VALTIOVARAINMINISTERIÖ
Julkisen hallinnon ICT-toiminto

VM047:22/2007
1864/00.01.00.01/2012

Päätelaitteiden tietoturvaohje, luonnos

Yliopistojen Sec-työvaliokunta (Sec-tv) on laatinut tämän lausunnon Valtionhallinnon turvallisuuden johtoryhmän VAHTIn ohjauksessa valmistellusta Päätelaitteiden tietoturvaohjeen luonnoksesta.

Päätelaitteiden tietoturvaohjeen lähestymistapa on looginen, alkaen tietojen ja palvelujen tietoturvaluokan määrittelemisestä, eri päätelaitteiden sijoittamisesta tietoturvatasoille ja niiden perusteella tehtävä päätöksenteko siitä, mitä palveluja ja tietoja on mahdollista käyttää päätelaitteen avulla. Ohjeessa on huomioitu hyvin BYOD-laitteisiin liittyvä riskien arviointiin perustuva käytön rajoittaminen teknisesti ja ohjein. Ohjeen johdannossa olisi kuitenkin tarpeen yksiselitteisesti selventää tietoturvatasojen ja suojaustasojen suhde toisiinsa. Lisäksi läpi ohjeen on tarpeen tarkastaa termien *salassa pidettävä* ja *suojaustaso* käyttö.

Luvussa 2.2 tietoturvallisuusasetus olisi hyvä kerrata asiakirjan määritelmä. Ohjeen tulisi selkeyden vuoksi sisältää keskeisten termien määritelmät ja välttää laajasti viittauksia.

Luku 2.4 sisäverkko-ohje, viitteessä 3.1 tulisi tarkentaa tavoite selkeäksi ja siihen liittyvä toimintamalli yksiselitteiseksi. Luvun 2.4 viitteessä 13.10 voisi täsmennetyn vaatimuksen kirjata ”*Päätelaiteessa estetään erikseen hyväksymättömien päätelaitteen tarjoamien palvelujen näkyminen verkkoon*”. Termiä massamuisti tulisi käyttää monikossa massamuistit, koska useissa puhelimissa/tableteissa/tietokoneista on useita massamuisteja. Massamuisti sanamuotona voi aiheuttaa käsityksen, että vain käyttöjärjestelmälevy on salattu.

Luvussa 2.6 olisi hyvä mainita mobiililaitteiden käytöstä vielä erikseen, esim. puhuminen ja sähköpostin lukeminen julkisissa tiloissa. Päätelaitteen käyttö tulee suhteuttaa tiedon luokitteluun ja suojata käyttötapahtuma esim. suojakalvolla.

Luvussa 3.1 tietoturvallisuus päätelaitteilla on syytä mainita esimerkkinä myös tietojen luvaton käyttöyritys sekä päätelaitteeseen liittyvä-

nä riskinä takaportin rakentaminen yhdessä laitetoimittajan kanssa tai laitetoimittajan tietämättä. Myös riittävällä tasolla suoritetusta riskianalyysistä ja auditoinista olisi hyvä mainita esimerkki tässä luvussa.

Luvussa 3.3 päätelaitteen tietoliikenne puuttuu maininta multipath TCP-liikenteestä ja automaattisten synkronointipalvelujen tuntemisen tärkeys.

Luvussa 3.4 herää kysymys rinnastetaanko VPN-yhteyden käyttö täysin sisäverkossa toimimiseen, vaikka tässäkin tapauksessa tulisi olla rajoitteita mitä palveluita VPN-yhteyden läpi on turvallista käyttää.

Kappaleessa 3.5 on tavoitteena kuvata USB-muistilla toteutettava ympäristö turvallisuutta parantavana ympäristönä. USB-laitteella tapahtuva järjestelmän käynnistäminen (boottaus) tulisi olla lähtökohtaisesti estettyä ja sallittua vain sellaisissa laitteissa, joissa erillinen ympäristön käynnistäminen on tarpeen. Lisäksi virtualisoinnista ei puhuta luvussa mitään (esim. VMware).

Luvussa 5.1 ei ole mainintaa jatkuvuussuunnittelusta. Whitelist ja blacklist rajoittamisessa mainitaan asentaminen, mutta pitäisi mainita myös ohjelman ajamisen rajoittaminen. Lukuun 5.1 olisi hyvä lisätä maininta, että pilvipalveluja käytettäessä organisaatiossa on syytä tehdä tiedon luokittelun ohjeistus ja ohjeistuksen jalkautus.

Luvussa 7.4. käyttö ja ylläpito tulisi huomioida laitteistoon liittyvät riskit, ei pelkästään ohjelmistoihin.

Luvussa 7.6 käytöstä poisto olisi hyvä mainita, että tyhjennys ei aina tuhoa riittävästi tietoja vaan ainoa luotettava tapa on murskaus, mikäli laitteella käsiteltyjen tietojen takia tämä on tarpeellista.

Luvussa 8.2 ”*Erilaisten verkkojen, erityisesti avoimien WLANien*” voisi tarkennuksen vuoksi korvata tekstillä ”*Erilaisten ei-luotettujen verkkojen käyttö.*.”, koska on olemassa myös ei-luotettuja mobiiliverkkoja.

Päätelaitteiden tietoturvaohjeen teksti kaipaa huolellista kielenhuollollista läpikäyntiä. Ohjeessa on mm. kaksitoista kertaa sana toimesta. Sana ”toimesta” on tyypillistä teknisissä kuvauksissa käytettyä kieltä, joka voidaan korvata ja asia esittää sujuvammin, esimerkiksi näin ”*Päätelaitetta on myös saatettu ulkopuolisen toimesta muokata*” korvattaisiin tekstillä ”*Ulkopuolinen on myös saattanut muokata päätelaitetta*”. Samoin teksti ”*Mikäli huolto tai ylläpito hoidetaan palvelutoimittajan tai muun tahon toimesta*” korvattaisiin tekstillä ”*Mikäli palvelutoimittaja tai muu taho hoitaa huollon tai ylläpidon*”.

Ohjeessa on myös hyvin pitkiä ja useita sivulauseita sisältäviä lauseita, joiden sisältöä on hankalaa hahmottaa. Sisällön selvyyden ja ymmärrettävyyden vuoksi pitkiä lauserakenteita kannattaa jakaa kahdeksi eri lauseeksi. Esimerkkinä ”*Edellisessä luvussa lueteltujen uhkien lisäksi tyypillinen uhka on kadotettu tai varastettu päätelaite*” kor-

Aalto-yliopisto

Lausunto
Yliopistojen Sec-työvaliokunta

4.10.2013

vaus tekstillä ”*Edellisessä luvussa lueteltujen uhkien lisäksi tyypillinen uhka on päätelaitteen katoaminen tai varastaminen*”.
Päätelaitteiden tietoturvaoppaan termistössä kannattaa pyrkiä mahdollisimman suureen yhtenäisyyteen. Samasta asiasta useiden eri termien käyttäminen vaikeuttaa kokonaisuuden hahmottamista. Esimerkkinä kohta, jossa oppaan alkupuolella puhutaan pääteistunnosta, loppuosassa (luku 8) terminaaliratkaisusta.

Ohjeen sisältöä tukemaan ja havainnollistamaan olisi hyvä lisätä joitakin kaavioita.

Sec-tv:n puolesta,

Riitta Gröhn
Tietoturvapäällikkö
Aalto-yliopisto