Valtiovarainministeriö

VM047:2112007, 1862/00.01.00.0112012

Poliisihallituksen lausunto Valtiovarainministeriölle tietoturvallisuuden arviointiohjeen luonnoksesta

1 Taustaa

Valtiovarainministeriö on pyytänyt kirjeellään Poliisihallituksen lausuntoa tietoturvallisuuden arviointiohjeen luonnoksesta. Poliisihallituksen lausunto sisältää myös Valtiovarainministeriön kirjeen jakelussa mainittujen poliisiyksiköiden lausuttavat asiat.

2 Yleiset kommentit

Poliisihallitus lausuu arviointiohjeen luonnoksesta seuraavaa. Lausunnolle toimitettu arviointiohjeen luonnos on hyvin laadittu kokonaisuus, joka tulee oikeaan tarpeeseen monissa virastoissa. Ohjeen luonnoksessa on selkeästi avattu mm. lainsäädäntöön ja arviointikriteeristöön liittyvät kohdat. Lisäksi ohjeessa on kuvattu hyvin koko tarkastusprosessin kulku.

Poliisihallituksessa on tehty jo pitkään omien tietojärjestelmien tarkastustyötä. Luonnoksessa kuvattu prosessi ja kuvatut käytänteet sopivat varsin hyvin yhteen Poliisihallituksen käytäntöjen kanssa.

3 Yksityiskohtaiset kommentit

Sivu 8: Kappaleessa "Laki tietoturvallisuuden arviointilaitoksista" on kuvattu kattavasti ko. asiaan liittyvä kokonaisuus. Kohtaan voisi laittaa maininnan mistä tiedot hyväksytyistä laitoksista julkaistaan.

Ohjeluonnoksessa (muun muassa sivu 9) on viitattu eduskunnan valmistelussa olevaan lakiin turvallisuusselvityksistä ja sen esitöihin. Näiltä osin tulee ennen ohjeen voimaantuloa varmistaa, ettei lain valmistelumateriaaliin tai säännöksiin ole tullut muutoksia valiokuntakäsittelyn kuluessa.
Tämä huomio koskee esimerkiksi luonnoksen sivulla 19 viitattuja turvallisuusselvityksiä ja sivulla 20 viitattuja yritysturvallisuusselvityksiä.

Sivu 11: Voisiko tässä kohdassa avata tarkemmin tietoturvavaatimuksien laadintaan liittyviä asiakokonaisuuksia, esim. valtion yhteisten tietoturvavaatimusten käyttö ja organisaation omien tietoturvavaatimusten käyttö.

POLIISIHALLITUS
Vuorikatu 20 A, PL 302, 00101 HELSINKI
kirjaamo.poliisihallitus@poliisi.fi
Puh. +358 295 480 181, Faksi +358 295 411 780

Sivu 13: Kappaleessa "Tietoturvallisuusasetuksen tasovaatimukset" todetaan, että "Arvioinnin kohteen johto tekee viime kädessä päätöksen riittävän tason saavuttamisesta ja hyväksyy jäännösriskit liittyen yksittäisten tietoturvallisuusvaatimusten toteuttamatta jättämiseen." Tässä yhteydessä olisi perusteltua edellyttää ja mainita, että päätöksen tulisi olla kirjallinen. Sama huomio koskee myös sivulla 17 viitattua tietojen luovutusta koskevaa päätöstä.

Sivu 14: Katakrin osalta yhtenä käyttötapana voisi mainita turvallisuusviranomaisten tapa auditoida mm. omat palvelutoimittajat ja tietojärjestelmät Katakin vaatimusten mukaisesti.

Sivu 16: Sivun viimeisessä kappaleessa mainitaan, että auditointeihin saa käyttää 1.6.2015 lähtien vain tietojärjestelmien arviointia koskevan lain mukaisesti hyväksymiä arviointilaitoksia. Toisaalla luonnoksessa on mainittu, että ko. velvoite tulee voimaan 2015 alusta alkaen (sivu 20).

Sivu 18: Hankinnoissa on luonnollisesti huomioitava myös ko. organisaation omat hankinta- ja hankintojen tietoturvaohjeet.

Sivu 18: sivun toiseksi viimeisessä kappaleessa mainitaan, että valtiohallinnon palvelukeskus voi suorittaa tarjoamaansa palveluun tietoturvallisuuden arvioinnin ennen palvelun käyttöönottoa. Tavoite on, että samaa palvelua ei olisi tarpeen auditoida eri virastojen käyttöönottojen yhteydessä. Tässä keskeinen huomioitava seikka on, että auditoinnit kaikille riittävien vaatimusten mukaisesti. Järjestelmän audioitiminen perustason vaatimusten mukaisesti ei riitä esim. poliisille.

Sivu 20: Sivun viimeisessä kappaleessa mainitaan, että auditointeihin saa käyttää 2015 lähtien vain tietojärjestelmien arviointia koskevan lain mukaisesti hyväksymiä arviointilaitoksia. Toisaalla luonnoksessa on mainittu, että ko. velvoite tulee voimaan 1.6.2015 alusta alkaen (sivu 18).

Sivu 23: Ensimmäisen kappaleen lopussa voisi muistuttaa, että kilpailutuksiin tulee sisällyttää ko. palvelua koskevat yksityiskohtaisemmat tietoturvavaatimukset.

Sivu 24: Tietojärjestelmien auditointivaatimus tulee sisällyttää jo kilpailutuksessa järjestelmän tai palvelun tietoturvavaatimuksiin.

Sivu 24: Tietoturvallisuuden arvioinnista järjestelmähankkeissa on turvallisuusviranomaisilla, kuten poliisilla, olemassa omat tarkentavat ohjeet. Tässä kohdassa voisi mainita, että asiaa tulee tarkentaa vielä organisaation omilla ohjeilla.

Sivu 25: Kohdan "Tietoturva-auditointien suunnittelu ja toteuttaminen" ensimmäisessä kohdassa mainitaan: "Arvioija voi antaa myös suosituksia poikkeaman korjaamiseksi". Poliisihallitus kokee tällaisen toiminnan erittäin positiivisena asiana. Tällä hetkellä ko. suosituksia saa kaupallisilta toimijoilta, mutta esimerkiksi Viestintävirasto ei asemaansa vedoten voi aina antaa korjausehdotuksia. Tilanne on nykyisessä toimintamallissa hieman hankala ja tähän menettelytapaan toivotaankin parannusta.

Sivu 31/32: Liite1/Käsitteistö vaikuttaa paikoittain keskeneräiseltä.

Ohjeluonnoksen liitteessä 1 on määritelty ohjeen sisältämiä keskeisiä käsitteitä, kuten "arviointi", "tarkastus" ja "auditointi". Näiden käsitteiden erot ovat ohjeessa kuitenkin joitain osin epäselviä. Joissakin ohjeen kohdissa kyseisiä käsitteitä on käytetty päällekkäin tai sekavasti, vaikka niitä ei ole liitteessä 1 määritelty toistensa synonyymeiksi. Esimerkiksi sivulla 24 kappaleessa "Tietoturvallisuuden arviointijärjestelmähankkeissa" todetaan, että "Tietojärjestelmähankkeissa auditointimahdollisuus tulee varmistaa etukäteen jo ennen hankkeen käynnistämistä." Kappaleen otsikossa puhutaan arvioinnista ja kappaleen tekstissä auditoinnista ja lisäksi kappaleessa käsitteitä on käytetty rinnakkain "Vaatimusmäärittelyn auditointi/arviointl'. Luonnoksen sivulla 25 on käsitelty yksityistä yritystä arvioinnin toteuttajana, vaikka käytännössä puhutaan yleensä auditoinnista. Sivulla 26 puhutaan arviointiprosessista, mutta toisaalta myös auditointien vaiheista ja sivulla 29 arviointiraportista mutta toisaalta myös auditoinnin kulusta. Käsitteiden erilainen käyttö voi aiheuttaa sekaannusta, joten ohjeessa tulisi varmistaa se, että eri käsitteitä on käytetty siten, etteivät ne sekoitu keskenään. Ohjeluonnoksen liitteessä 1 joitakin käsitteitä on jäänyt määrittelemättä kokonaan (ulkoinen arviointi, vaatimus, kriteeri).

Poliisihallituksella ei ole muuta lausuttavaa tietoturvallisuuden arviointiohjeen luonnoksesta.

Turvallisuuspäällikkö Kari Santalahti

Tietoturva-asiantuntija Tomi Moilanen

Asiakirja on sähköisesti allekirjoitettu Aspo-asianhallintajärjestelmässä. Poliisihallitus 11.08.2014 klo 09.36. Allekirjoituksen oikeellisuuden voi todentaa kirjaamosta.

Liitteet -

Jakelu Valtiovarainministeriö

Tiedoksi -