbedno čuvaju sve vaše lozinke, čineći lakim korišćenje različitih lozinki za svaki vaš nalog. Menadžeri lozinki pojednostavljuju čuvanje lozinki, jer umesto da pamtite sve vaše lozinke morate da zapamtite samo glavnu (master) lozinku vašeg menadžera lozinki.

Gost urednik

Kris Kristianson je konsultant za informacionu bezbednost iz Kalifornije, iza sebe ima 20 godina iskustva i brojne tehničke sertifikate. Prezentovao je na raznim konferencijama i bio je saradnik u mnoštvu stručnih članaka. Krisa možete pronaći na Tviteru **@cchristianson** i na veb stranici **https://ismellpackets.com**.

Kako rade menadžeri lozinki

Menadžeri lozinki rade tako što čuvaju sve vaše lozinke u bazi podataka, koja se naziva još i sef. Menadžer lozinki šifruje sadržaj baze i štiti ga pomoću glavne lozinke koje znate samo vi. Kada hoćete da koristite vašu lozinku, npr. da biste se prijavili na vaš nalog za onlajn bankarske usluge ili elektronsku poštu, potrebno je samo da unesete vašu glavnu lozinku u menadžer lozinki kako biste otključali bazu (sef). U dosta slučajeva menadžer lozinki će automatski izvući vašu lozinku i prijaviti se na vaš nalog na bezbedan način. Na ovaj način postaje jednostavno da imate stotine jedinstvenih, jakih lozinke, pošto ne morate da ih pamtite.

Neki menadžeri lozinki čuvaju bazu sa lozinkama na vašem računaru ili mobilnom uređaju, dok drugi koriste Cloud za čuvanje. Pored toga, većina menadžera lozinki uključuje mogućnost automatske sinhronizacije vaše baze sa lozinkama na više različitih uređaja koje ste vi odobrili. Na ovaj način kada ažurirate lozinku na vašem laptopu, te promene će se sinhronizovati na sve vaše uređaje. Bez obzira gde se čuva baza sa lozinkama, da biste koristili menadžer lozinki, morate

Menadžeri lozinki

da instalirate aplikaciju menadžera lozinki na vašem uređaju ili sistemu.

Kada prvi put konfigurišete menadžera lozinki, morate ručno da unesete ili uvezete svoje naloge za prijavu i lozinke. Nakon toga, menadžer lozinki može da detektuje kada pokušavate da registrujete novi nalog ili da promenite lozinku na postojećem i da u skladu sa tim automatski ažurira vašu bazu sa lozinkama. Ovo je moguće jer većina menadžera lozinki rade ruku pod ruku sa vašim veb pregledačem. Ova integracija takođe omogućava menadžerima lozinki da vas automatski prijavljuju na veb sajtove.

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

Od izuzetne važnosti je da glavna (master) lozinka koju koristite za zaštitu sadržaja menadžera lozinki bude jaka i veoma teška za pogađanje. U stvari, preporučuje se da glavnu lozinku napravite kao pristupnu frazu, koja je jedna od najjačih vrsta lozinki. Ukoliko vaš menadžer lozinki podržava verifikaciju iz dva koraka koristite je za vašu glavnu lozinku. Na kraju, budite sigurni da ste dobro zapamtili vašu glavnu lozinku. Ako je zaboravite, nećete moći da pristupite bilo kojoj drugoj lozinki koje čuvate u menadžeru lozinki.

Izbor menadžera lozinki

Postoji veliki izbor menadžera lozinki. U odeljku Dodatne informacije dati su linkovi na neke preglede menadžera lozinki. U međuvremenu, dok budete tražili najbolje rešenje za vas, vodite računa o sledećem:

- Vaš menadžer lozinki treba da bude jednostavan za korišćenje. Ako ste pronašli rešenje koje je suviše složeno, pronađite drugo koje više odgovara vašem načinu rada i vašim veštinama.
- Menadžer lozinki treba da radi na svim uređajima na kojima treba da upotrebljavate lozinke. Takođe, trebalo bi da vam bude jednostavna sinhronizacija lozinki između svih vaših uređaja.
- Koristite samo dobro poznate i pouzdane menadžere lozinki. Budite obazrivi prema proizvodima koji su novi na tržištu ili o kojima ima malo povratnih informacija korisnika. Sajber kriminalci mogu da naprave lažne menadžere lozinki i tako vam ukradu informacije. Takođe, budite veoma obazrivi u slučajevima kada proizvođači tvrde da su sami razvili rešenje za enkripciju.

Menadžeri lozinki

- Izbegavajte bilo koji menadžer lozinki za koji proizvođač tvrdi da može da vam oporavi vašu glavnu lozinku. Ovo znači da oni znaju vašu glavnu lozinku, a samim tim je rizik kojem se izlažete dosta veći.
- Uverite se, nevezano za rešenje koje ste odabrali, da proizvođač kontinuirano ažurira i izdaje ispravke za menadžera lozinki i postarajte se da uvek koristite najnoviju verziju.
- Menadžer lozinki treba da podržava mogućnost da automatski generiše jake lozinke za vas i da vam pokazuje jačinu lozinke koju ste odabrali.
- Menadžer lozinki treba da vam pruži mogućnost da sačuvate i druge osetljive podatke, kao što su odgovori na vaša tajna bezbednosna pitanja ili podaci o kreditnim karticama.

Menadžeri lozinki su odličan način za bezbedno čuvanje svih vaših lozinki i drugih osetljivih podataka. Međutim, pošto oni čuvaju informacije od takve važnosti, postarajte se da koristite jedinstvenu i jaku glavnu lozinku koja ne samo da je teška napadaču za pogađanje, već je i vama laka za pamćenje.

Saznajte više

Prijavite se na OUCH! mesečni bilten za podizanje svesti o bezbednosti informacija namenjen svima, pročitajte prethodne brojeve OUCH!-a i saznajte više o SANS-ovim rešenjima za unapređenje svesti o bezbednosti informacija na našoj internet prezentaciji securingthehuman.sans.org/ouch/archives.

Dodatne informacije

Najbolji menadžeri lozinki u 2017:	https://www.pcmag.com/article2/0,2817,2407168,00.asp
Pristupne fraze:	https://securingthehuman.sans.org/ouch/2017#april2017
Verifikacija iz dva koraka:	https://www.securingthehuman.org/ouch/2015#september2015
Zaštitite vaš nalog:	https://www.lockdownyourlogin.org/
SANS bezbednosni savet dana:	https://www.sans.org/tip-of-the-day

Redakcija: Walt Scrivens, Phil Hoffman, Кэти Клик, Cheryl Conley
Preveli: Dragan Ristić i Gordana Živanović