Valtiovarainministeriö

Lausuntopyyntö 13.6.2014 (VM047:21/2007)

Sisäministeriön lausunto luonnokseksi tietoturvallisuuden arviointiohjeeksi

Valtiovarainministeriö on pyytänyt sisäministeriön lausuntoa Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän VAHTI:n ohjauksessa valmistellusta luonnoksesta tietoturvallisuuden arviointiohjeeksi.

Sisäministeriö toteaa asiassa lausuntonaan seuraavaa.

Yleistä

Ohjeluonnoksen johdannossa todetaan, että ohje on tarkoitettu valtionhallinnon viranomaisille, joiden tulee säännöllisesti arvioida organisaationsa tietoturvallisuuden tilaa sekä toteutettujen toimenpiteiden asianmukaisuutta ja riittävyyttä. Sisäministeriö esittää, että ohjeen kohderyhmää koskevaa kirjausta täsmennetään ja tämän jälkeen ohjeen arvioidaan uudelleen sen pohjalta.

Ohjeessa painotetaan huomattavasti Viestintäviraston viranomaistarkastustyyppistä auditointia ja hyväksyntäprosessia, vaikka valtaosa tarkastuksista valtionhallinnossa on sisäministeriön käsityksen mukaan itse arviointia tai viranomaisen ulkopuoliselta toimittajalta tilaamaa tarkastustyötä. Tätä painotusta olisi sisäministeriön näkemyksen mukaan hyvä arvioida uudelleen. Nyt ohjeluonnoksesta saattaa saada sen käsityksen, että viranomainen ei itsenäisesti saisi tarkastaa omia järjestelmiään tai toimintaansa. Tämä ei liene ohjeen tavoitteena.

Ohjeluonnoksen viranomaistarkastuksiin liittyvissä kohdissa on jonkin verran epätarkkuuksia ja niiden paikkaansa pitävyys voisi olla syytä varmistaa kansalliselta turvallisuusviranomaiselta.

Ohjeessa käytettävään käsitteistöön olisi hyvä kiinnittää jatkovalmistelussa huomiota. Ohjeluonnoksessa käytettään käsitteitä auditointi ja arviointi vaihtelevasti ja niillä viittaavat useissa kohdin samaan asiaan, vaikka ne ovatkin määrittelyissä mukana. Ohjeessa voisi olla hyvä mahdollista kiinnittää esimerkiksi käsite "*viranomaistarkastus*" kuvaamaan DSA:n tekemää hyväksyntä- tai muuta vastaavaa auditointia ja "*tarkastus*" kuvaamaan viranomaisen itse tekemää tai ulkopuoliselta tilaamaa auditointia, joka ei johda ohjeessa mainittuun viranomaishyväksyntään.

Sisällysluettelon mukaista asioiden käsittelyjärjestystä voisi olla sisäministeriön näkemyksen mukaan hyvä arvioida uudelleen. Eri tarkastustyypit ja niihin liittyvä käsitteistö olisi hyvä kuvat jo ohjeen alkupuolella.

Yksityiskohtaisia huomioita

Johdanto

- Kappale 1: "Tämä ohje on tarkoitettu valtionhallinnon viranomaisille, joiden tulee säännöllisesti arvioida…" Lainsäädännössä mahdollisesti asetettuun yleiseen vaatimukseen tulisi viitata. Jos tässä kohdassa tarkoitetaan erityisiä tahoja, joilla tällainen vaatimus on, myös sen voisi tuoda esiin.

- Kappale 2, rivi 2 "lainsäädännöllinen velvoite": Tulisiko tässä kohdassa viitata siihen, miltä osin tietoturvatyön lähtökohtana tulee olla tietoisuus tietoturvallisuuden tasosta tai vaihtoehtoisesti muotoilla virka toisin.

Postiosoite:
Sisäministeriö
PL 26
00023 Valtioneuvosto

Käyntiosoitteet:
Kirkkokatu 12, Helsinki
Vuorikatu 20, Helsinki

Puhelin:
Vaihde
0295 480 171
Faksi:
09 1604 4635

Virkasähköpostiosoite:
kirjaamo@intermin.fi
www.intermin.fi

18.08.2014

Tausta

- Sivu 5, kappale 2: Kappaleessa tuodaan esiin melko vahvasti olettamus viranomaisten epätietoisuudesta arviointien tekemisessä. Virke tulisi pyrkiä muotoilemaan uudelleen.

Edellytykset tietoturvallisuuden arvioinnille

- Sivu 5, kappale 1: ISO/IEC27001 standardi saattaa olla vieras osalle lukijoista. Tulisiko avata ensimmäisen kerran käytettäessä?

- Sivu 5, kappale 1: "Organisaation tulee laatia oman tietoturvallisuuden hallintajärjestelmän…" Virkkeessä mainitaan suuri määrä erilaisia asiakirjoja ja suunnitelmia joiden tulee olla laadittuna jo ennen arvioinnin aloittamista. Tietoturvan arviointi voitaneen kuitenkin todellisuudessa aloittaa jo ennen kuin nämä asiakirjat on laadittu, erityisesti silloin, kun tunnistetaan tietoturvallisuuden nykytila.

- Sivu 6, kappale 2: Tulisiko erityyppiset arvioinnit kuvata ensin?

- Sivu 6, kappale 4: Kustannusten jakaantumisen osalta lienee useampia vaihtoehtoisia tapoja. Tarkastuksista ja niiden kustannuksista voi vastata esimerkiksi aina yksi taho tai kustannukset jaetaan eri toimijoiden kesken. Ei liene tarkoituksenmukaista kiinnittää vain yhtä tapaa ohjeeseen.

Laki tietoturvallisuuden arviointilaitoksista

- Sivu 9, kappaleet 2 ja 3: Ohjeluonnoksessa esitetään tältä osin varsin seikkaperäinen kuvaus. Onko tarkoituksenmukaista näin yksityiskohtaisesti esim. arviointilaitosten vaatimuksia?

Julkisia hankintoja koskeva lainsäädäntö

- Luku kokonaisuutenaan liittyy sisällöltään varsin niukasti ohjeen otsikkoon. Onko relevanttia kuvata hankintalainsäädäntöä arviointiohjeessa tällä tarkkuustasolla?

Tietoturvallisuuden ohjausta koskeva lainsäädäntö

- Ks. edellinen kommentti.

Tietoturvallisuuden arviointiperusteet

- Luvusta puuttuu kuvaus siitä, että erilaisia perusteita tulee aina soveltaa tarkastuskohteeseen nähden. Tarkastuskriteerit tulee valita sillä perusteella mitä tarkastetaan.

- Lukuun voisi lisätä kappaleen siitä, että virastoilla voi olla omia tietoturvavaatimuksia, joita viraston johto on hyväksynyt ja joita vasten toimintaa tarkastetaan. Vaatimusten tulee toki pohjautua voimassa olevaan normistoon.

- Lukuun voisi lisätä myös kappaleen jossa kuvattaisiin myös yleisimpiä kansainvälisiä arviointikriteeristöjä, vaikka esimerkein siitä, mihin ne soveltuvat. Nyt on avattu käytännössä vain ISO27001, KATAKRI ja VAHTI 2/2010. Lukijan on hyvä ymmärtää ero lopputuloksessa jos tarkastus tehdään verkkopalveluun OWASP TOP10 haavoittuvuuksien tai tietoturvatasojen mukaan.

Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyiden arviointi

- Sivu 16, kappale 2: "Tietojärjestelmien arviointia koskevan lain mukaisia arviointeja voivat tehdä vain Viestintävirasto…" Kappaleen vaatimukseen tulisi liittää viite, mistä mainittu vaatimus tulee.

- Sivu 17, kappale 1: "Viranomaiset voivat kuitenkin…" Kappaleen vaatimukseen tulisi liittää viite, mistä mainittu vaatimus tulee.

- Luvussa tulisi käydä asianmukaisesti ilmi myös Viestintäviraston mandaatti ja sen rajaukset. Nyt kuvaus antaa ehkä turhankin laajan kuvan Viestintäviraston mandaatista.

Tietoturvallisuuden arviointilaitokset

- Sivu 20, kappale 1: Tulisi lisätä asianmukainen viite.

Arviointityypit

- Luvun sijoittaminen ohjeeseen tulisi arvioida uudelleen. Sijainti voisi olla parempi ohjeen alussa.

Tietoturvallisuuden arviointi järjestelmähankkeissa

- Sivu 24, kappale 2: "Tyypillisiä auditointikohteita ja vaiheita ovat…" Tulisiko lisätä myös merkittävissä muutoksissa tehtävä auditointi ja/tai säännöllinen uusinta-auditointi.

Arvioinnin seuranta

- Tulisiko lisätä kappale, jossa mainitaan toimenpiteiden vastuuttamisen tärkeydestä.

Liite 1, käsitteistö

- Tässä yhteydessä kannattaisi arvioida tarkasti arvioinnin, auditoinnin, tarkastuksen, viranomaistarkastuksen ja -hyväksynnän ero.
- Luettelomainen liite voisi olla paremmin luettavissa aakkosjärjestyksessä.

Liite 2, Muut arviointeja ja tarkastuksia suorittavat viranomaiset

- Tässä yhteydessä tulisi selvittää, onko Valtori tosiasiallisesti listalla tarkastuksia suorittava viranomainen vai palvelukeskus, joka on kilpailuttanut yritysten palveluita hankittavaksi.
- Tulisiko avata myös FINAS ja Poliisin (Poliisihallituksen) rooli (esim. turvallisuusalan valvonta ja arpajais- ja rahankeräysvalvonta)?

Kansliapäällikkö Päivi Nerg

Neuvotteleva virkamies Henri Helo

Asiakirja on sähköisesti allekirjoitettu asianhallintajärjestelmässä. Sisäministeriö SM 18.08.2014 klo 07:38. Allekirjoituksen oikeellisuuden voi todentaa kirjaamosta.

Tiedoksi

Poliisiosasto
Pelastusosasto
Rajavartiolaitoksen esikunta
Maahanmuutto-osasto
Tietoturvapäällikkö Samuli Bergström
Tietopalvelupäällikkö Manu Herna