31. 01. 2012

10.1.2012

VALTIOVARAINMINISTERIÖ

Julkisen hallinnon ICT-toiminto

Valtiovarainministeriön lausuntopyyntö VM047:13/2007 2125/00.01.00.01/2011

Lausunto Teknisen ICT – ympäristön tietoturvataso-ohjeesta

Vuonna 2010 voimaan astunut tietoturvallisuusasetus ja sen täytäntöönpanoa tukeva VAHTI 2/2010-ohje toimivat keskeisenä valtionhallinnon virastojen tietoturvallisuuden kehitystyötä ohjaavana kokonaisuutena. Valtiokonttori toteaa, että lausunnolla olevalla ohjeistuksella saadaan yksityiskohtaisempia, käytännön tason ohjeita siitä, miten näitä vaatimuksia voidaan organisaatiossa erilaisilla teknisillä ja hallinnollisilla ratkaisuilla toteuttaa.

Ohjeessa on otettu huomioon myös kansallisen turvallisuusauditointikriteeristön (KATAKRI) vaatimuksia. Toteamme, että tarve yhteen sovittaa tietoturvatasojen vaatimusten ja siitä tulevien auditointivaatimusten ja KATAKRI-auditointikriteeristön vaatimusten on suuri.

Valtiokonttori täyttää tietoturvatasojen perus- ja hallinnollisella puolella korotetun tason vaatimukset. Toteamme, että tällaisella työvälineellä olisi mahdollista arvioida tarvittavat muutokset esimerkiksi perustaso KATAKRI-vaatimusten täyttämiseksi ja siten suunnitella tietoturvallisuuden kehittämistä lähivuosien osalta.

Ohjeessa tulisi tuoda paremmin esille se, miten sellaisen organisaation, joka käyttää itse ja tarjoaa myös palveluita laajalle asiakaskunnalle, tulisi perus- ja korotetun tietoturvatason tekninen ympäristö toteuttaa. Kuinka tulisi esimerkiksi huomioida ja rajata organisaation puhtaasti omaan käyttöön, välillisesti tai kokonaan asiakkaille tarjottavat palvelut siten, että ne eivät estä esimerkiksi korotetun tason saavuttamista. Käytännön esimerkki korotetun ja perustason teknisestä ympäristöstä, jossa selkeästi on rajattu yhteys- ja tietoliikennepisteet eri tasoille, helpottaisi teknisen arkkitehtuurin suunnittelua.

Valtiokonttori näkee keskeisenä haasteena sen, miten organisaatiossa voidaan rajata perus- ja korotetun tason käyttöön tarkoitetut tekniset ympäristöt siten, että korotetusta tietoturvatasosta ei tule de facto tietoturvatasoa, sen takia, että organisaation muutama keskeinen tietojärjestelmä ja niitä tukeva infrapalvelu sitä edellyttää.

Suojattavan kohteen / ICT-järjestelmän tietoturvatasoja määritettäessä erittäin tärkeässä roolissa on tietoaineistojen luokittelu, joka määrää minimitason, mitä suojattavan kohteen tulee täyttää. Näemme, että tietoturva-asetuksen osalta haasteeksi muodostuu se, miten virasto voi toimittaa ST III-tietoaineistoja

Sörnäisten rantatie 13, Helsinki | PL 14, 00054 VALTIOKONTTORI
Puh. (09) 77251, Faksi (09) 7725 208, www.valtiokonttori.fi

toiselle virastolle, joka ei ole tehnyt tietoturvallisuusasetuksen mukaista luokituspäätöstä ja varmistua tällöin siitä, että myös vastaanottava viranomainen käsittelee saamansa tietoa tietoturva-asetuksen edellyttämällä, korotetun tietoturvatason vaatimukset täyttävällä tavalla.

Ohjeessa käydään läpi kattavasti pilvipalveluiden tuottamiseen liittyvät tuotantomallit. On ymmärrettävää, että on lähes mahdotonta tuottaa ja ottaa huomioon kattavasti tiedon luottamuksellisuudessa, eheydessä ja saatavuudessa tarvittavat kontrollit erilaisissa jaetun kapasiteetin mallilla tuotettavissa virtualisoiduissa palveluissa, mutta tyypillisimpien käyttöpalvelutuotantomallien hyödyntämistä ja mahdollisia lisähaasteita tulisi edelleen purkaa auki yksityiskohtaisemmalla tasolla.

Mitä enemmän perustietotekniikkaan liittyviä tukipalveluita keskitetään palvelukeskuksiin, sitä vähemmän organisaation vastuulle jää teknisten ratkaisuiden tietoturvallisuuden toteuttaminen. Tuolloin organisaation kannalta pääpaino jää hallinnollisten vaatimusten toteuttamiseen.

Tämän takia palveluiden keskittämistä ml organisaatioiden ydintoimintaan liittyvien tukipalveluiden tuottaminen tulisi valtionhallinnossa edelleen jatkaa, koska useiden pienten virastojen kyky ja kustannustehokkuus toteuttaa esimerkiksi korotetun, puhumattakaan korkean tietoturvatason teknistä ympäristöä on puutteellinen. Tällöin aikaisemmin kuvattu haaste tietoaineistojen välittämisessä organisaatioiden välillä pienentyy, koska teknisesti voidaan varmistua tarvittavasta tietoturvatasosta palvelukeskuksen vastatessa teknisestä tietoturvallisuudesta.

Nyt voimassa olevat tietoturvatasovaatimukset saattavat estää SaaS -toimintamallia käyttävien perus- tai korotettua tietoturvatasoa edellyttävien ICT-palveluiden hankkimisen riippuen toimittajan käyttämästä tuotantomallista. Tämän johdosta on toivottavaa, että tietoturvatasojen vaatimusten päivityksessä huomioidaan se, että korvaavaa menettelyä voitaisiin käyttää laajemmin yksittäisen vaatimuksen sijaan, kuitenkin tiedostaen ne puutteet ja mahdolliset riskit, mitä tällainen tuotantomalli aiheuttaa.

Ohjeen ehkä tärkein työväline on liitteessä neljä oleva tärkeysjärjestystyöväline. Valtiokonttori on käyttänyt työvälinettä apuna luokiteltaessa Valtiokonttorin käyttämiä sisäisiä ja asiakkaille tarjottavia ulkoisia palveluita. Olisi toivottavaa, että valtiovarainministeriö edellyttäisi virastoja laatimaan omistamistaan tietojärjestelmistä tämän luokittelun, koska se helpottaisi osaltaan organisaatioiden välistä tietojenvaihtoa sekä käyttöpalvelutoimittajia priorisoimaan heidän valtionhallintoon tarjoamien ja tuottamien palveluiden jatkuvuus- ja toipumisprosesseja häiriötilanteiden yhteydessä.

Liitteiden 1-3 osalta Valtiokonttori esittää, että tässä olevat vaatimukset ovat esimerkkejä kontrolleista, joilla näitä vaatimuksia voidaan täyttää eivätkä sellaisenaan velvoittavia. Taulukoissa olevien ohjeiden lisäksi tulisi taulukkoon mahdollistaa viraston omien kontrollien syöttäminen, joilla virasto osoittaa täyttävänsä kyseisen vaatimuksen.

Sörnäisten rantatie 13, Helsinki | PL 14, 00054 VALTIOKONTTORI
Puh. (09) 77251, Faksi (09) 7725 208, www.valtiokonttori.fi

10.1.2012

Liitteessä 7 on kuvattu etäkäyttöön liittyviä teknisiä vaatimuksia. Toteamme, että tähän yhteyteen olisi hyvä tuoda esille se mahdollisuus, että organisaatio voi toteuttaa nämä vaatimukset usealla erilaisella teknisellä ja hallinnollisella toimintatavalla.

Pääjohtaja Timo Laitinen

Tietohallintoyksikön johtaja Juha Pietarinen