

Valtiovarainministeriö

VM 2125/00.01.00.01/2011

Lausunto ICT-ympäristön tietoturvaso-ohjeeseen

Valtiovarainministeriö on pyytänyt oikeusministeriöltä lausuntoa VAHTI:n valmistelemasta teknisen ICT-ympäristön tietoturvaso-ohjeesta.

Lausuttavan ohjeen teksti on selkeää sekä ymmärrettävää. Eräänä haasteena Vahti-ohjeistuksessa yleisesti kuitenkin on, että niissä viitataan aikaisempiin Vahti-ohjeisiin ja toisaalta käsitellään asioita, joita on ohjeistettu toisissa Vahti-ohjeissa. Tällöin lukija joutuu perehtymään suureen määrään Vahti-ohjeita yrittäessään selvittää johonkin tiettyyn asiaan liittyviä turvallisuussuosituksia. Nykyisen sekanaisten ja päällekkäisen aihesisällön vuoksi ohjeiden käytettävyys ja ymmärrettävyys on melko heikkoa.

Järjestelmien tärkeysluokituksen (luku 3. Suojattavien kohteiden määrittäminen s.30 – 31) määrittelyssä olisi lausuttavassa dokumentissa tullut huomioida järjestelmän tärkeysluokitukseen liittyvät kaksi näkökohtaa:

1. Järjestelmän tärkeysluokka (elintärkeä, erittäin tärkeä, tärkeä, jonkin verran tärkeä, vähäinen merkitys) suhteessa viraston omaan, sisäiseen toimintaan.
2. Järjestelmän tärkeysluokka suhteessa kansalaisiin, toisiin viranomaisiin sekä muihin sidosryhmiin.

Järjestelmä voi olla elintärkeä viraston oman toiminnan kannalta, jolloin sitä tulee arvioida viraston oman toimintaprosessin kannalta, jonka lamautuminen voi jopa estää viraston palveluiden tarjonnan. Toisaalta järjestelmä voi olla suhteellisen vähämerkityksellinen viraston omassa toimintaprosessissa mutta hyvinkin tärkeä tietojen ulkopuolisten käyttäjien näkökulmasta. Jotta tärkeysluokitus osuisi oikeaan tulee molempaa näkökohtaa arvioida.

Koskien vaatimuksia tekniselle tietotekniikkaympäristölle voidaan todeta, että esitetyt vaatimukset lienevät jo monelta osin laajalti toteutettuja ja valtaosaltaan tarvittavat muutokset ovat toteutettavissa kohtuullisin lisäkustannuksin. Poikkeuksena tästä ovat virastojen lähiverkot, joiden osalta ainakin oikeusministeriön hallinnonalalla on käsityksemme mukaan tuntuva puutteita, kuten:

Jakamot, ristikytkepaikat ja verkon aktiivilaitteet sisältävät telineet eivät välttämättä sijaitse lukituissa tiloissa, joihin on pääsy vain valtuutetuilla henkilöillä.

Verkkoa ei ole suunniteltu ja rakennettu siten, että se tukee tiedon suojaamista tiedon luokittelun mukaisesti siten, että kriittisemmät tiedot on suojattu paremmin.

Näiden nostaminen ohjeessa kuvatulle tasolle aiheuttaa merkittäviä lisäkustannuksia ja edellyttää lisärahoitusta.

Eräitä yksityiskohtaisia huomautuksia ohjeesta

s. 6. *Kuva 1. Organisaation tietoturvallisuuteen vaikuttavat:* Miksi yllä oleva organisaation tietoturvallisuus-palkki ei ylety ydintoimintaan saakka?

s 9. Sanamuoto on huono: *"Tietoturva-arviointia voidaan pitää ei niin muodollisena."*

s. 13. Onko syytä erikseen mainita, että ohjetta käytetään eräissä ajallisesti lyhytaikaisissa projekteissa. *" Tätä ohjetta hyödynnetään valtiovarainministeriön tuottamissa, Valtiokonttorin..."*.

Ohjeessa on turhaa toistoa. Esim. suojaustasoa on käsitelty sivulla 10 "Suojaustaso" otsikon alla sekä luvussa 2.3 *"Tietoaineistojen käsittely ja luokittelu"*. Sanastossa olevan osion voi jättää pois.

Luku 2.5 *"Kansallinen turvallisuusauditointikriteeristö (KATAKRI)"* voisi olla ohjeessa aiemmin, koska Katakriin viitataan useassa kohtaa sitä ennen olevassa tekstissä.

s 24. Listasta *"Lisäksi mahdollisesti huomioitavat: "* puuttuu Katakri vaikka on juuri edellisessä luvussa esitelty ja mainittu, että pitää tarvittaessa noudattaa.

s. 26. Tarkoittaako *"...sekä tietoturvallisuusasetus että VAHTI 2/2010 sisältävät lukuisia muita vaatimuksia, joita tässä ohjeessa ei oteta huomioon..."* että muita asioita ei oikeasti tarvitse huomioida vai että muita asioita ei tässä ohjeessa käsitellä?

Luvut 4.4 *"ICT-palveluiden tuottaminen"* , *"4.4.3 Palveluiden tuotantomallit"* olisi sopinut paremmin Vahti ohjeeseen *"Valtion ICT-hankintojen tietoturvaohje, VAHTI 3/2011"*. Tässä se on hieman turhaa teoriaa jota ei tarkemmin konkretisoida.

Tietohallintojohtaja


Max Hamberg

Erityisasiantuntija


Erkki Saukkonen