VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Tietojärjestelmien vaatimustenmukaisuuden arviointi

Lainsäädäntöneuvos Eeva Lantto
Julkisen hallinnon tietojärjestelmien yleissääntelyä kehittävän työryhmän kokous 15.6.2021

Nykytila

Sääntely ja toimivaltaiset viranomaiset
Käytäntö

Nykytila - Sääntely ja toimivaltaiset viranomaiset

- Arviointilaki (viranomaisten tietojärjestelmien tietoturvan arviointi)
  - Liikenne- ja viestintävirasto
- Arviointilaitoslaki (tietoturvan arviointilaitosten hyväksyntä)
  - Liikenne- ja viestintävirasto (SUPOn mahd. lausunto) ja FINAS
- L kv tietoturvallisuusvelvoitteista (yritysturvallisuusselvitystodistus)
  - UM, PLM, PE, SUPO, Liikenne- ja viestintävirasto
- Turvallisuusselvityslaki (yritysturvallisuusselvitys ja –todistus)
  - SUPO, PE, Liikenne- ja viestintävirasto
- Asiakastietolaki ja toisiolaki (vaatimukset, tietoturvallisuus-vaatimustenmukaisuuden arviointi, toimijoiden valvonta)
  - THL ja Valvira sekä arviointilaitokset

Nykytila – Sääntely ja toimivaltaiset viranomaiset

- Yleinen tietosuoja-asetus (sertifiointielimien hyväksyminen)
  - tietosuojavaltuutettu
- EU:n kyberturvallisuusasetus (vaatimustenmukaisuusilmoitusten valvonta ja seuranta, vaatimustenmukaisuuden arviointilaitosten valtuuttaminen, valvonta ja seuranta sekä korkean tietoturvatason kyberturvallisuussertifikaattien myöntäminen)
  - Liikenne- ja viestintävirasto

Nykytila - Käytäntö

- arviointilaitosten (3 kpl) pätevyysalueet ylimmillään TL III, lisäksi asiakastietolain ja toisiolain mukaiset arvioinnit
- tyypillisesti kansallisten tietojen käsittelyyn käytettyjen tietojärjestelmien arvioinnissa tilataan arviointilaitoksen arviointiraportti, jonka jälkeen viranomaisen jäännösriskien arviointi ja omahyväksyntä
- kansallisille arvioinneille on vain harvoin haettu arviointilaitoksen tai Liikenne- ja viestintäviraston todistusta
- vaatimustenmukaisuuden arvioinnissa hyödynnetään ”epävirallisia” kriteeristöjä, kuten NSA:n Katakri-kriteeristö (ja vanhentuneet VAHTI-ohjeet), jonka Liikenne- ja viestintävirasto (tilaajat?) on arvioinut soveltuvan myös kansallisten tietoturvallisuusvaatimusten arviointiin

Nykytila - Käytäntö

- arviointilaitoslaissa säädetyt edellytykset arviointilaitoksen hyväksymiselle ovat hyvin yleisluontoiset. Tämä on johtanut siihen, että hyväksyntä perustuu suurelta osin Liikenne- ja viestintäviraston antamaan ohjeeseen tietoturvallisuuden arviointilaitoksille (Ohje 210/2016 O) – eli ei sitovaan normistoon
- toiminnan/tietojärjestelmien jatkuvuudelle ja varautumiselle ei konkreettisia vaatimuksia
- ei ole säädetty (olennaisista) vaatimuksista, jotka koskisivat hallinnon APT-tietojärjestelmiä - erityisesti, kun niillä tehdään etuja, oikeuksia ja velvollisuuksia koskevia päätöksiä tai ne muuten vaikuttavat suoraan hallinnon asiakkaan oikeudelliseen asemaan, kuten palveluihin pääsyyn
  - ei ole säädetty myöskään vaatimustenmukaisuuden arvioinnista

Kehittämistarpeet

- Arviointilakien soveltamisala
- Vaatimustenmukaisuutta arvioivat viranomaiset
- Arviointilaitosten hyväksyminen, hyväksyjä ja valvonta
- Vaatimustenmukaisuuden osoittaminen
- Tietoturvallisuutta ja tietojärjestelmiä koskevat vaatimukset
- Tietojärjestelmän vaatimustenmukaisuuden arviointiprosessi
- Vastuukysymykset

Arviointilakien (arviointilaki ja –laitoslaki) soveltamisala

- *pitäisikö säätää arviointilaki ja arviointilaitoslaki koskemaan laajemmin tietojärjestelmiin kohdistuvien vaatimustenmukaisuuden arviointia*
- *vaihtoehtoisesti arviointilaitoslaki voitaisiin jättää ennalleen ja säätää arviointilaissa laajemmin viranomaisten tietojärjestelmien vaatimustenmukaisuuden (viranomaisen suorittamasta/viranomaisen johdolla suoritettavasta) arvioinnista*
- *pitäisikö mahdolliset viranomaisille pakolliset arvioinnit tehdä arviointilain mukaista menettelyä noudattaen*
- *miltä osin APT-toiminnallisuuksia voi ylipäätään arvioida ulkopuolinen arvioija (viranomaisen vastuu päätöksentekosäännöistä ja –logiikasta)*

Vaatimustenmukaisuutta arvioivat viranomaiset

- *Liikenne- ja viestintävirasto on ehdottanut, että sen arvioinnit sisältäisivät lisäksi arvioitavaan tietojärjestelmään liittyvän turvallisuusjohtamisen sekä salaustuotteiden arvioinnin*
- *mikäli viranomaisten tietojärjestelmien (pakollisia arviointeja) tehtäisiin vain arviointilain mukaisesti, ei Liikenne- ja viestintäviraston käyttämiä arviointiperusteita voida rajata (vain ylimpiin) turvallisuusluokkiin*
- *Liikenne- ja viestintävirasto voisi käyttää apunaan yksityisiä henkilöitä (arvioija tms.), jotka täyttävät arvioijalle asetetut pätevyysvaatimukset*
  - *arvioijan pätevyysvaatimukset*
  - *julkinen hallintotehtävä*

Vaatimustenmukaisuutta arvioivat viranomaiset

- *pitäisikö viranomaisen (tietojärjestelmien) tietoturvallisuuteen liittyvä fyysisen turvallisuuden arviointi säätää (myös kansallisella tasolla) SUPOn tehtäväksi*
- *PV on ehdottanut, että PV olisi arviointiviranomainen vastuualueenaan maanpuolustukseen liittyvien TL-tietoa käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden (ml. jatkuvuus ja varautuminen) arviointi ja hyväksyntä sekä salaustuotteiden hyväksyntä*
  - *tämä edellyttäisi muutoksia myös turvallisuusselvityslakiin*
- *mikä viranomainen olisi toimivaltainen arvioimaan mahdollisia automaattisen päätöksentekoon liittyviä vaatimuksia*
- *viranomainen voisi käyttää apunaan yksityisiä henkilöitä (arvioija tms.), jotka täyttävät arvioijalle asetetut pätevyysvaatimukset.*
- *tietosuojavaltuutetun ja mahdollisten sertifiointielinten rooli?*

Arviointilaitosten hyväksyminen (hyväksymiskriteerit ja –prosessi), hyväksyjä ja valvonta

- *arviointilaitoslaissa tulisi asettaa sekä arviointilaitokselle että sen palveluksessa olevalle arvioitsijalle yksilöidyt vaatimukset, joita voidaan lakitasoiseen sääntelyyn perustuen valvoa*
- *arviointilaitoslain viranomaistoimijoilla tulisi olla selkeä ja perusteltu toimivalta päättää akkretoinnista ja suorittaa kelpoisuusvaatimusten noudattamista koskevaa valvontaa*
- *mikäli arviointilaitoksia käytettäisiin viranomaisten APT-tietojärjestelmien arviointiin, arviointilaitoslain sääntelykohde tulisi olla tietojärjestelmien arviointi tietoturvallisuuden arvioinnin sijaan*
  - *arviointilaitos voisi toimia pelkästään esim. tietoturvallisuuden arviointilaitoksena tai tietojärjestelmien arviointilaitoksena*
- *PL 124 §:stä johdettavat sääntelyvaatimukset arviointilaitoksille*

Arviointilaitosten hyväksyminen (hyväksymiskriteerit ja –prosessi), hyväksyjä ja valvonta

- *tietojärjestelmien tietoturvallisuuteen keskittyville arviointilaitoksille voitaisiin (nykyisen käytännön mukaan) antaa pätevyysalueeksi arvioida TL IV ja III sekä salassa pidettäviä ja julkisia tietoja käsittelevien tietojärjestelmien tietoturvallisuutta*
- *arviointilaitoksia hyväksyvälle taholle säädettäisiin velvollisuus pitää yllä lain soveltamisalaa vastaavaa kuvausta mahdollisista arviointilaitosten pätevyysalueista sekä pätevyysalueelle hyväksymisen vaatimuksista/kriteereistä*
- *arviointilaitosten hyväksyntäprosessi, hyväksyntävastuu ja valvonta (FINASin rooli,TSV:n rooli). Asia edellyttänee poliittista linjausta*
  - *turvallisuusselvityslain mukaisen yritysturvallisuusselvityksen merkitys hyväksynnässä/akkreditoinnissa*

Arviointilaitosten hyväksyminen (hyväksymiskriteerit ja –prosessi), hyväksyjä ja valvonta

- *pitäisikö viranomaisten tietojärjestelmien (ainakin pakolliset) arvioinnit tehdä arviointilain mukaisena viranomaistoimintana, jossa arviointiviranomainen voisi käyttää arvioinnissa apunaan yksityisiä määritetyn ammattipätevyyden täyttäviä arvioijia*
  - *pätevyysvaatimukset arvioijille*
- *säännökset arviointilaitoksen lopettaessa tai luovuttaessa toimintansa toiselle*

Vaatimustenmukaisuuden osoittaminen

- *tulisiko vaatimustenmukaisuuden arviointi ja hyväksyntä säätää osin pakolliseksi (kuten asiakastietolaissa), esim.*
  - *tietoturvallisuuden (korkeimmat turvallisuusluokat)*
  - *oikeusturvan (automaattinen päätöksenteko) taikka*
  - *jatkuvuuden*

kannalta kriittisimmät järjestelemät

- *nämä tulisi määritellä yksiselitteisesti laissa. Lisäksi olisi arvioitava velvoitetta säännöllisiin seuranta-arviointeihin*
- *velvoittavan sääntelyn kustannusvaikutukset*
- *milloin riittäisi viranomaisen lakiin perustuva itsearviointi, testaus ja valvonta, mahdollinen konsultatiivinen arviointi, mahdollinen valmistajanvakuutus tms.*

Vaatimustenmukaisuuden osoittaminen

- *yhteisiä tieto- ja viestintäteknisiä palveluja koskevia hyväksyntöjä olisi mahdollista hyödyntää laajemminkin*
- *arviointikohde on täsmennettävä siten, että viranomainen ei voi ulkoistaa tietojärjestelmiensä kelpoisuuden arviointia kokonaisuudessaan, koska sillä on merkittävä vaikutus julkisen vallan käyttöön tietojärjestelmän toiminnallisuuksia käytettäessä esimerkiksi hallintoasiaan liittyvässä päätöksenteossa*
- *vaatimustenmukaisuuden osoittaminen kuuluisi lähtökohtaisesti kussakin yleis- tai erityislaissa säädettäviin tietojärjestelmän käyttöä/käyttöönoton edellytyksiä koskeviin vaatimuksiin (kuten asiakastietolaissa)*

Tietoturvallisuutta ja tietojärjestelmiä koskevat vaatimukset (ja ns. arviointikriteeristöt)

- *arviointi haastavaa yksinomaan lain vaatimusten perusteella varsinkin, jollei ole toimivaltaisen viranomaisen yksityiskohtaisempia tulkintoja*
- *lakia alemman asteiseen sääntelyyn liittyy kysymys kuntien ym. itsehallinnosta/itsenäisestä asemasta*
- *ohjeet ja suositukset (kriteeristöt) eivät ole sitovia eikä niitä voida arviointien kautta muuttaa sitoviksi esim. erilaisia kelpoisuuksia määriteltäessä tai todistuksia annettaessa*
- *standardien suoraan (ja osin välilliseenkin) käyttöön liittyy ongelmia, jos ne on tarkoitettu sitovasti noudatettavaksi*
- *jatkuvuuden sekä APT-järjestelmien vaatimukset puuttuvat*
- *riskienhallinnan merkitys arvioinnissa/vaatimuksenmukaisuuden osoittamisessa*

Tietojärjestelmän vaatimustenmukaisuuden arviointiprosessi

- *tulisiko vaatimustenmukaisuuden arviointiprosessia tarkentaa lainsäädännössä*
- *tulisiko arvioinnin tilaajaa koskevaa sääntelyä täsmentää silloin kun arviointia suoritetaan useaa viranomaista/viranomaisen käyttämää tietojärjestelmää koskevien vaatimusten mukaisuuden arvioimiseksi*
  - *arviointien tilaamista koskevaa (arviointilain) sääntelyä tulisi selkeyttää mm. yhteishankintayksiköiden ja yhteisten palvelujen osalta.*
- *Haukka-raportissa nähtiin puutteena, että tilaaja ei saa arviointiviranomaiselta tai –laitokselta riittävän nopeasti riittävän tarkkaa arvioita arvioinnin kustannuksista tai kestosta*

Vastuukysymykset vaatimustenmukaisuuden osoittamisesta ja toisaalta tietojärjestelmän käytännön toiminnasta

- *viranomainen vastaa päätöksentekoon käytetyn tietojärjestelmän toiminnasta ja päätöstensä lainmukaisuudesta (virkavastuu)*
- *vastuusta arviointiprosessissa (vastuu puutteiden ilmoittamisesta sekä mahdollisesta arviointilaitoksen/arvioivan viranomaisen/arvioijan vastuusta ym.) voitaneen säätää arviointia koskevassa säädännössä*
- *mahdollisesti tarvitaan erityisiä säännöksiä vastuunjakautumisesta (esim. asiakastietolaki)*
  - *esim. osavastuun kohdentaminen lainsäädännössä myös tietojärjestelmän valmistajaan/tuottajaan*