



Tietoturvavinkkejä pilvitallennuspalveluiden turvallisempaan käyttöön

11/2014

Sisällysluettelo

Johdanto	3
1 Mikä on pilvipalvelu?	3
2 Mikä on pilvitallennuspalvelu?	3
3 Ovatko pilvipalvelut turvallisia?	3
Vinkkejä pilvipalvelun turvallisempaan käyttöön	4
4 Harkitse, mitä tallennat pilvitallennuspalveluihin	4
5 Pilvitallennuspalvelu ei voi olla ainoa varmuuskopiointiväline	4
6 Huolehdi käyttäjätunnuksesta.....	4
6.1 Tarkasta verkko-osoite, ennen kuin luovutat pilvitallennuspalvelun salasanan	4
6.2 Käytä eri salasanaa eri palveluihin	5
6.3 Käytä kahden tekijän varmennusta	5
7 Tarkkaile, kuka käyttää pilvitallennuspalveluasi	6

Johdanto

1 Mikä on pilvipalvelu?

Pilvipalvelulla tarkoitetaan palvelumallia, jossa usean käyttäjän kesken jaettuja tietoteknisiä resursseja tarjotaan tietoverkkojen yli. Ominaista pilvipalveluille on, että ne mukautuvat nopeasti ja joustavasti kysynnän ja tarpeiden muuttuessa.

2 Mikä on pilvitallennuspalvelu?

Kuluttajien näkökulmasta pilvipalveluilla tarkoitetaan yleensä pilvessä sijaitsevia tiedostojen tallennuspalveluita, joista tunnetuimpia lienevät Dropbox, Microsoft OneDrive, Google Drive, Box ja Apple iCloud Drive.

Pilvitallennuspalvelut toimivat yleensä siten, että ne luovat käyttäjän kotikansioon oman kansion, jonka sisältö siirtyy automaattisesti verkkoon palveluntarjoajan palvelimelle. Pilvitallennuspalvelusta ne siirtyvät edelleen myös muille tietokoneille ja palveluun kytketyille laitteille, joihin palvelun ohjelmisto on asennettu ja joissa synkronointi on kytketty päälle. Pilvitallennuspalveluiden avulla on helppoa ja kätevää jakaa tiedostoja useiden tietokoneiden kesken ja varmistaa pääsy tiedostoihin verkon ylitse myös silloin, kun omalle tietokoneelle ei pääse.

Valtaosalla pilvitallennuspalveluista on myös mobiilisovellus, jonka avulla omiin tiedostoihinsa pääsee käsiksi esimerkiksi tabletilla tai matkapuhelimella. Monet mobiilisovellukset osaavat myös automaattisesti siirtää matkapuhelimella tai tabletilla otetut valokuvat pilveen. Pilvitallennuspalveluun taltioituihin kuviin voi myös luoda julkisia linkkejä, jolloin niiden jakaminen on helppoa.

3 Ovatko pilvitallennuspalvelut turvallisia?

Pilvitallennuspalveluita käytettäessä on hyvä muistaa, että tiedot siirtyvät aina kolmannen osapuolen ylläpitämille palvelimille. Kolmannen osapuolen tarjoaman tallennuspalvelun ongelmana on, että palvelun tietoturva on palvelun toteuttajan käsissä. Tällöin käyttäjän mahdollisuudet vaikuttaa palveluun tallennettujen tietojen yksityisyyteen ovat rajalliset.

Esimerkiksi palveluntarjoajan palvelimen tietomurtoon tai vieraan valtion tiedusteluviranomaisen tietopyyntöön ei pilvitallennuspalvelujen käyttäjä voi vaikuttaa. Näitä uhkia vastaan voi parhaiten suojautua harkitsemalla mitä tietoja pilvipalveluun tallentaa.

Käyttäjään kohdistuva todennäköisin uhka lienee kuitenkin oman käyttäjätunnuksen ja salasanan päätyminen väärin käsiin. Tällöin palveluun tallennettujen tietojen yksityisyys saatetaan menettää. Käyttäjätunnuksen ja salasanan avulla tapahtuvan tietomurron riskiä voi pienentää yksilöllisten salasanojen, kahden tekijän varmennuksen ja oman harkinnan avulla.

Vinkkejä pilvitallennuspalvelun turvallisempaan käyttöön

4 Harkitse, mitä tallennat pilvitallennuspalveluihin

Pilvitallennuspalvelu on hyvä paikka sellaisille tiedostoille, joiden vuotamisesta ei ole merkittävää haittaa käyttäjälle. Esimerkiksi perheen lomakuvat, omat kirjoitukset, koulutyöt ja muut ei-arkaluontoiset dokumentit voi hyvin tallentaa pilvitallennuspalveluun.

Sen sijaan selkokieleistä salasanalista tai pankkitietoja sinne ei kannata laittaa. Myös yksityiset, arkaluontoiset kuvat on parempi tallentaa jonnekin, jossa pääsyä voidaan rajoittaa fyysisin keinoin. Tällaisille tiedoille turvallisin vaihtoehto on kotona säilytetty, salakirjoitettu varmuuskopiolevy.

Varmuuskopiolevylle murtautuminen edellyttää pääsyä tilaan, jossa sitä säilytetään. Verkkopalveluun murtautumiseen riittää käyttäjätunnuksen ja salasanan hankkiminen esimerkiksi tietojenkalastelun avulla.

5 Pilvitallennuspalvelu ei voi olla ainoa varmuuskopiointiväline

Tietokoneen kiintolevyn rikkoutuessa pilvitallennuspalvelu saattaa auttaa tärkeiden tiedostojen palauttamisessa, mutta sitä ei kuitenkaan tule mieltää varmuuskopiointivälineeksi.

Esimerkiksi tiedostojärjestelmän ongelmat, tiedostojen poistaminen vahingossa tai tiedostoja salakirjoittavat haittaohjelmat iskevät pilvitallennuspalvelun kansioon siinä missä muihinkin paikallisiin kansioihin. Koska pilvitallennuspalvelu synkronoi paikallisen ja pil-

vessä sijaitsevan kansion keskenään, paikalliset virheelliset muutokset tiedostoihin synkronoituvat pilvipalveluun ja pahimmassa tapauksessa käyttäjän kaikille koneille.

Joissakin tallennuspalveluissa on olemassa toiminnallisuus, jonka avulla poistettuja tiedostoja voidaan palauttaa tai tiedostoista ottaa käyttöön vanhempia versioita. Tämä saattaa pelastaa yksittäisiä tiedostoja, mutta esimerkiksi levyrikon tai haittaohjelman seurauksena menetettyä käyttöjärjestelmää niillä ei voi sellaisenaan palauttaa.

Pilvitallennuspalvelu on sellaisenaan hyvä varmuuskopioinnin lisäapu esimerkiksi tulipalon varalta. Silti ajantasaisten varmuuskopioiden ottaminen koko tietokoneen kiintolevystä on tarpeen. Lisäksi pilvipalveluina tarjotaan erityisiä varmuuskopiointipalveluita, joita voi tuki hyödyntää.

6 Huolehdi käyttäjätunnuksesta

6.1 Tarkasta verkko-osoite, ennen kuin luovutat pilvitallennuspalvelun salasanan

Tyypillisimmässä tapauksessa oma käyttäjätunnus menetetään siten, että se erehdyksessä annetaan tietojenkalastelusivulle. Verkkorikolliset saattavat esimerkiksi lähettää käyttäjälle sähköpostin, joka näyttää tulevan tallennuspalvelun ylläpidolta ja jossa kehoitetaan kirjautumaan sisään palveluun ja päivittämään omat tiedot. Sisäänkirjautumislinkki kuitenkin vie verkkorikollisten luomalle sivulle, joka saattaa visuaalisesti muistuttaa oikeaa sisäänkirjautumissivua, mutta sen verkko-osoite on eri.

6.2 Käytä eri salasanaa eri palveluihin

Käytä jokaisessa palvelussa vahvaa, yksilöllistä salasanaa. Näin yhdestä palvelusta vuotanut salasana ei avaa kaikkia käyttäjän palveluita rikollisille.

Jos yksilöllisten salasanojen ylläpito useisiin eri palveluihin tuntuu hankalalta, apuna voidaan käyttää esimerkiksi perinteistä paperille kirjoitettua muistilistaa tai erillistä tarkoitukseen luotua salasananhallintaohjelmistoa.

6.3 Käytä kahden tekijän varmennusta

Kahden tekijän varmennus tarkoittaa salasanan lisäksi syötettävää kertakäyttöistä koodia. Koodi voidaan vastaanottaa esimerkiksi matkapuhelimeen tekstiviestillä tai älypuhelimeen erillisellä sovelluksella

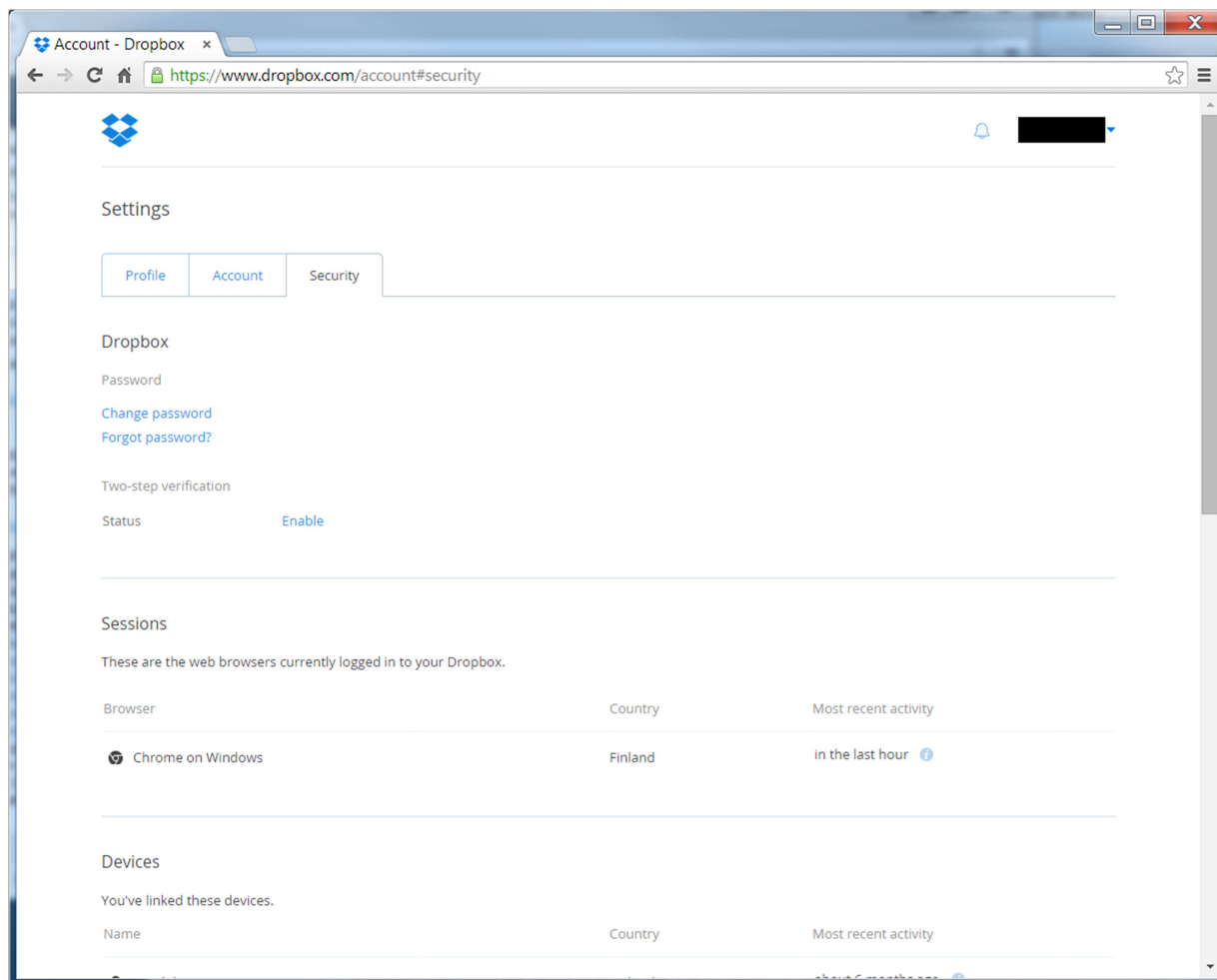
Kahden tekijän varmennus tekee tietojenkalastelun, salasanan arvaamisen tai

muun käyttäjätunnuksen avulla tilille tunkeutumisen vaikeammaksi.

Verkkopalvelun voi asettaa muistamaan sisäänkirjautumiseen käytetyn laitteen, jolloin kahden tekijän varmennus hidastaa palvelun käyttöä vain ensimmäisellä kerralla.

Tekstiviestikoodiin perustuvaa kahden tekijän varmennusta käytettäessä kannattaa huomioida, että jos puhelinnumero vaihtuu esimerkiksi työpaikkaa tai liittymää vaihdettaessa, täytyy uusi numero muistaa vaihtaa myös kahden tekijän varmennusta käytäviin palveluihin.

Esimerkiksi Dropbox-palvelusta kahden tekijän varmennuksen voi kytkeä päälle käyttäjätilin Settings-sivun Security-välilehdeltä kohdasta "two-step verification" ja seuraamalla annettuja ohjeita (Kuva 1).



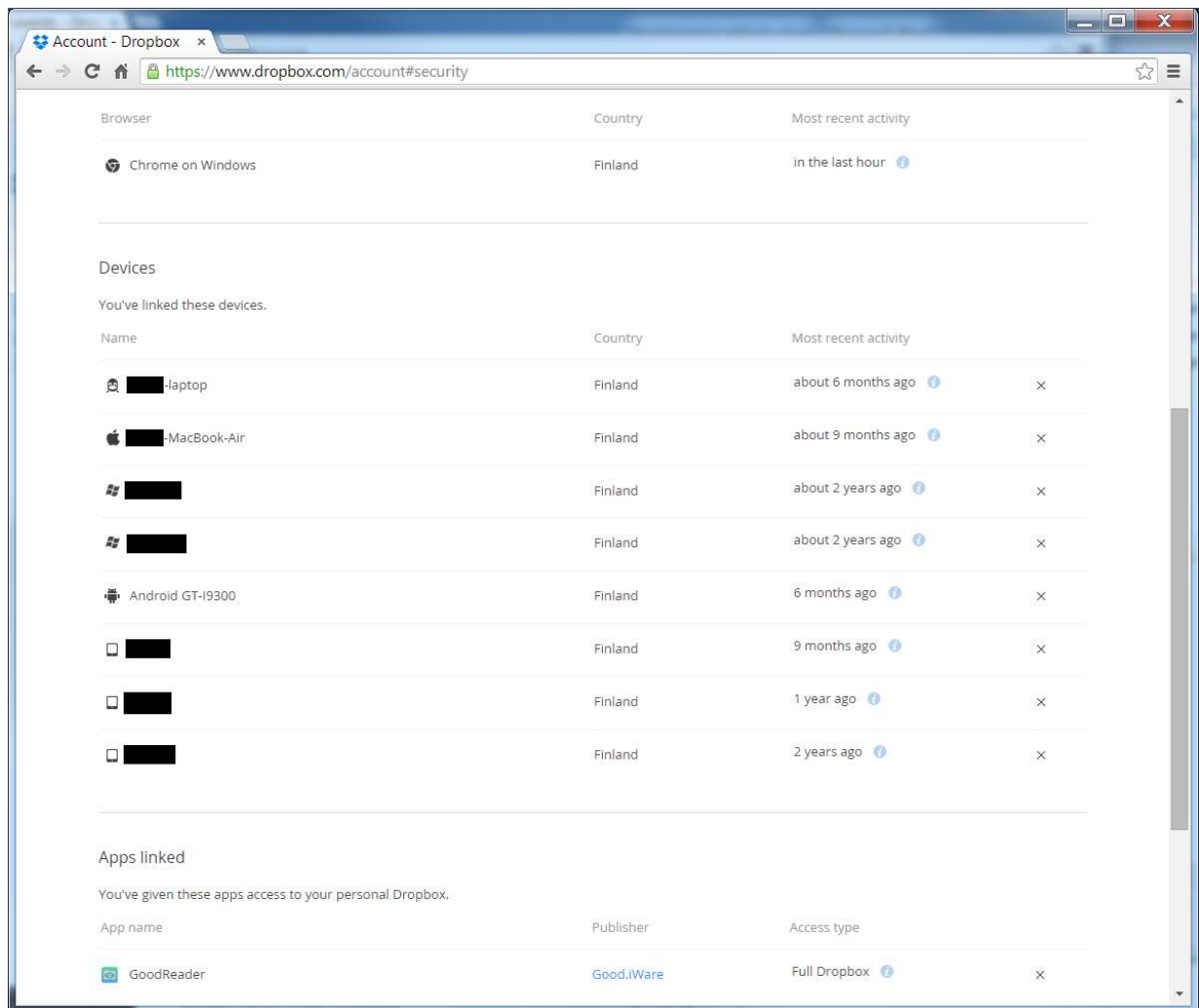
Kuva 1 Kaksivaiheinen tunnistautuminen kannatta kytkeä pilvipalveluun päälle. Yleensä se löytyy Security-välilehden alta nimellä "two-step verification"

7 Tarkkaile, kuka käyttää pilvitalennuspalveluasi

Monissa palveluissa on mahdollista tarkkailla, miltä päätelaitteilta käyttäjättilille on kirjaututtu. Näin voi havaita palvelun luvattoman käytön. Useimmissa palveluissa kirjautumisia seuraava

toiminnallisuus löytyy käyttäjätilinhalinnan "Security"-välilehden alta.

Esimerkiksi Dropboxin Security-välilehdeltä voi tarkastaa, mitkä selaimet, laitteet ja applikaatiot on linkitetty Dropbox-tiliin (Kuva 2).



Kuva 2 Dropbox-palvelun Security-välilehdeltä voi nähdä, mitkä laitteet on kytketty käyttäjätiliin.

Yhteystiedot

Viestintävirasto

PL 313

Itämerenkatu 3 A

00181 Helsinki

Puh: 0295 390 100 (vaihde)

kyberturvallisuuskeskus.fi

viestintävirasto.fi