Kuukausittainen uutiskirje tietoturvatietoisuuteen liittyvistä aiheista

OUCH!

Tässä numerossa…

Pilvipalveluiden turvallinen käyttö

Yleiskatsaus

Pilvipalvelut tarkoittavat eri asioita eri ihmisille, mutta yleensä sillä tarkoitetaan palveluntarjoajan palveluita, joissa sinä tai palvelutarjoaja säilyttää ja käsittelee tietojasi internetissä perinteisen suljetun konesalin sijaan. Pilvipalveluiden suurin hyöty on helppo pääsy sekä tietojen ja palveluiden helppo synkronointi monista eri laitteista ympäri maailmaa. Tiedon jakaminen muiden kanssa on myös helpompaa. Näitä palveluita kutsutaan pilvipalveluiksi, koska useimmiten käyttäjä ei tiedä missä tiedot fyysisesti sijaitsevat. Esimerkkejä monien käyttämistä pilvipalveluista on tiedostojen editointi G Suitessa, tietojen tallentaminen Dropboxiin, Amazon pilvipalvelimien käyttö, asiakastietojen tallentaminen Salesforce-palveluun ja tietojen varmuuskopiointi Applen iCloudiin. Tämä verkkopalvelut saattavat tehdä sinusta tuottavamman, mutta niissä on omat riskinsä. Tässä uutiskirjeessä kerromme miten saat turvallisesti pilvipalveluista enemmän irti.

Vierastoimittaja

Dave Shackleford (**@daveshackleford**) on "Voodoo Security"- nimisen yrityksen omistava konsultti ja monia SANS- kursseja, mm. "SANS Security 579: Virtualization and Private Cloud Security" ja "Security 524: Cloud Security Fundamentals" laatinut tietoturva-alan ammattilainen.

Pilvitarjoajan valinta

Pilvipalveluita ei voi kategorisoida pahoiksi tai hyviksi, vaan enemmänkin kyseessä on työkalu jolla asioita saa tehtyä, niin kotona, kuin töissä. Kuitenkin kun käytät pilvipalveluita, luovutat yksityisen tietosi muille ja luotat siihen, että he pitävät sen turvassa. Tämän vuoksi on äärimmäisen tärkeää varmistaa, että valitset hyvä pilvipalveluiden tarjoajan. Työympäristössä voit varmistaa esimieheltäsi, salliiko yrityksesi pilvipalveluiden käytön ja jos sallii, varmista mitä pilvipalveluita voit käyttää ja mitkä ovat periaatteet näiden käyttämiseen. Jos käytät pilvipalveluita henkilökohtaiseen käyttöön, varmista ainakin seuraavat asiat:

1. **Tuki**: Kuinka helppoa on saada tukea tai vastauksia kysymyksiin? Löytyykö tarjoajalta sähköpostiosoite, keskustelufoorumi tai FAQ-sivusto joista voit saada apua ongelmiin?
2. **Yksinkertaisuus**: Kuinka yksinkertainen palvelu on käyttää? Mitä monimutkaisempi palvelu on, sitä todennäköisemmin

Pilvipalveluiden turvallinen käyttö

teet virheitä ja saata paljastaa tai hävittää tietojasi. Valitse palvelu jonka toimintaa ymmärrät, osaat käyttää ja jonka asetukset ovat selkeitä.

3. **Turvallisuus**: Mitä tietoja sinusta kerätään? Miten tietosi siirretään laitteeltasi pilveen ja miten niitä säilytetään siellä – onko tietosi kryptattu ja jos ovat, kuka pystyy purkamaan salauksen?
4. **Käyttöehdot**: Käytä hetki tutustuaksesi palvelu käyttöehtoihin (ne ovat usein yllättävän ymmärrettäviä). Varmista kuka tietoihisi pääsee käsiksi ja mitkä ovat juridiset oikeutesi ja myös turvallisuusvaatimukset jotka palvelun tarjoaja odottaa sinun täyttävän.

Pilvipalvelut helpottavat tietojesi käyttömahdollisuuksia ja lisäävät tuottavuuttasi, mutta varmista miten pääset tietoihisi käsiksi ja miten jaat tietojasi.

Tietojesi turvaaminen

Kun olet valinnut pilvipalveluiden tarjoajan, seuraavaksi sinun pitää asentaa palvelu tietoturvallisesti ja oikein. Se miten tietoihisi pääset käsiksi on tietoturvan kannalta usein paljon tärkeämpää kuin mikään muu. Varmista vähintään seuraavat asiat:

1. **Autentikaatio**: Käytä vahvaa, uniikkia salasanalauseketta palveluihin kirjautuessa. Jos palvelu tarjoaa kaksivaiheista tunnistautumista, suosittelemme vahvasti sen käyttöönottoa. Tämä on tärkein yksittäinen asia jonka voit palvelussasi tehdä.
2. **Tiedostojen ja kansioiden jakaminen**: Pilvipalveluissa tietojen jakaminen on yleensä erittäin, usein jopa liian helppoa. Pahimmassa tapauksessa luulet jakavasi tietoja vain yhden tietyn henkilön kanssa, kun tosiasiassa tietosi ovat jaettuna kaikille internetissä. Paras tapa on varmistaa, että oletuksena mitään tiedostoja tai kansioita ei jaeta kenenkään kanssa ja tämän jälkeen voit jakaa haluamasi tiedot haluamiesi henkilöiden kanssa. Kun joku ei enää tarvitse pääsyä tiedostoihisi, muita poistaa henkilön oikeudet. Palveluntarjoajan pitäisi tarjota kattavat lokitiedot siitä kenellä on pääsy mihinkin tietoihisi.
3. **Tiedostojen ja kansioiden jakaminen linkkien avulla**: Yksi yleinen ominaisuus monissa pilvipalveluissa on luoda linkkejä tiettyihin tiedostoihisi tai kansioihin. Tällä tavalla voit helposti jakaa tietojasi kenelle tahansa jakamalla kyseistä linkkiä. Kuitenkin tässä tavassa tietoturva helposti unohtuu, koska kenellä tahansa kenellä on kyseinen linkki,

Pilvipalveluiden turvallinen käyttö

on pääsy linkin takaisiin tietoihin. Vaikka lähetät linkin vain yhdelle henkilölle, voi kyseinen henkilö laittaa linkin kenelle tahansa, tai vaikka jakaa sen internetissä. Jos käytät linkkejä tietojesi jakamiseen, muista poistaa linkki käytöstä käytön jälkeen asettamalla vanhenemispäivän tai jos mahdollista, suojaa linkin takainen tieto salasanalla.

4. **Asetukset**: Tutustu palvelun turvallisuusasetuksiin mahdollisimman hyvin. Jos esim. jaat kansion jonkun muun kanssa, voivatko he edelleen jakaa kyseistä kansiota ilman tietämystäsi. Tutustu myös palvelun lokitusasetuksiin ja yritä löytää sieltä lokit siitä kuka tietojasi on katsellut ja koska. Palvelun pitäisi myös tarjota mahdollisuus jakaa tietoihisi pelkkiä lukuoikeuksia, kirjoitusoikeuksien sijaan, jolloin muut henkilöt voivat muuttaa tietojasi.
5. **Antivirus**: Varmista, että kaikilla laitteilla joilla käytät pilvipalveluita, on asennettuna viimeisimmät versiot virustorjunta-sovelluksista. Jos joku pilvipalvelusi tiedostoista saastuu, se saattaa saastuttaa muutkin laitteet joihin sama palvelu on asennettu.

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 IT-johtaja. Kirill turvaa tällä hetkellä Elisa Appelsiinin liiketoimintaa vastaamalla niin yrityksen omasta kuin asiakkaiden tietoturvasta.

Lähteet

Kaksivaiheinen tunnistautuminen:	https://securingthehuman.sans.org/ouch/2015#september2015
Salasanalausekkeet:	https://securingthehuman.sans.org/ouch/2015#april2015
Salasananhallintasovellukset:	https://securingthehuman.sans.org/ouch/2015#october2015
Mitä ovat haittaohjelmat?:	https://securingthehuman.sans.org/ouch/2016#march2016
SANS SEC524: Cloud Security Fundamentals:	https://sans.org/sec524

Lisenssi