SANS SECURITY AWARENESS

OUCH! | Joulukuu 2017

Kuukausittainen uutiskirje tietoturvatietoisuuteen liittyvistä aiheista

OUCH!

Tässä numerossa…

- **Salasanat**
- **Mikä on kaksivaiheinen tunnistautuminen**
- **Miten se toimii**

Kaksivaiheinen tunnistautuminen

Yleiskatsaus

Vierastoimittaja
Tiffany Schoenike kampanjapäällikkönä National Cyber Security Alliance-yhdistyksessä (**@staysafeonline**). Vuonna 2016, Tiffany kehitti yhdessä Valkoisen talon, Yhdysvaltojen hallinnon ja alan johtavien asiantuntijoiden kanssa ”Lock Down Your Login, a STOP. THINK. CONNECT.™”-kampanjan liittyen kaksivaiheiseen tunnistautumisen.

Autentikointi eli käyttäjän tunnistaminen on yksi tietoturvan perusprosesseista ja on erittäin tärkeässä roolissa tietojesi ja tiliesi suojaamisessa. Et välttämättä ole koskaan tullut ajatelleeksi, mutta jokaisella meillä on kolme eri keinoa autentikoida itsensä. Jotain mitä tiedät, esim. salasanasi, jotain mitä sinulla on, esim. ajokortti ja osa jotain mitä itse olet, esim. sormenjälkesi. Jokaisessa näissä autentikointitavassa on omat hyvät ja huonot puolensa. Yleisin autentikointitapa on salasana, eli jotain mitä tiedät. Valitettavasti pelkkien salasanojen käyttäminen on vuosien varrella osoittautunut jatkuvasti turvattomammaksi. Tässä uutiskirjeessä kerromme miten voit suojata itsesi paremmin ja varmistaa autentikointisi kaksivaiheisen kirjautumisen avulla.

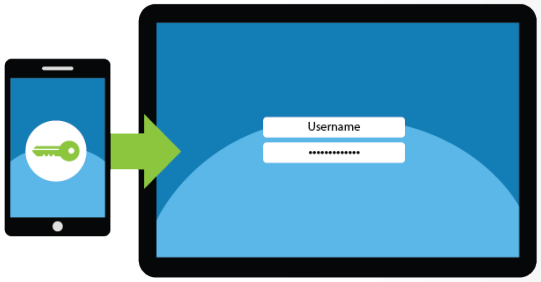
Pelkät salasanat eivät enää riitä

Salasana todistaa sen kuka olet perustuen johonkin mitä vain sinä tiedät, mutta jos joku muu saa salasanasi käsiinsä tai arvaa sen, tämä henkilö pystyy esittämään sinua ja pääsemään käsiksi tietoihisi. Tämän vuoksi on suositeltavaa käyttää salasanojen muodostamiseen salasanalausekkeita, käyttää eri salasanaa joka palvelussa ja pitää hyvää huolta salasanoista. Vaikka nämä ohjeet ovat edelleen erittäin päteviä, salasanoja ei tästä huolimatta enää pidetä kovin turvallisena. Onneksi on olemassa helppo ja nopea keino, jolla salasanojen ja tämän myötä tiliesi turvallisuutta pystyy tehostamaan merkittävästi – keino on nimeltään kaksivaiheinen tunnistautuminen.

Kaksivaiheinen tunnistautuminen

Mitä on kaksivaiheinen tunnistautuminen

Kaksivaiheinen tunnistautuminen (myös monivaiheinen tunnistautuminen, “two-step verification” tai “2FA”) on paljon vahvempi tunnistautumistapa kuin pelkkien salasanojen käyttäminen. Perusperiaate on se, että tunnistautumiseen vaaditaan useampi kuin yksi tunnistautumistapa. Pankkiautomaatin käyttäminen on hyvä esimerkki kaksivaiheisesta tunnistautumisesta. Ennen kuin voit nostaa rahaa automaatilta, sinut tunnistetaan kahdella eri tavalla, luottokortilla (jotain mitä sinulla on) ja PIN-koodilla (jotain mitä tiedät). Vaikka hukkaisit korttisi, rahasi ovat silti tallessa. Kukaan ei pysty nostamaan kortillasi rahaa ilman PIN-koodiasi. Vastaavasti, vaikka joku tietäisi PIN-koodisi, niin ilman korttiasi hän ei tee sillä mitään. Käyttämiseen vaaditaan aina sekä kortti että PIN, sama periaate tekee kaksivaiheisesta tunnistautumisesta huomattavasti turvallisemman.



Suojaa tunnuksesi kaksivaiheisen tunnistautumisen avulla aina kun mahdollista, se on yksi tehokkaimmista keinoista tietoturvasi parantamiseksi.

Miten se toimii

Monet johtavat pankit, sähköpostit ja sosiaalisen median sivustot tarjoavat palveluidensa käyttöön kaksivaiheista tunnistautumista ja useimmat näistä mahdollistavat ominaisuuden käyttöönoton hyvin helposti. Kun otat ominaisuuden käyttöön, se toimii yleensä seuraavalla tavalla: kirjaudut ensin palveluun normaaleilla tunnuksillasi kuten tähänkin asti. Tämä on ensimmäinen vaihe kaksivaiheisuudesta – jotain mitä tiedät. Tämän jälkeen tarvitset uniikin koodin joka yleensä toimitetaan puhelimeesi. Tämä on kaksivaiheisuuden toinen vaihe – jotain mitä sinulla on, eli puhelimesi. Syötät tämän koodin palveluun, kirjaudut sisään normaalisti ja tilisi on suojattu hyvin vahvasti.

Kaksivaiheinen tunnistautuminen

Voit myös vastaanottaa edellä mainitun koodin erilliseen sovellukseen joka kehittää jatkuvasti uusiutuvia koodeja turvallisuutesi varmistamiseksi. Sovelluksen käyttö lisää turvallisuutta entisestään, kun koodeja ei tarvitse lähettää viestinä. Lisäksi sovelluksen avulla pystyt kirjautumaan palveluihin myös silloin jos puhelimesi ei ole verkossa.

Vaikka kaksivaiheisen tunnistautumisen käyttö vaikuttaa alussa hankalalta, henkilökohtaiset tietosi tulevat olemaan huomattavan paljon paremmin suojattuja sitä käytettäessä. Älä odota siihen, että joudut hakkeroinnin uhriksi, vaan suojaa tunnuksesi jo nyt kaksivaiheisen tunnistautumisen avulla kaikissa palveluissa jotka sen mahdollistavat.

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

Salasanalausekkeet:	https://securingthehuman.sans.org/ouch/2017#april2017
Kaksivaiheista tunnistautumista tukevat palvelut:	https://twofactorauth.org
Stop|Think|Connect:	https://www.lockdownyourlogin.org
Googlen kaksivaiheinen tunnistautuminen:	http://www.google.com/landing/2step/

Lisenssi