Kuukausittainen uutiskirje tietoturvatietoisuuteen liittyvistä aiheista

OUCH!

Tässä numerossa…

- **Yleiskatsaus**
- **Salasanat**
- **Kaksivaiheinen tunnistautuminen**

Kaksivaiheinen tunnistautuminen

Yleiskatsaus

Autentikointi eli käyttäjän tunnistaminen on yksi tietoturvan perusprosesseista ja yksi tärkeimpiä osuuksia tietojesi suojaamisessa. Vahvalla tunnistautumisella pyritään varmistamaan, että vain sinä pääset käsiksi sähköposteihisi, valokuviisi, pankkitiliisi ja muihin tietoihisi. On kolme eri tapaa tunnistaa käyttäjä: jotain mitä käyttäjä on (esim. sormenjälki), jotain mitä vain käyttäjä tietää (esim. salasana) ja jotain mitä käyttäjällä on (esim. ajokortti). Jokaisessa näistä on huonot ja hyvät puolensa. Yleisin tapa tunnistaa käyttäjä on jotain mitä käyttäjä tietää, yleisimmin salasana. Tässä uutiskirjeessä kerromme miten voit tehostaa suojausta kaksivaiheisen tunnistautumisen avulla. Tämä on huomattavasti tietoturvallisempi tapa tunnistaa käyttäjä kuin pelkkä salasana, mutta samalla erittäin helppokäyttöinen. Ymmärtääksemme kaksivaiheisen tunnistautumisen periaatteet, meidän tulee aloittaa salasanoista.

Vierastoimittaja

Keith Palmgrenilla on yli 30 vuoden kokemus tietoturvasta. Hän toimii kouluttajana SANS:lla ja on kirjoittanut materiaalit SANS SEC301-tietoturvan alkeet kurssia varten. Kun Keith ei ole opettamassa, hän keskittyy konsultointiin ja kirjoitusprojekteihin. Voit seurata häntä Twitterissä **@kpalmgren**.

Salasanat

Salasanoja käytetään yleisimmin käyttäjien tunnistamiseen, mutta salasanojen yleisyys on samalla niiden suurin ongelma. Jos joku onnistuu arvaamaan tai muuten saamaan salasanasi käsiinsä, he pystyvät esittämään sinua ja pääsemään käsiksi kaikkiin tietoihin, joita kyseinen salasana suojaa. Tämän vuoksi on erittäin tärkeää suojata salasanasi hyvin ja käyttää laadukkaita, joka palvelussa erilaisia salasanoja. Nämä ohjeet pitävät edelleen paikkaansa, mutta hyvistä käytännöistä huolimatta salasanat eivät enää täytä tämän päivän tietoturvavaatimuksia. Hakkereiden käyttämät uusimmat teknologiat mahdollistavat laadukkaidenkin salasanojen murtamisen. Sen sijaan tarvitaan helppo, tietoturvallisempi tapa tunnistautumiseen, ja kaksivaiheinen tunnistautuminen ratkaisee suurimmat haasteet.

Kaksivaiheinen tunnistautuminen

Kaksivaiheinen tunnistautuminen (two-step verification, two-factor authentication tai 2FA) on salasanoja varmempi tapa tunnistaa käyttäjä. Perusperiaate on se, että tunnistautumiseen vaaditaan useampi kuin yksi tunnistautumistapa. Pankkiautomaatin käyttäminen on hyvä esimerkki kaksivaiheisesta tunnistautumisesta. Ennen kuin voit nostaa rahaa

© SANS Institute 2015

Kaksivaiheinen tunnistautuminen

Otto-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, koska PIN-koodisi ei ole heidän tiedossaan (ellet ole kirjoittanut sitä korttiisi, mikä ei ole kovin hyvä idea). Vastaavasti, vaikka joku tietäisi PIN-koodisi, niin ilman korttiasi hän ei tee sillä mitään. Käyttämiseen vaaditaan aina sekä kortti että PIN, mikä tekee kaksivaiheisesta tunnistautumisesta huomattavasti turvallisempaa.

Käytä kaksivaiheista tunnistautumista aina kun mahdollista, se on yksi varmimpia tapoja suojata tietosi.

Kaksivaiheisen tunnistautumisen käyttäminen

Kaksivaiheinen tunnistautuminen konfiguroidaan aina järjestelmäkohtaisesti ja jokaiselle tilille erikseen, mutta monet verkkopalvelut tarjoavat sitä nykyisin käyttäjälle helpolla tavalla. Google on maailman johtavimpia kaksivaiheisen tunnistautumisen tarjoajia. Koska Google tarjoaa käyttäjilleen monia erilaisia globaaleja, suosittuja ilmaispalveluita, kohdistuu sen tarjoamiin palveluihin myös paljon kyberhyökkäyksiä. Tämän vuoksi Googlella tunnistettiin tarve kehittyneemmälle käyttäjätilien suojaamiselle ja Google oli ensimmäisiä laajalle joukolle kaksivaiheista tunnistautumista tarjonnut yritys. Tällä hetkellä heidän palvelunsa ulottuu käytännössä kaikkiin Googlen tarjoamiin ja muutaman muun tarjoajan palveluihin. Kun ymmärrät miten Googlen kaksivaiheinen tunnistautuminen toimii, ymmärrät miten se toimii muissakin palveluissa, kuten Facebookissa, Twitterissä ja Applen sovelluksissa.

Ensimmäisenä sinun pitää aktivoida kaksivaiheinen tunnistautuminen Google-tililtäsi ja rekisteröidä palveluun puhelinnumerosi. Tämän jälkeen kirjaudut tilillesi salasanalla (jotain mitä tiedät) kuten ennenkin, jonka jälkeen saat Googlelta tekstiviestin, jossa on lyhyt numerosarja. Aivan kuten salasanankin, syötät tämän numerosarjan seuraavaan kenttään, tämä on kaksivaiheisuuden toinen vaihe. Tarvitset kirjautumiseen siis sekä salasanasi, että puhelimeen tulevan koodin, joten vaikka salasanasi onnistuttaisiin murtamaan tai se häviäisi, niin tilillesi ei päästä sisään ilman koodia. Puhelimeesi tuleva koodi ei turvallisuussyistä ole koskaan kahta kertaa sama.

Tekstiviestikoodien lisäksi voit käyttää myös toista vaihtoehtoa kirjautumiseen. Google ja muut tarjoajat tarjoavat mahdollisuuden saada kirjautumiskoodi suoraan puhelimeesi asennettavaan sovellukseen. Tämä sovellus generoi

© SANS Institute 2015

Kaksivaiheinen tunnistautuminen

kirjautumiskoodin sinulle myös silloin kun et ole puhelinverkossa ja lisäksi voit lisätä sovellukseen useita tilejä. Koska koodia ei lähetä sinulle, sen kaappaaminen on myös hankalampaa.

Muista, että kaksivaiheinen tunnistautuminen ei ole käytössä vakiona palveluita käyttöönotettaessa, vaan sinun pitää aktivoida se käyttöön itse. Vaikka kaksivaiheisen tunnistautumisen käyttöönotto vaikuttaa työläältä, suosittelemme sen käyttöä aina kun mahdollista, erityisesti kriittisissä palveluissa kuten sähköpostissa ja tiedostojen tallentamisessa. Kaksivaiheinen tunnistautuminen tekee tiliesi käyttämisestä merkittävästi tietoturvallisempaa.

LUE LISÄÄ

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

Elisa Appelsiini on korkean osaamisen IT-palvelutalo. Noin 400 IT-alan ammattilaisen voimin tuotamme monipuolisia ja tietoturvallisia tietotekniikkaan liittyviä pilvi-, työn tuottavuus-, konsultointi- ja ulkoistuspalveluja. Kehitämme myös asiakkaidemme liiketoimintaa tukevia sovelluksia ja tuotteita. Toimintamme perustuu syvään teknologiaosaamiseen ja aidosti asiakaslähtöiseen toimintaan.

Elisa Appelsiini is a comprehensive IT service provider owned by the leading provider of communications services in Finland, Elisa. Elisa Appelsiini helps its customers to enhance their business and increase competitiveness by offering high-end IT services in consulting, cloud, integration, software development and outsourcing.

Lähteet

Salasanalausekkeet:	http://www.securingthehuman.org/ouch/2015#april2015
Kaksivaiheisuutta tukevat palvelut:	https://twofactorauth.org
Stop|Think|Connect:	http://stopthinkconnect.org/2stepsahead
Googlen kaksivaiheinen tunnistautuminen:	http://www.google.com/landing/2step/
SANS, päivän tietoturvavinkki:	http://www.sans.org/tip_of_the_day.php

Lisenssi

OUCH! julkaisijana toimii “SANS Securing The Human”-organisaatio ja jakelu tapahtuu Creative Commons BY-NC-ND 3.0 lisenssillä. Voit vapaasti jakaa tätä uutiskirjettä ja käyttää sitä osana tietoturvatietoisuusohjelmaasi kunhan et muokkaa uutiskirjettä. Käännös- ja lisätietoja varten, ota yhteys www.securingthehuman.org/ouch. Toimitus: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Käännös suomeksi: Kirill Filatov, CISO, Elisa Appelsiini Oy

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus