Kuukausittainen uutiskirje tietoturvatietoisuuteen liittyvistä aiheista

OUCH!

Tässä numerossa…

Salasanojen hallintaohjelma

Yleiskatsaus

Yksi parhaista tavoista itsesi suojaamiseen verkossa, on käyttää ainutlaatuista, vahvaa salasanaa ja joka palvelussa erilaista salasanaa. Valitettavasti nykyinen tilien suuri määrä tekee edellä mainitun hyvin hankalaksi ja jopa mahdottomaksi ja tämän vuoksi monet käyttävät joka palvelussa samoja, liian huonoja salasanoja. Jos haitallinen taho saa käsiinsä tämän yhden salasanan, niin hänellä on tämän jälkeen pääsy kaikkiin tileihisi. Helppo ratkaisu tähän ongelmaan on käyttää salasanojen hallintaohjelmaa. Nämä ohjelmat on suunniteltu salasanojen tietoturvalliseen säilyttämiseen mahdollistaen eri salasanan käyttämisen jokaiseen palveluun. Ohjelman käyttäminen on helppoa, koska monien salasanojen muistamisen sijaan, käyttäjän pitää muistaa vain yksi salasana, jolla hallintaohjelman saa auki.

Vierastoimittaja

Chris Christianson on Kalifornialainen tietoturvakonsultti, jolla on 20 vuoden kokemus tietoturvasta ja lukuisia alan sertifikaatteja. Hän on ollut puhujana useissa tietoturvakonferensseissa ja osallistunut useisiin alan artikkelien kirjoittamiseen. Löydät hänet Twitteristä **@cchristianson** ja **https://ismellpackets.com**.

Miten salasanojen hallintaohjelmat toimivat

Salasanojen hallintaohjelma toimii tallentamalla kaikki salasanasi tietokantaan, jota jotkut valmistajan kutsuvat Holviksi (’Vault’). Ohjelma salakirjoittaa ja suojaa tietokannan pääsalasanalla jonka käyttäjä määrittelee. Kun tarvitset salasanaa, kirjoitat hallintaohjelman pääsalasanan ja ohjelma avaa tietokannan käyttöösi. Monissa tapauksissa ohjelmat myös pystyvät hakemaan salasanan automaattisesti ja tietoturvallisesti kun kirjaudut palveluihin laitteellasi. Hallintaohjelman ansiosta pystyt käyttämään yksinkertaisesti satoja erilaisia, vahvoja salasanoja muistamatta niitä ulkoa.

Ohjelmat tallentavat valmistajasta riippuen tietokantasi sisällön joko vain sinun laitteesi muistiin tai myös valmistajan pilvessä sijaitsevaan tietokantaan, jolloin ohjelma tarjoaa yleensä myös synkronointimahdollisuutta eri laitteidesi välillä. Tässä tapauksessa päivittäessäsi salasanatietosi esim. mobiililaitteellasi, päivittyvät tiedot myös saman ohjelman työpöytäversiolle, tabletille tai mille tahansa muulle laitteelle jolle olet ohjelman aktivoinut. Riippumatta siitä mihin tiedot ovat tallennettu, sinun tulee asentaa kaikille haluamillesi laitteille kyseinen salasanojen hallintaohjelma.

Salasanojen hallintaohjelma

Kun otat salasanan hallintaohjelmaa käyttöön ensimmäistä kertaa, sinun pitää manuaalisesti lisätä kaikki tunnuksesi ja salasanasi sovellukseen tai tuoda ne jostakin muualta. Tämän jälkeen ohjelma huomaa automaattisesti kun rekisteröidyt uuteen palveluun, tai kun päivität olemassa olevia tietoja ja pystyy jopa päivittämään tiedot sovellukseen automaattisesti. Salasanahallintasovellukset integroituvat yleensä selaimeesi ja tämän ansiosta tietojen päivittäminen ja lisääminen onnistuvat helposti. Tämän integraation ansiosta sovellukset pystyvät usein kirjaamaan sinut automaattisesti sisään palveluihin.

Sanasanojen hallintaohjelmalla hallitset helposti ja tietoturvallisesti kaikkia eri palveluiden salasanojasi.

On äärimmäisen tärkeää, että valitset laadukkaan pääsalasanan ohjelmaan, koska sillä suojataan kaikki muut salasanasi. On suositeltavaa, että pääsalasana muodostetaan käyttämällä salasanalauseketta, jonka avulla saat tehtyä salasanasta erittäin laadukkaan. Jos salasanan hallintaohjelma tukee kaksivaiheista tunnistautumista, ota myös se käyttöön. Varmista myös, että et käytä sovelluksen pääsalasanaa missään muualla, tällöin tietokantasi pysyy turvassa, vaikka tietosi onnistuttaisiin hakkeroimaan. Älä unohda pääsalasanaasi, sillä jos et muista sitä et todennäköisesti pääse enää käsiksi tietoihisi.

Oikean ohjelman valitseminen

Markkinoilla on monia sekä ilmaisia että maksullisia salasanasovelluksia joista valita. Olemme listanneet joitakin vaihtoehtoja uutiskirjeen lopussa. Kun valitset sinulle sopivinta ohjelmaa, ota huomioon ainakin seuraavat asiat:

- Ohjelman pitää olla helppokäyttöinen juuri sinulle. Jos ohjelma on mielestäsi liian monimutkainen, yritä etsiä toinen, sinulle paremmin sopiva.
- Varmista, että valitsemasi ohjelma toimii kaikilla käyttämiesi laitteiden käyttämillä käyttöjärjestelmillä. Ohjelman pitäisi myös tarjota helppo synkronointi näiden laitteiden välillä.
- Käytä vain tunnettuja ja yleisesti luotettavia sovellustoimittajia. Suhtaudu varauksella ohjelmiin, jotka ovat uusia markkinoilla tai joista ei löydy riittävästi käyttäjien kommentteja. Hakkerit saattavat esim. luoda omia sovelluksiaan käyttäjien tietojen keräämiseksi. Suhtaudu varauksella sovelluksiin jotka käyttävät tuntemattomia tai outoja salakirjoitusteknologioita. Ohjelman tulisi käyttää alan johtavia ja tunnettuja teknologioita ja jos toimittaja kertoo kehittäneensä oman, tällaista kannattaa lähtökohtaisesti välttää.

Salasanojen hallintaohjelma

- Vältä ohjelmia jotka lupaavat palauttaa hukatun tai unohdetun pääsalasanan, tämä käytännössä tarkoittaa, että toimittajalla on pääsy sinun salasanaasi, joka vaarantaa tietosi.
- Mitä tahansa ohjelmaa käytätkin, varmista, että toimittaja päivittää ohjelmaa säännöllisesti ja että käytät aina viimeisintä versiota.
- Ohjelman pitäisi mahdollistaa laadukkaiden salasanojen helppo luominen, sisältäen mm. pituusvaatimukset ja erikoismerkkien käytön.
- Ohjelman pitäisi mahdollistaa myös muiden luottamuksellisten tietojen, kuten luottokorttinumeroiden tallentamisen.

Salasanojen hallintasovelluksen käyttö on erittäin hyvä ratkaisu salasanojesi ja muiden tietojesi suojaamiseen. Koska ohjelma suojaavat tärkeimpiä tietojasi, varmista että pääsalasanasi on tarpeeksi laadukas ja että tuntemattoman on mahdotonta arvata sitä, mutta sinun on silti helppo muistaa se.

LUE LISÄÄ

Liity kuukausittaisen OUCH! tietoturvatietoisuus-uutiskirjeen postituslistalle, lue OUCH! arkistoja ja tutustu SANS-järjestön muihin tietoturvatietoisuuteen liittyviin ratkaisuihin osoitteessa securingthehuman.sans.org/ouch/archives.

Uutiskirjeen kääntäjä Kirill Filatov (KTM) on GIAC-sertifioitu tietoturvaa rakastava, kokenut IT-ammattilainen. Kirill turvaa tällä hetkellä Nebula Oy:n asiakkaiden liiketoimintaa konsultoimalla ja kehittämällä asiakkaiden tietoturvaviitekehyksiä ja toimintamalleja.

Lähteet

2017 parhaat salasanojen hallintaohjelmat:	https://www.pcmag.com/article2/0,2817,2407168,00.asp
Salasanalausekkeet:	https://securingthehuman.sans.org/ouch/2017#april2017
Kaksivaiheinen tunnistautuminen:	https://www.securingthehuman.org/ouch/2015#september2015
Lock Down Your Login:	https://www.lockdownyourlogin.org/
SANS päivän tietoturvavinkki:	https://www.sans.org/tip-of-the-day

Lisenssi

 Toimitus: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley Käännös suomeksi: Kirill Filatov, Senior Security Consultant, Nebula Oy