

21.5.2012

VALTIOVARAINMINISTERIÖ

Julkisen hallinnon ICT-toiminto

28. 05. 2012

Valtiovarainministeriön lausuntopyyntö VM047:14/2007

Lausunto Sovelluskehityksen tietoturvaohjeesta

Valtiokonttori toteaa, että lausunnolla oleva Sovelluskehityksen tietoturvaohje on tärkeä ja tarpeellinen tietoturvan huomioimiseksi sovelluskehityksessä. Ohje on hyvä työkalu sovelluksen hankkijoille ja sovelluskehittäjille. Ohjeeseen on pyritty saamaan kaikki tietoturvaan liittyvät erilaiset vaatimukset yhdeksi kokonaisuudeksi.

Sovelluskehityksen tietoturvaohje on kuitenkin sisällöltään erittäin laaja-alainen. Ohjeen kohderyhmä on myös hyvin suuri ja sisältää useita erilaisia tehtäväkuvia. Tämä asettaa haasteita sille, että ohjeen asiasisältö saadaan kohdistettua oikeille ryhmille eikä ohjeesta tule liian yleisellä tasolla olevaa ohjetta. Ohjeessa kuitenkin mennään hyvin tarkalle tasolle. Tämä aiheuttaa sen, että ohjeen sisällöstä tulee hyvin raskas. Yleisenä huomiona todetaan myös se, että ohje on päällekkäinen monien muiden Vahti-ohjeiden kanssa.

Ohjeeseen kirjatut yleiset organisaation tietoturvallisuuden hallintaan ja ICT-ympäristöön liittyvät vaatimukset tulisi käsitellä muissa Vahti-ohjeissa. Nämä vaatimukset tulisi rajata lausunnolla ohjeen ulkopuolelle. Todetaan, että näiden vaatimusten osalta ohjeessa riittäisi hyvin vain viittaukset muihin ohjeisiin tarpeellisin osin. Edellä mainitun kaltaisia vaatimuksia ovat mm. STR-002 – STR-005, POL-001, POL-003 – POL-007, OSK-003, OSK-004, OSK-007, OSK-008, STA-001, JTH-001 – JTH-005, KTY-016 – KTY-018.

Valtiokonttori näkee keskeisenä haasteena sen, miten ohjeen edellyttämän vaatimustason noudattaminen vaikuttaa sovelluskehityksen kustannuksiin. Ohjeen noudattaminen kokonaisuudessaan voi tuoda sovelluskehityshankkeisiin merkittäviä lisäkustannuksia. Kilpailutuksissa ohjeen käyttö vaatimusmäärittelyn pohjana saattaa olla haasteellista johtuen erilaisista tulkinnoista liittyen vaatimuksiin.

Vaatimustaulukkoon tulisi merkitä selkeämmin ne kohdat, joita edellytetään tietoturvasoissa. Taulukon käytettävyyttä saataisiin parannettua, mikäli taulukko olisi käytettävissä Excel-muodossa.

21.5.2012

Toisena vaatimustaulukon havaintona on perustason yhteydessä käytetyt termit "vahva suositus" ja "suositus", jotka tulisi määritellä ja erotella tarkemmin mitä tarkoitetaan.

Vaatimustaulukon yksittäisenä havaintona vielä todetaan vaatimuksen VTM-001 kuvauksessa termi "korkea taso". Tämä termi tulisi selkeyden vuoksi korvata jollain muulla ilmaisulla, jottei termiä sekoiteta esimerkiksi tietoturvasojen tasoihin.

Pääjohtaja


Timo Laitinen

Yksikönjohtaja


Juha Pietarinen