Valtiokonttori
Hallinto ja kehittäminen
Riskienhallinta

4.7.2014

Valtiovarainministeriölle

Lausuntopyyntönne VM047:21/2007

Valtiokonttorin lausunto tietoturvallisuuden arviointiohjeesta

Organisaation laadukkaan ja toimivan tietoturvallisuuden kehittäminen ja ylläpitäminen edellyttävät riittävää ja oikeaa kuvaa organisaation tietoturvan käytännön toteutumisesta. Tämä edellyttää säännöllisten arviontien tekemistä oman toiminnan tietoturvallisuuden tasosta ja toimivuudesta. Valtiokonttori pitää tärkeänä, että organisaatiolla on käytettävissään käytännönläheinen ohje ja mallit arviointien toteuttamiseen joko itsearviointina tai ulkopuolisen tahon toteuttamana.

Ohje on pitkä ja sen alussa on varsin laaja taustoittava osuus ja vasta sivulta 26 alkaa varsinaisen arvioinnin toteuttamisen kuvaaminen. Pitkä taustoittavan osuuden lukeminen saattaa vähentää kiinnostusta lukea ohje loppuun ja päästä itse asiaan. Valtiokonttori ehdottaa, että taustoittavasta osasta laadittaisiin ohjeen alkuun lyhyt tiivistelmä ja laajempi osuus olisi liitteenä.

Luonnoksen kohdassa tietoturvallisuusasetuksen tasovaatimukset (s. 13) todetaan, että "korotetun ja korkean tason arvioinneissa on siten painotettava tietojen käsittelyn kokonaisuutta, eikä välttämättä kaikkien yksittäisten tietoturvatasovaatimusten toteutumista. Arvioinnin kohteen johto tekee viime kädessä päätöksen riittävän tason saavuttamisesta ja hyväksyy jäännösriskit liittyen yksittäisten tietoturvavaatimusten toteuttamatta jättämiseen." Tämä on Valtiokonttorin mielestä tärkeä asia, joka korostaa johdon roolia tietoturvallisuuden tason määrittelyssä ja jäännösriskin hyväksymisessä. Sen vuoksi tätä asiaa voisi korostaa jo ohjeen johdannossa ja tarvittaessa tuoda selvemmin esille myös ohjeen muissa osissa.

Kohdassa tietoturvallisuuden arviointi järjestelmähankkeissa (s.24) viitataan Vahti 1/2013 ohjeeseen ja todetaan, että korotetun tason sovelluksen tietoturvallisuus on auditoitava ennen käyttöönottoa, käytettävä automaattisia ja manuaalisia menetelmiä sekä ulkopuolista auditoijaa. Selvyyden vuoksi olisi syytä mainita, ovatko nämä tämän ohjeen perusteella ehdottomia vaatimuksia, kuten sanamuodosta voi päätellä vai ohjeen mukaisia suosituksia?

Ohjeluonnoksessa on lyhyesti mainittu eri arviointitavat: itse-, sisäinen, vertais- ja ulkoinen arviointi. Luonnoksessa ei ole kuitenkaan kuvattu, missä tilanteissa eri tapoja voisi soveltaa ja miten arvioinnin toteuttaminen eroaa käytettäessä eri arviointitapoja. Ulkoisilla arvioitsijoilla on yleensä omat arviointimallit, joita he käyttävät niin yksityisiä kuin julkisia toimijoita arvioidessaan. Sen vuoksi tässä ohjeessa olisi hyvä tuoda selkeästi esille, mitä edellytyksiä julkisen tahon on ulkopuoliselle arvioitsijalle asetettava. Tämän voisi esittää esimerkiksi liitteeksi liitettävän vaatimusluettelon muodossa.

Valtiokonttori
Statskontoret
State Treasury

Sörnäisten rantatie 13, Helsinki | PL 14, 00054 VALTIOKONTTORI
Puh. 0295 50 2000, Faksi 0295 50 3333, www.valtiokonttori.fi

4.7.2014

Kuten lausuntomme alussa toteamme, pidämme tietoturvallisuuden arviointien toteuttamista tärkeänä ja ohjeluonnoksessakin todetaan, että usein liikkeelle kannattaa lähteä itsearvinoinnilla ennen ulkopuolisen auditoinnin toteuttamista. Jotta myös niiden virastojen, joilla ei itsellään ole käytettävissään riittävää tietoturvaresurssointia, kynnys itsearviointien toteuttamiseen saataisiin vieläkin matalammaksi, ohjeeseen tulisi lisätä arvioinnin toteuttamisen kuvauksen lisäksi myös selkeät ja yksinkertaiset työkalut, mallit, taulukot, luettelot tms., joiden avulla itse- tai sisäisen arvioinnin toteuttaminen tehtäisiin mahdollisimman helpoksi ja näin arviointien määrä valtionhallinnossa saataisiin entisestään lisättyä.

Timo Laitinen
Pääjohtaja

Juha Pietarinen
Riskienhallintajohtaja