1.10.2013 / DNRO 41/020/2013

VALTIOVARAINMINISTERIÖ
Julkisen hallinnon ICT-toiminto
Lausuntopyyntö VM047:22/2007 1864/00.01.00.01/2012

Ilmatieteen laitoksen lausunto VAHTI:n Päätelaitteiden tietoturva-ohjeeseen

Ilmatieteen laitos näkee positiivisena, että VAHTI on ajantasaistamassa Päätelaitteita koskevan tietoturvaohjeen. Päätelaitteiden tietoturvallisuudella on tärkeä merkitys organisaation kokonaisturvallisuuden kannalta ja tietoaineiston luottamuksellisuuden säilyttämisessä. Päätelaiteympäristö kehittyy jatkuvasti ja henkilöstö haluaa ottaa myös uusia tarjolla olevia laitteita työkäyttöön (myös BYOD). Ohjeessa on pyritty ottamaan huomioon päätelaiteympäristöstä tulevat haasteet, annettu tietoaineiston käsittelyohjeita suojaustasoluokitusten mukaisesti ja tuotu esille myös pätelaitteiden käytön uhkia.

Jotta ohje olisi helppokäyttöisempi, ehdotamme että sen sisältöä jaotellaan aliotsikoilla asiakokonaisuuksien mukaisesti. Sivujen mittaisista teksteistä on hankala löytää hakemaansa. Ohjeessa olisi hyvä olla myös jokunen kuva valoittamassa ohjeen sisältöä. Esimerkiksi kuva etäkäytöstä, jossa näkyy siihen liittyviä tietoturvavaatimuksia ja käytön suhde suojaustasojen tietoaineiston luokitukseen olisi hyödyllinen. Ohjeen kieliasua on hyvä tarkistaa myös ennen julkaisua. Joissain lauseissa merkitys jää epäselväksi. Ohjeessa on usein käytetty huomioida sanaa, jolloin usein tarkoitetaan ottaa huomioon, mikä olisi tarkempi ilmaus monissa ohjeen asiayhteyksissä.

Alla koottu vielä muutamia yksityiskohtaisia kommentteja ohjeen tekstiin:

Kommentti sivun 21 tekstiin, jossa on epäloogisuusta: Bulletinin tekstissä käsitellään uhkia ei eriyttämiskeinoja.

- ”Pääsy organisaation palveluihin voidaan mahdollistaa esimerkiksi alla kuvatulla eriyttämisellä muusta ympäristöstä, virtualisoimalla tai pääteistunnoilla. Mikäli näiden päätelaitteiden käyttöä ei riittävällä tavalla kontrolloida, on riskeinä ainakin:
- salassa pidettävää tietoa päätyy organisaation ulkopuolisille laitteille, jotka eivät välttämättä vastaa tietojen käsittelyssä vaadittavaa tietoturvatasoa
- salassa pidettävää tietoa päätyy käyttäjän omien laitteiden kautta myös kaupallisten yritysten palveluihin ja tietojärjestelmiin, jotka eivät välttämättä vastaa tietojen käsittelyssä vaadittavaa tietoturvatasoa. Palveluita, joihin tietoa voi päätyä ovat esimerkiksi eri pilvitallennuspalvelut.
- käyttäjien henkilötietoja päätyy EU-alueen ulkopuolelle, jossa lait saattavat mahdollistaa henkilötietojen laajemman hyväksikäytön
- laitteiden kautta saattaa organisaation sisäverkossa oleviin laitteisiin tarttua erilaisia haittaohjelmia
- tietoa vuotaa ulkopuolisille
- tietojen käsittelystä ei jää lokia tai muuta jälkeä, jolloin esimerkiksi rikollisen tai muutoin haitallisen toiminnan jälkiselvittely voi hankaloitua merkittävästi tai olla mahdotonta. ”

Ilmaisut voisi olla selkeämpiä ettei tule epäselvyyksiä sisällön tarkoituksesta. Esimerkiksi kappaleessa 6 Päätelaitteiden hallinta sivulla 24 pääkäyttäjän ohjeistuksessa luetelluissa vaatimuksissa on:

- ”Ylätason kuvaus, miten päätelaitteen turvallisuudesta on huolehdittu ja että käyttöä valvotaan ”

Tarkoitetaanko turvallisuudesta tulee huolehtia ja myös pääkäyttäjän käyttöä valvotaan?
Käytön valvonnan yhteydessä voisi olla paikallaan mainita SVTSL laki.

Määrittelyt jatkuu
”Korkean tietoturvatason päätelaitteella pitää lisäksi toteuttaa ainakin:

- Huomioida korkean tietoturvatason verkon, tietojärjestelmien ja palveluiden vaatimukset päätelaitteelle. ”

Edellä oleva määrittely on hyvä tiedostaa alkuvaiheessa, kun ryhdytään määrittelemään päätelaitteen tasoluokittelua.

- Tulee ottaa huomioon verkon, tietojärjestelmien ja palveluiden tietoturvatason vaatimukset päätelaitteelle

Sivu 27 Kappaleen 6.2 Päätelaitteiden omistajuus ja yhteiskäyttö viimeiseen kappaleeseen lisäyksenä.

- Käyttäjän levypalvelimella olevien omien profiilitietojen avulla suoritettu päätekäyttö, jolloin käyttäjän ei tule tallettaa tietojaan työaseman levylle

Ohjeessa olisi hyvä olla kappale myös ajankohtaisiin uusiin teknisiin keinoihin, joilla päätelaitteita ja organisaation tietoja voidaan suojata yhä paremmin (esm. liitteen muodossa).

Helsingissä 2.10.2103

Matti Keränen	Pirkko Kilpeläinen
yksikön päällikkö	tietoturvallisuuspäällikkö