Tietoturvavinkkejä henkilökohtaisten pilvitallennuslaitteiden turvallisempaan käyttöön

11/2014

Viestintävirasto
Kyberturvallisuuskeskus

Tietoturvavinkkejä henkilökohtaisten pilvitallennuslaitteiden turvallisempaan käyttöön

1 Mikä on henkilökohtainen pilvitallennuslaite?

Kuluttajille ja pienyrityksille on tarjolla henkilökohtaisia pilvitallennuslaitteita, joissa tieto säilötään käyttäjän kotiverkkoon liitettyyn laitteeseen. Vaikka tallennuslaite sijaitsee mahdollisen palomuurin takana kotiverkossa, siihen pääsee käsiksi myös mistä tahansa internetistä.

Käytännössä tämä on toteutettu joko avaamalla kotipalomuuriin reitti pilvitallenninta varten tai useimmassa tapauksessa ylläpitämällä jatkuvaa yhteyttä henkilökohtaisen pilvitallennuslaitteen ja valmistajan palvelimen välillä. Valmistajan palvelimen kautta tehty kirjautuminen mahdollistaa pääsyn tietoihin, vaikka laite sijaitsisi vaihtuvan internetosoitteen ja/tai osoitteenmuunnoksen (NAT) takana.

2 Mitä riskejä pilvitallennuslaitteiden käyttöön liittyy?

Henkilökohtaisten pilvitallennuslaitteiden toteutustavasta johtuen kuka tahansa, jolla on käyttäjätunnus ja salasana, pääsee käsiksi kaikkiin laitteen tiedostoihin. Esimerkiksi tietojenkalastelun seurauksena menetetyt käyttäjätunnukset avaavat varkaille oven kaikkeen pilvitallennuslaitteeseen varastoituun tietoon.

Toisaalta kotiverkon muihinkin laitteisiin on mahdollista päästä kiinni, jos verkkorikolliset onnistuvat murtautumaan pilvitallennuslaitteeseen esimerkiksi jonkin haavoittuvuuden avulla. Pilvitallennuslaitteen ohjelmisto kannattaakin päivittää säännöllisesti. Laitteen elinkaaren loppupuolella päivityksiä voi kuitenkin olla heikosti saatavilla.

Käyttäjän kannattaa harkita, onko hänellä aitoa tarvetta käsitellä tallennuslaitteen tiedostoja kotiverkon ulkopuolella.

3 Vinkkejä pilvitallennuslaitteen turvallisempaan käyttöön

1. Kytke pilvitallennusominaisuus pois käytöstä, ellei tiedostoja yleensä käsitellä kotiverkon ulkopuolella. Laitteen eristäminen julkisesta verkosta pienentää hyökkäyspinta-alaa merkittävästi.

2. Mieti mitä tietoja laitteeseen tallennetaan. Aiheutuisiko tallennettujen tietojen vuotamisesta haittaa?

3. Käytä mahdollisimman pitkää ja vaikeasti arvattavaa salasanaa. Älä käytä samaa salasanaa muissa palveluissa.

4. Vaihda valmistajan oletuksena asettama ylläpitosalasana, eli admin- tai root-tunnuksen salasana. Ylläpitosalasanan tulee olla eri kuin pilvitallennuspalveluun kirjautumiseen käytetty salasana.

5. Pidä laitteen ohjelmisto ajan tasalla valmistajan tarjoamien päivitysten avulla.

6. Käytä kaksivaiheista varmennusta, jos se on laitteen ohjelmiston puolesta mahdollista.

   Joissain laitteissa kaksivaiheinen varmennus toimii älypuhelimeen asennettavalla kertakäyttöisiä koodeja tarjoavalla tunnistautumissovelluksella (TOTP). Toistaiseksi kaksivaiheista varmennusta

kuitenkin tukee vain harva tallennuslaite.

4 Vinkkejä edistyneemmille käyttäjille

1. Seuraa säännöllisesti laitteen lokitiedostoja luvattoman käytön huomaamiseksi.

2. Poista oletus admin- tai root-tunnus kokonaan, ja luo uusi ylläpitoon käytetty tunnus eri nimellä. Tällöin ylläpitotunnuksen nimen arvaaminen ei ole niin helppoa.

3. Kytke pois käyttämättömiä protokollia (SMB, AFP, NFS, FTP, HTTP ja DLNA) ja sovellukset (TimeMachine, iTunes, tulostus), ellei käyttäjä hyödynnä niitä. Tämä pienentää laitteeseen kohdistuvaa hyökkäyspinta-alaa.

4. Kytke ominaisuus, joka estää IP-osoitteen esimerkiksi viiden peräkkäisen epäonnistuneen kirjautumisyrityksen jälkeen. Tällä voidaan hillitä salasanan arvaukseen perustuvia hyökkäyksiä. Ominaisuus ei välttämättä ole saatavilla kaikissa laitteissa.

Yhteystiedot
Viestintävirasto
PL 313
Itämerenkatu 3 A
00181 Helsinki
Puh: 0295 390 100 (vaihde)
kyberturvallisuuskeskus.fi
viestintävirasto.fi