VALTIOVARAINMINISTERIÖ

Esityö julkisen hallinnon digitaalisen turvallisuuden arviointikriteeristön luomiseksi

11.5.2021

Sisällys

1 TAUSTA JA TAVOITTEET

Valtioneuvosto teki 8.4.2020 periaatepäätöksen Julkisen hallinnon digitaalisesta turvallisuudesta (VM 2020:33). Periaatepäätöksen mukaisesti digitaalisen turvallisuuden viitekehykseen sisältyy riskienhallintaan, toiminnan jatkuvuudenhallintaan ja varautumiseen sekä kyberturvallisuuteen, tietoturvallisuuteen ja tietosuojaan liittyviä asioita. Periaatepäätöksessä on kuvattu julkisen hallinnon digitaalisen turvallisuuden kehittämisalueet ja kehittämisen periaatteet, sekä keskeisiä hallinnon toimintaa ja prosesseja tukevat digitaalisen turvallisuuden palvelut. Periaatepäätöksen linjauksia toteuttaa Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020-2023 (Haukka) (VM 2020:33).

Yhtenä Haukka-toimeenpanosuunnitelman tehtävänä on julkisen hallinnon palveluiden ja palvelutuotannon digitaalisen turvallisuuden arviointi. Tehtävä liittyy lain julkisen hallinnon tiedonhallinnasta (906/2019, tiedonhallintalaki) voimaantuloon. Tiedonhallintalakiin on kirjattu, että elinkaarimallin mukaisesti tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Olennaiset tietojenkäsittelyyn kohdistuvat riskit on selvitettävä ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. Kokonaisuuteen kuuluu riskien arviointi, tietoturvallisuustoimenpiteiden suunnittelu tunnistettujen riskien perusteella sekä tietoturvallisuustoimenpiteiden toteuttaminen (ks. HE 284/2018 vp, 13 §:n yksityiskohtaiset perustelut). Tiedonhallintalain 13 § 5 momentissa on informatiivinen viittaus viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annettuun lakiin (1046/2011, arviointilaki). Tämän mukaan viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista säädetään erikseen.

Digitaalisen turvallisuuden arvioinnin nykytilaa ja kehitysehdotuksia on käsitelty Haukka-hankkeessa tehdyssä selvityksessä. Selvityksen yhtenä osaa-alueena on ollut digitaalisen turvallisuuden arviointikriteeristöjen nykytila ja kehitysehdotukset. Arviointilain mukaan viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arviointiperusteina voidaan käyttää:

1. lailla tai asetuksella säädettyjä viranomaisten toimintaa koskevia tietoturvallisuusvaatimuksia ja valtiovarainministeriön tietoturvallisuutta koskevia ohjeita;
2. kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitetun kansallisen turvallisuusviranomaisen antamia kansainvälisten tietoturvallisuusvelvoitteiden toteuttamista koskevia ohjeita;
3. Euroopan unionin tai muun kansainvälisen toimielimen antamia tietoturvallisuutta koskevia säännöksiä ja ohjeita;
4. julkaistuja ja yleisesti tai alueellisesti sovellettuja tietototurvallisuutta koskevia säännök-siä, määräyksiä tai ohjeita;
5. vahvistettuun standardiin sisältyviä tietoturvallisuutta koskevia vaatimuksia.

Katakri-kriteeristö täsmentää kansainvälisistä tietoturvavelvoitteista annettua lakia (588/2004). Sitä käytetään myös turvallisuusluokiteltavia tietoja käsittelevien kansallisten tietojärjestelmien ja tietoliikenneratkaisujen arvioinneissa. Se ei sisällä julkisten tai salassa pidettävien tietojen eikä toiminnan jatkuvuudenhallinnan ja varautumisen arviointikriteerejä. VAHTI-ohjeet ovat pääosin valtionhallinnon käyttöön tarkoitettuja (mm. vanhentunut VAHTI 2/2010). Vanhentuneita VAHTI-ohjeita ja aiempia Katakri-versioita käytetään edelleen. Katakri-kriteeristön ja Vahti-ohjeiden soveltuvuus koko julkisen hallinnon käyttöön on rajallinen, koska kuntasektorilla turvallisuusluokittelua ei käytetä (1109/2019). Digitaalisen turvallisuuden vaatimusmäärittelyt eivät myöskään perustu laajasti

kansainvälisiin standardeihin (mm. ISO27001 – Tietoturvallisuuden hallinta, ISO22301 – Jatkuvuuden hallinta, ISO31000 – Riskienhallinta), joita olisi tarvittaessa täydennetty kansallisilla erityisvaatimuksilla.

Riskienarvioinnin käyttäminen palvelujen toteutuksen perusteena on sekä tiedonhallintalain että käytännössä kaikkien kansainvälisten hallintaviitekehysten edellyttämä menettely. Arviointiperustaa tulisi kehittää edelleen siten, että arvioinneissa huomioidaan entistä paremmin riskien arviointiin perustuva toiminta. Arviointikriteeristöt tulisi muotoilla siten, että ne mukautuvat joustavasti digitaalisen toimintaympäristön nopean kehittymisen myötä. Kriteeristöjen tulisi pohjautua kansainvälisiin standardeihin ja muihin yleisesti käytettyihin vaatimusluetteloihin, joita on täydennetty kansallisilla erityisvaatimuksilla. Niiden toteutumista arvioitaessa on huomioitava palvelun käyttötarkoitus, palvelun käytön riskit, palvelussa käsiteltävien tietojen suojaaminen ja palvelun saatavuustarpeet. Hallintakeinojen toteutuksessa käytettyjen ratkaisujen tulee perustua tiedonhallintayksikön (tai vastaavan) ajantasaiseen riskiarvioon, jonka tiedonhallintayksikkö on hyväksynyt. Palvelun arvioinnissa tulee huomioida myös tiedonhallintayksikön ja ulkopuolisen riippumattoman riskienarvioinnin eroavat roolit ja perusteet. Tiedonhallintayksikön riskienarvioinnissa korostuu viranomaisen toiminnan erityispiirteiden huomiointi. Ulkopuolisen riippumattoman arvioinnin roolina on puolestaan arvioida kuinka suojautua tiedonkäsittelyyn kohdistuvia yleisiä riskejä vastaan. Kuten nykytilassa, ulkopuolisen arvioijan näkemyksen riskeistä tulisi pohjautua ajantasaiseen tilannekuvaan.

Julkisen hallinnon digitaalisten palvelujen turvallisuuden arvioinnissa käytettävässä arviointikriteeristössä tulee määritellä eri digitaalisen turvallisuuden osa-alueiden vähimmäiskriteerit, joiden avulla kaikkia palveluja arvioidaan. Sen lisäksi arviointikriteeristössä pitäisi osoittaa, missä tilanteissa, mihin riskeihin vastaten, millä perusteilla ja millä digitaalisen turvallisuuden osa-alueilla tarvitaan vähimmäistason ylittäviä kriteerejä, sekä kuvata, mitä nämä tilanteet, riskit, perusteet ja kriteerit ovat. Arviointikriteeristön tulee soveltua mm. palvelujen kehittämisen aikana tehtäviin arviointeihin, hankintavaiheessa palvelulle asetettujen vaatimusten todentamiseen sekä käytön aikaisiin arviointeihin. Oppivien ja itsenäisesti kehittyvien järjestelmien laajenevan käytön myötä tarvitaan myös näitä järjestelmiä koskevia arviointikriteerejä.

Haukka-hankkeessa on tehty esivalmistelua tässä kuvatun arviointikriteeristön luomiseksi. Kriteeristön jatkotyöstö tehdään tiedonhallintalautakunnan tätä tarkoitusta varten perustetussa jaostossa.

2 KRITEERISTÖ

Julkisen hallinnon digitaalisen turvallisuuden arviointikriteeristö sisältäisi määritelmiä, käyttötapauskuvauksia sekä viittaukset säädöspohjaan ja ohjeistuksiin. Tarkoituksena on myös luoda työkalu, joka ohjaa oikeiden digitaalisen turvallisuuden vaatimusten ja niiden arvioinnin kriteerien tunnistamiseen.

2.1 Määritelmät

Kriteeristössä käytettävien käsitteiden määrittelyjen tavoitteena on määritellä käsitteet sekä käyttäjien (tiedonhallintayksiköt, hankinta-asiantuntijat) että palvelun toimittajien näkökulmasta selkeästi ja täsmällisesti jättäen niihin riittävää palvelun toteuttamiseen liittyvää liikkumavaraa.

Termi	Määritelmä	Lähde
akkreditointi (1)	Pätevyyden toteaminen ja osoittaminen. Säädelty EU-alueella lainsäädännöllä (EU 765/2008)	FINAS
akkreditointi (2)	Virallista valtuuttamista hakevan toimielimen pätevyyden toteaminen	https://termipankki.fi/tepa/fi/haku/akkreditointi
akkreditointi (3)	Kolmannen osapuolen toteuttama vahvistaminen, joka liittyy vaatimustenmukaisuuden arviointielimeen ja jolla osoitetaan muodollisesti sen pätevyys ja puolueettomuus sekä jatkuva kyky suorittaa määriteltyjä vaatimustenmukaisuuden arviointitehtäviä.	ISO/IEC 17000:2020 (7.7)
vaatimustenmukaisuuden arviointikohde	Kokonaisuus, johon määriteltyjä vaatimuksia sovelletaan	ISO/IEC 17000:2020 (4.2)
arviointi	Tarkastelun kohdetta koskevan tiedon analysointi ja tulkitseminen ja niiden pohjalta tehtävä kohteen arvottaminen. (vrt. auditointi). Itsearviointi ja ulkoinen arviointi	https://termipankki.fi/tepa/fi/haku/arviointi
auditointi	Systemaattinen tarkastus, jossa tarkastettavasta riippumattomat tarkastajat selvittävät, miten tarkastettavan toiminta ja toiminnan tulokset vastaavat niille asetettuja tavoitteita ja edellytyksiä. (1., 2., 3. osapuolen auditointi)	https://termipankki.fi/tepa/fi/ryhm%C3%A4/3/haku/audit
hallintakeino	riskiä muuttava toimenpide (esim. riskiä muuttava prosessi, politiikka, laite, käytäntö tai muu toimenpide)	ISO/IEC 27000:2020 (3.14)
hallintatavoite	toteamus, jossa kerrotaan, mitä hallintakeinojen toteuttamisella on tarkoitus saavuttaa	ISO/IEC 27000:2020 (3.15)
hyväksyntä (1)	lupa, jolla sallitaan tuotteen, palvelun tai prosessin markkinointi tai käyttö	ISO/IEC 17000:2020 (9.1)

	määriteltyihin tarkoituksiin tai määritellyissä olosuhteissa	
hyväksyntä (2)	sekä yleis- että oma hyväksyntä	-
kontrolli	ks. hallintakeino	-
kontrollitavoite	ks. hallintatavoite	-
kriteeri (1)	arviointiperuste	https://termipankki.fi/tepa/en/search/kriteeri
kriteeri (2)	Kohteen arvioimiseen tai mittaamiseen käytettävä vertailuperuste. Soveltuvat kriteerit mahdollistavat kohteen kohtuullisen johdonmukaisen arvioimisen tai mittaamisen ammatillista harkintaa käyttäen.	Tilintarkastuksen ja säännönmukaisuuden tarkastuksen käsikirja (Euroopan tilintarkastustuomioistuin)
muutoksenhallinta	Prosessi, joka kontrolloi kaikkien muutosten elinkaarta mahdollistaen, että hyödylliset muutokset toteutetaan häiritsemällä mahdollisimman vähän IT-palveluja.	ITIL
palvelu	Organisoidun toiminnan tuloksena syntyvä aineeton hyödyke tarpeiden tyydyttämiseksi (*tulee vielä tarkentaa tähän kontekstiin, voidaanko käyttää muuhun kuin palveluihin? Tarkoitetaanko vain sovelluskerrosta, kattaako alustan, voiko palvelu olla TLIII tietojenkäsittely-ympäristö)*	https://termipankki.fi/tepa/fi/haku/palvelu
pilvipalvelu	eri pilvipalvelumallit, kansallinen ja globaali jaottelu sekä niiden eri hankintamallien tuomat erot	-
protection profile		-
pätevyys	kyky soveltaa tietoja ja taitoja halutun tuloksen saavuttamiseksi	ISO/IEC 17021-1:2015
security target		-
sertifiointi (1)	kolmannen osapuolen toteuttama vahvistaminen, joka koskee vaatimustenmukaisuuden arviointikohdetta, ellei kyseessä ole akkreditointi	ISO/IEC 17000:2020 (7.6)
sertifiointi (2)	Vaatimustenmukaisuuden arviointi	FINAS
SOA (statement of applicability)	ks. soveltamisala	-
soveltamisala		-

todistus		ISO/IEC TS 17027
tiedonhallintayksikkö	viranomainen, jonka tehtävänä on järjestää tiedonhallinta tiedonhallintalain vaatimusten mukaisesti	Laki julkisen hallinnan tiedonhallinnasta (906/2019) 2.1 § 2 k
tietojenkäsittely-ympäristö		-
tietojärjestelmä	tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuvaa kokonaisjärjestelyä	Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011) 2.1 § 1 k
tietoliikennejärjestely	tiedonsiirtoverkosta, tiedonsiirtolaitteista, ohjelmistoista ja muista tietojenkäsittelystä koostuvista järjestelyistä muodostuvaa järjestelmää	Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011) 2.1 § 2 k
(määritelty) vaatimus	Ilmaistu tarve tai odotus. Määriteltyjä vaatimuksia voidaan esittää velvoittavissa asiakirjoissa, kuten määräyksissä, standardeissa ja teknisissä spesifikaatioissa. Määritelty vaatimus voi olla yleinen (esim. säädöksen vaatimus) tai yksityiskohtainen (esim. tietojärjestelmävaatimus)	ISO/IEC 17000:2020 (5.1)
vaatimustenmukaisuuden arviointi	sen osoittaminen, että määritellyt vaatimukset täyttyvät	ISO/IEC 17000:2020 (4.1)
varmennelausunto		-

Keskeisiä sanastoja

- SFS-EN ISO/IEC 17000:2020. Vaatimustenmukaisuuden arviointi. Sanasto ja yleiset periaatteet
- SFS-EN ISO/IEC 27000:2020. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto
- SFS-EN ISO/IEC 17021-1:2015. Vaatimustenmukaisuuden arviointi. Vaatimukset johtamisjärjestelmiä auditoiville ja sertifioiville elimille. Osa 1: Vaatimukset"

2.2 Käyttötapauskuvaukset

Julkisen hallinnon digitaalisen turvallisuuden arvioinnin tukityökalua voidaan hyödyntää esimerkiksi seuraavissa käyttötapauksissa digitaalisen palvelun turvallisuusvaatimusten tunnistamiseen, varmentamiseen ja todentamiseen. Kaikissa käyttötapauksissa on kuvattava selkeästi kuka palvelua käyttää, miten käyttää, missä käyttää ja mikä on tavoite.

Palvelun suunnittelu ja vaatimusmäärittely: Julkisen hallinnon viranomainen käyttää työkalua palvelun suunnittelu- ja vaatimusmäärittelyvaiheessa ennen hankintaa tavoitteenaan tunnistaa palvelulle asetettavat digitaalisen turvallisuuden vaatimukset.

Palvelun arviointi: Julkisen hallinnon viranomainen käyttää työkalua tavoitteenaan tunnistaa hankintatilanteessa palvelulle digitaalisen turvallisuuden minimivaatimukset kilpailutuksessa tai osana palvelusopimusta.

Toimittajan arviointi: Julkisen hallinnon viranomainen käyttää työkalua tavoitteenaan tunnistaa hankintatilanteessa digitaalisen turvallisuuden minimivaatimukset toimittajalle kilpailutuksessa tai osana palvelusopimusta sekä varmistaa toimittajan vaatimusten toteutuminen.

Digitaalisen turvallisuuden arviointi: Julkisen hallinnon viranomainen käyttää työkalua tavoitteenaan arvioida digitaalisen turvallisuuden palvelun toimituksen lopputuotteen vaatimustenmukaisuus suhteessa hankinnan ja palvelusopimuksen minimivaatimuksiin. Arviointi voi olla joko toimijan itsearviointi tai kolmannen osapuolen tekemä ulkoinen arviointi, joka voidaan mahdollisesti varmennuslausunnon tyyppisesti perustaa olemassa oleviin kriteeristöihin, sertifikaatteihin ja varmennuslausuntoihin.

Mahdollisia muita käyttötapauksia

Tietosuojaa koskeva arviointi: Onko tietosuoja erillinen käyttötapaus vai onko se osa kriteeristöä? Osoitusvelvollisuuden riittävän tason täyttäminen

Muun EU-sääntelyn noudattaminen (NIS-direktiivi jne.)

Toimijoiden arviointi (tiedonhallintayksikkö, tiedon käsittelijät jne.)

2.3 Säädöspohja

Julkisen hallinnon digitaalisen turvallisuuden arvioinnin tukityökalu perustuu seuraaviin säädöksiin, joiden perusteella tunnistetaan palvelun kontrollitavoitteet. Palveluun liittyvästä erityslainsäädännöstä tulevat vaatimukset tulee huomioida minimivaatimusluettelon lisäksi. Lainsäädännössä asetettujen vaatimusten lisäksi työkalussa tulee huomioida myös muut digitaalisen turvallisuuden osa-alueet, kuten tiedon eheyden ja saatavuuden turvaaminen.

Säädökset:

Työkalun säädöspohja koostuu laista julkisen hallinnon tiedonhallinnasta (906/2019) ja siihen liittyen arkistolaista (831/1994). Tiedonhallintalakia täydentää asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019). Julkisen hallinnon viranomaisen asiakirjojen julkisuutta ja tiedonkäsittelyä määrittää yleisesti laki viranomaisten asiakirjojen julkisuudesta (621/1999).

Muita julkisen hallinnon viranomaisten tietoturvallisuutta sääntteleviä lakeja ovat laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004), turvallisuusselvityslaki (726/2014) sekä laki digitaalisten palvelujen tarjoamisesta (306/2019). Tietyillä osa-alueilla julkisen hallinnon digitaalista turvallisuutta säännellään laissa julkisen hallinnon turvallisuusverkkotoiminnasta (10/2015) sekä laissa sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019).

EU:n verkko- ja tietoturvallisuusdirektiivissä (NIS-direktiivi) säännellään tietoturvavelvollisuuksista ja häiriöraportoinnista. Tietosuojan näkökulmasta säädöspohja koostuu yleisestä tietosuoja-asetuksesta ja rikosasioiden tietosuojadirektiivistä. Näitä kansallisesti tarkentavat ja täydentävät tietosuojalaki (1050/2018), rikosasioiden tietosuojalaki (1054/2018) ja henkilötietojen suojaa koskeva erityislainsäädäntö.

Ohjeistukset:

Tiedonhallintalautakunta on laatinut tiedonhallintalain vaatimuksien toteuttamista edistäviä suosituksia, jotka on otettu huomioon työkalussa. Tietosuojan osalta vaatimusten toteuttamisen ohjeistamisesta ja suosituksista vastaavat Euroopan tietosuojaneuvosto (EDPB) ja kansallisesti Tietosuojavaltuutetun toimisto.

Näiden lisäksi työkalussa tulee ottaa huomioon sidosryhmien asettamat vaatimukset, kuten Digi- ja väestötietoviraston tietoluvan hakemismenettely ja PCI DSS -standardin vaatimukset.