VALTIOVARAINMINISTERIÖ

Tietoturvatasot

LAUSUNTOJEN YHTEENVETO JA JOHTOPÄÄTÖKSET

Minna Romppanen

minna.romppanen@vm.fi p. 09 – 160 33206

Lausuntoaika marras-joulukuu 2008

Ministeriöitä, virastoja ja laitoksia sekä valittuja lukuisia sidosryhmiä pyydettiin lausumaan näkemyksiään marraskuussa 2008.

Organisaatioiden erikseen toimittamat sähköiset ja kirjalliset lausunnot on pyritty ottamaan huomioon käsikirjaan.

Lausuntopyynnön saajat

Ministeriöt
Virastot ja laitokset
Valtiontalouden Tarkastusvirasto
Tietosuojavaltuutetun toimisto
Kansaneläkelaitos

Muut julkisen hallinnon toimijat
CSC Tieteellinen Laskenta
Julkisen hallinnon tietohallinnon neuvottelukunta JUHTA
KuntaIT
Suomen Kuntaliitto
Valtion yhteishankintayksikkö Hansel Oy

Tieto- ja viestintätekniikka-alan toimijoita edustavat järjestöt ja organisaatiot

Finnsecurity ry
ICT Suomi ry
ISACA
Keskuskauppakamari
Ohjelmistoyrittäjät ry
Suomen open source -keskus COSS
Suomen Yrittäjät ry
EK Elinkeinoelämän Keskusliitto
TIEKE Tietoyhteiskunnan kehittämiskeskus ry
Tietoalojen liitto ry / Teknologiateollisuus ry
Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry
Tietotekniikan liitto ry
Tietoturva ry

Lausunnon antajat: (tilanne 8.12.2008)

- Kirjallisen sähköisen lausunnon antoi 39 (+1) organisaatiota
- Sähköiseen versioon jätti vastauksen 29 organisaatiota
- Kirjallisen lausunnon antoi XX organisaatiota

- Osa ilmoittanut antavansa lausunnon myöhässä
- Lausuntoja tulee vielä..

- VTV antoi epävirallisen muistion, jota kuitenkin saa käyttää viittauksissa kuin lausuntoa.

Lausuntoa pyydettiin seuraavista aiheista

- Yleiset kommentit käsikirjan tietoturvataso-ajatteluun

- Kommentit liitteiden sisältöön:
  - Liite 1 Organisaation kypsyys
    - Webropol-kyselyssä pyydettiin arvioimaan myös vaatimusten toteutuminen
  - Liite 2 IT:n hallinta
  - Liite 3 Sanasto
  - Liite 4 Korvaava menettely

Hyvänä ja toimivana pitivät

- Enemmistö vastaajista: 33 kpl organisaatioita

- *”Käyttökelpoinen”*
- *”Selkeä”*
- *”Tarpeellinen”*
- *”Kattava”*
- Liitteiden esimerkkejä pidettiin *”havainnollisina ja tervetulleina”.*

Sanasto (Liite 3)

- Tarpeellinen olla mukana (useita kommentteja)
- Synkronoitava jatkossakin VAHTI-sanaston kanssa (3 kommenttia)
- Ehdotuksia lisättäviksi sanoiksi joitakin

- Työterveyslaitos: *”Melko lyhyt, mutta tärkeimmät asiat on määritelty.”*

- Oulun hallinto-oikeus: *”Hyvä sanasto. Oma tietotaso huomioiden tarpeellinen, Voisi olla laajempikin.”*

Korvaava menettely (liite 4)

- Suurin osa ei ole maininnut mitään
- Erityisen tärkeä: 1 (EK)
- Tarpeellinen ja hyvä: 11 kpl
- Raskas menettely: 1 kpl (Tiehallinto)
  - Haltik: *”Käytön seuranta tulee määritellä ”*
  - Vaasan yliopisto: *”Vaarantaa tasoajattelun”*
- Normit osa 2: *”Korvaava menettely on välttämätön edellytys tasojen toteutumiselle”*

Toimenpide-ehdotus:
→ Säilytetään korvaava menettely

Velvoittavuudesta

TUKES:

”Käsikirjasta ei selviä, onko tulossa jokin säädös, joka velvoittaa virastoja johonkin 1.1.2011. Tulisi sanoa selvästi, perustuuko käsikirja lakiin tai asetukseen vai onko kyseessä suositus.”

Toimenpide-ehdotus:

→Keskusteltava ohjausryhmässä

→Normit, osa 2 ehdotuksista valinta (”polku eteenpäin”)

→Sidotaan tulosohjaukseen, muut normit tukena

- Tietoturva-asetus viivästynyt
  - olisi paras, mutta ei tällaisenaan toimi
- Tietohallintolain tulevaisuus avoin, ei jäädä odottamaan

Velvoittavuudesta & normeista

Oikeuskanslerin virasto:

”*On jossain määrin kyseenalaista, voiko pelkän laajennetun tilivelvollisuuden perusteella antaa lausuttavana olevan kaltaisia sitovia määräyksiä valtionhallinnolle. Käsikirjassa tulisi käsitykseni mukaan selkeästi tuoda esiin ne normit, joitten nojalla valtionhallinnon noudatettavaksi tarkoitetut määräykset on annettu.*”

Toimenpide-ehdotus

→ VM määrää/ohjaa hallinnon tietoturvallisuutta ja voi antaa velvoittavia määräyksiä, asetuksia tai muuta lainsäädäntöä, valtioneuvostotason velvoitteen tms.

→ Valtiokonttori / VIP toteuttaa

YETT & Velvoittavuus

Ympäristöministeriö

- *”Käsikirjassa todetaan, että yhteiskunnan elintärkeitä toimintoja tuottavilta organisaatioilta voidaan edellyttää myös perustasoa korkeampaa tietoturvatasoa. Olisiko jo tässä raportissa mahdollista määritellä kuka ja missä tämän tason määrittelee ? ”*

→ Toimenpide-ehdotus:

- →YETT-strategia päivitetään v. 2009, esitetään tasot huomioitavaksi siinä sekä VARE-hankkeen yhteistyössä
- →Perustason toteuttaminen on pakollista 1.1.2011 alkaen
- → Palvelukeskukset ja alihankkijat velvoitetaan noudattamaan +1 tasoa (tilaaja-asiakkaaseen verrattuna)
- → Organisaatio voi itse päättää muilta osin tavoittelemansa tason/tasot, tarkennetaan käsikirjaan keinot (luku 1)

Taloudelliset vaikutukset

- *”Voisiko Hansel arvioida tietoturvatasoja jo valmiiksi kilpailuttamisvaiheessa”?*
  - Ostajan on itse määriteltävä tarvittava taso (palvelu sekä toteuttava organisaatio)

- Toimenpide-ehdotus
- → VIP:ltä kaivataan konsultaatiota ja määrittelyapua

- Pilotoinnissa esimerkkejä soveltamisen kustannuksista:
  - Liite 1: 0€, enimmäkseen sopimista
  - Liite 2: useimmissa enin työ on tehty jo nyt

→ Kustannushyötyanalyysi hallinnosta perustason tilasta tarvitaan, nyt olemassa luonnos tietoturvatasoista perustasosta

→ VAREn kautta v. 2009 laaja analyysi, jossa varautuminen ja tietoturvatasot samassa?

Aikataulu

- Tilastokeskus:
- ”*Aikataulutavoitteen siirtäminen 1.1.2012*”

- Tämä tarkoittaisi yhtä vuotta lisäaikaa velvoittavuuden alkamiselle, koska virastot eivät ole voineet huomioida tietoturvatasoja vuoden 2009 suunnitelmissa.

→ Ei ehdoteta siirtämistä, valmistelua voi aloittaa v. 2009

→ VAREn velvoittavuus synkronoidaan?

Missä ja miten tasoja ylläpidetään jatkossa?

VM omistaa ja markkinoi Tietoturvatasot, VIP toteuttaa.

- v. 2009 jatkotyö ja ohjaus VARE-hankeryhmän kautta, niin kauan kunnes on sovittu jotain pysyvää ylläpidosta ja tarpeeksi valvoittavuutta.
- Itsearviointimallit käytettävissä ja jaetaan 1/2009 (.xls)

→ Toimenpide-ehdotus

- **Liite 1: organisaation kypsyystaso ja sen arviointi**
  - → Päivittäminen VM/HKO, CAF:n ym. laatutyön ohessa
  - → Itsearviointi HVK:n HUOVI-arviointivälineen sisällä (valmistuu syksy 2009)

- **Liite 2: IT:n hallinta**
  - → Päivitetään VAREn ym. HUOVI-vaatimusten mukana
  - → Itsearviointi HVK:n HUOVI-arviointivälineen sisällä
  - → Päivityssykli tarpeeksi pitkä, minimissään 1 v. välein?
  - → Ohjaavassa ryhmässä oltava erityisesti kypsyysmallien osaaja

Kypsyys vs. tasojen ”soveltamisen onnistuminen”

- Kypsyysajattelussa on joustettu joissakin vaatimuksissa tarkoituksella
  - dokumentointivelvoite (ks. myöhemmin)
  - Suomen lakisääteiset vaatimukset on nostettu velvoittavaksi
    - vaikuttaa arviointimallin kaavoihin

→Toimenpide-ehdotus:

→Auditoijalla oltava riittävä osaaminen

→VIP:n vastuuhenkilöiden yhteistyö VTV:n ja controllerin kanssa

→Auditoijien koulutus (esim. 2 krt/v), ..

Roolit, parhaat käytännöt

- HY: ”*Tietoturvatasojen roolit tulisi määritellä käsikirjassa ja sanastossa.*”

→ Työkirjaan ja työkalupakkiin tulee materiaalia perustason soveltamiseen

→ Toimenpide-ehdotukset

→ määritellään rooleja ja osaamistarpeita VARE-hankkeessa

→ VIP:n työkalupakkiin mallipohjia tms. välineitä

Toimenpiteitä tasojen toteutumiselle

- Best practices –pankki VIP:ille

- EK: *”Kaikki vaatimukset eivät tule normiohjauksen kautta, sopimisperusteisiin tietoturvavelvoitteisiin kiinnitettävä huomiota.”*
  - → Tiiviiksi yhteistyötahoksi HVK:n SopiVa-hanke”
  - → Huoltovarmuuskeskuksen rooli korostuu jatkossa

- Voiko joku valtuutettu antaa sertifikaatin organisaatiolle tai palvelulle?
  - → Ei ehdoteta ainakaan alkuvaiheessa, sopimukset ja ostajan velvoitteet alihankkijalle riittävät.
  - → Hallinnosta vaihtoehtoja esim. VIP, VTV tai vastaava
  - → Jostain osa-alueesta sertifiointityötä tekevä yritys (joitakin Suomessa)

Esimerkkejä lisäämällä yhteissetti laajaan yhteiseen hallinnon käyttöön

- KELA luvannut toimittaa lisää esimerkkejä vaatimuksiin
  - Näin saadaan Tietoturvatasovaatimukset sopimaan heidän ja terveystoimialan tarpeisiin riittäväksi ja lisävaatimussettiä ei tarvita.
    - v. 2009 alkuvuodesta

    → Yhteyshenkilö KELAn tietoturvapäällikkö

Tietoaineistojen luokittelut ym.

- Keskuskauppakamari: *”Lisää ohjeistusta”.*

- → tulossa lausunnoille VM:stä joulukuussa 2008 (VAHTI x/2009)
  - **Valtionhallinnon tietoaineistojen**
    - **käsittelyn tietoturvallisuusohje**
  - **Tietoaineistojen käsittely valtionhallinnossa:**
    - **Käyttäjän ohje**

Indeksointi muihin standardeihin

- Organisaatio voi jatkossakin toimia nykyisten standardien kanssa.
- Mäppäykset tekeillä
- Työkirjassa soveltamisapuja

Johtopäätöksiä

- Lausuntojen perusteella tehdään sisältöön ja ulkoasuun muutoksia
- Poikkeavat mielipiteet ääripäistä on jätetty enimmäkseen huomiotta
- Velvoittavuus suurin ongelma, tarvitaan tietoturvatasojen sitominen lainsäädäntöön.
- Auditointiin tarvitaan päätöksiä vastuuorganisaatiosta ja auditointiprosessista.