**Kotimaisten kielten keskus**

31.1.2012

# Lausunto luonnoksesta teknisen ICT-ympäristön tietoturvataso-ohjeeksi

Valtiovarainministeriö on pyytänyt lausuntoa luonnoksesta teknisen ICT-ympäristön tietoturvataso-ohjeeksi. Ohje on miellyttävänoloinen kooste siitä, miten tietoturva-asetuksen ja sen pohjalta jo annettujen ohjeiden vaatimukset koskevat tieto- ja viestintäteknisen ympäristön teknistä toteutusta, ja etenkin palveluiden ulkoistamista koskeva luku on tervetullut täydennys tähänastiseen ohjeistoon.

Tietojen suojaustasoluokittelua koskevassa luvussa 2.3 on muutama kohta, joka herättää hiukan hämmennystä. Tietoturva-asetuksen henki on tähän saakka tuntunut olevan, että aineistojen turvallisuusluokittelun edellytyksissä ”muut yleiset edut” olisi tulkittava melko suppeasti eikä julkisuuslain 24.1§ kohtien 7–8 mukaan salassa pidettäviä aineistoja suinkaan olisi aina syytä turvallisuusluokitella. Luonnoksen kuvissa 6 ja 7 annetaan kuitenkin ymmärtää, että salassapito näiden kohtien perusteella edellyttäisi aina turvallisuusluokittelumerkintää.

Kun käytännössä turvallisuusluokiteltua aineistoa on jatkossa määrä käsitellä KATAKRI-vaatimusten mukaisesti, vaatimus kaiken turvajärjestelyjä ja varautumista koskevan salassa pidettävän aineiston turvallisuusluokittelusta on raskas ja johtaa vain tarpeettomiin kustannuksiin. Erityisen selvästi tämä koskee niitä valtion laitoksia, joiden toiminta ei muuten edellyttäisi KATAKRI-vaatimusten soveltamista. Ohjeeseen olisikin syytä kirjata selvästi, että myös turvajärjestelyjä ja varautumista koskevat tietoaineistot voidaan jättää pelkän suojaustasoluokittelun varaan, jos niillä ei ole todellista merkitystä kansainvälisten suhteiden, valtion turvallisuuden tai maanpuolustuksen kannalta.

Työasemia ja päätelaitteita koskevassa luvussa 4.2 esitetään työasemien, etenkin kannettavien laitteiden, kiintolevyjen salaus hiukan väljemmin kuin sisäverkko-ohjeessa (VAHTI 3/2010). Sisäverkko-ohje esittää kannettavien työasemien kiintolevyjen salauksen pakollisena vaatimuksena jo perustasolla, tässä luonnoksessa taas salaus on esimerkkinä hyvästä käytännöstä. Kaiken kaikkiaan pidän nyt käsillä olevan luonnoksen muotoiluja hyödyllisempinä: sisäverkko-ohjeen ongelmana on muutenkin, että monet vaatimukset (vaikkapa juuri kiintolevyjen salaus) on esitetty ilman perusteluja, mikä tekee ohjeen käytännön soveltamisen kovin vaikeaksi. Nyt valittu linja, jossa yksityiskohtaisten vaatimusluettelojen sijaan velvoitetaan perustamaan ratkaisut tietoiseen harkintaan ja riskinarviointiin, on kokonaisuutena käyttökelpoisempi.

Vastaavasti luvussa 4.3 esitetään, että heikko tunnistaminen on organisaation sisäverkossa toimittaessa riittävä valtaosaan palveluita. Sisäverkko-ohjeessa sen sijaan suositellaan perustasollakin käyttäjätunnuksen ja salasanan yhdistelmää vahvempaa tunnistamista; korotetulla tasolla tämä on jo vahva suositus, josta poikkeaminen sallitaan vasta kirjallisen riskianalyysin jälkeen. Organisaation ulkopuolelta kirjauduttaessa vahva tunnistaminen on jo perustasolla vahva suositus. Tässäkin olisin taipuvainen pitämään nyt käsillä olevan ohjeluonnoksen muotoilua käyttökelpoisempana kuin runsaan vuoden takaista sisäverkko-ohjetta, mutta ristiriita lienee hyvä mainita selvästi.

Antti Leino
tietoturvapäällikkö

Vuorikatu 24
00100 Helsinki
Y-tunnus: 0245872-8

Puhelin 020 7813 200
Faksi 020 7813 219
S-posti etunimi.sukunimi@kotus.fi