VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Selvitys organisaation tietoturvatehtävistä ja niiden organisoimisesta

9.3.2022

Sisällys

1 JOHDANTO

Digitaalisen turvallisuuden kunta-valtio-yhteistoimintamallin esiselvityksessä (11.6.2021) kartoitettiin odotuksia ja kehityskohteita digitaalisen turvallisuuden kunta-valtio-yhteistoiminnalle ja sen hallinnalle. Selvityksessä kuvataan tehtäviä yhteistoiminnan kehittämiseksi ja yhtenä tällaisena tehtävänä on Haukka-hankkeessa laadittava selvitys kuntien ja hyvinvointialueiden tietoturvavastaavan roolista ja vastuista. Yhteistoiminta- ja hallintamallin kehittämistä varten Haukka-hankkeessa haastateltiin 25 organisaatioita ja haastatteluiden osana kartoitettiin näkemyksiä tietoturvallisuuden vastuuhenkilön roolista tehtäväkuvauksen alustavan luonnoksen pohjalta.

Yleinen tietosuoja-asetus (EU 2016/67) edellyttää rekisterinpitäjää nimittämään tietosuojavastaavan (data protection officer), jonka asema ja tehtävät on kuvattu asetuksessa. Tietosuojavastaavan rooli on huolehtia rekisteröityjen oikeuksien toteutumista, kun taas tietoturvavastaavan tehtävinä ovat tyypillisesti organisaation oman tietoturvallisuus, sen kehittäminen ja seuranta.

Tietoturvallisuussäännösten, lähinnä lain julkisen hallinnon tiedonhallinnasta (906/2019, jatkossa tiedonhallintalaki) velvoitteista voidaan kuitenkin muodostaa tiedonhallintayksikön velvoitteiden ja tehtävien yleiset kuvaukset sekä mahdollisia tietoturvatehtäviä jaettavaksi eri rooleille. Tässä selvityksessä tehtävien kuvauksen ensisijaisena tarkoituksena onkin määrittää sellaiset tietoturvallisuuden kehittämiseen ja ylläpitoon liittyvät tehtävät, joita tiedonhallintayksikössä on toteutettava tiedonhallintalain vaatimusten toteuttamiseksi. Organisaation tai tiedonhallintayksikön tietoturvavastuiden sisäisestä tietoturvavastuiden jakautumisesta esimerkiksi nimetylle vastaavalle johtajalle, nimetylle tietoturvapäällikölle tai -asiantuntijalle ei ole velvoittavaa lainsäädäntöä, mutta tämän suosituksen avulla voidaan organisaatioissa arvioida suositeltujen roolien ja tehtävien jakautumista oma toiminta ja yleisempi vastuunjako huomioiden.

Tällä hetkellä saatavilla ei ole laajasti yhteisesti hyväksyttyä tietoturvavastaavan rooli- tai tehtäväkuvausta ja usein nämä toimivat oman toimensa ohella nimettynä tietoturvallisuuden yhteyshenkilönä. Tiedonhallintalain tarkoittamien tiedonhallintayksiköiden tietoturvapolitiikat (tai vastaavat), joissa tietoturvavastaavan rooli on usein kuvattu, sisältävät usein keskenään samankaltaisia tehtävänkuvauksia[1, 2]. Varsinkin suuremmilla organisaatioilla voi olla erillinen tietoturvajohtaja tai -päällikkö (Chief Information Security Officer, CISO), jonka tehtävät ja vastuut ovat samankaltaisia[3, 4].Vaikka tässä selvityksessä on roolikuvauksen työnimenä käytetty tietosuojavastaavasta johdettua tietoturvavastaa, on näiden kahden roolin välillä kuitenkin eroja: tietosuojavastaan lakisääteisenä tehtävänä on valvoa rekisteröityjen oikeuksien toteutumista, kun taas tietoturvallisuuden tehtävien toteuttamisen kautta kehitetään ja parannetaan tiedonhallintayksikön omaa tietoturvallisuutta.

[1] https://www.parkano.fi/wp-content/uploads/2019/08/Parkanon-kaupungin-tietoturvapolitiikka-hyv%c3%a4ksytty-KH-18.12.2017-%c2%a7-302.pdf
[2] https://www.jikky.fi/files/6461/Tietoturva-_ja_tietosuojapolitiikka_2019.pdf
[3] https://www.protectivesecurity.govt.nz/governance/protective-security-roles-and-responsibilities/roles-and-responsibilities-for-information-security/the-ciso-leads-and-oversees-information-security/
[4] https://www.informationssakerhet.se/metodstodet/utforma/#ciso-rollen

Yhtenäinen tietoturvallisuustehtävien kuvaus tukee tiedonhallintalain vaatimusten toteutumista tiedonhallintayksiköissä ja siten edistää digitaalisen turvallisuuden kehittymistä. Noudattamalla tiedonhallintalain vaatimuksia ja annettuja suosituksia tiedonhallintayksiköt voivat määritellä tietoturvavastuiden toteuttamisen itselleen soveltuvalla tavalla ja varmistua siitä, että roolikuvaus on tiedonhallintalain vaatimusten mukainen ja että tietoturvallisuuden kehittämisen, toteutuksen, valvonnan ja raportoinnin vastuut on määritelty riittävän tarkasti. Lisäksi kuvauksen avulla tiedonhallintayksikön on mahdollista määrittää tehtävät ja niiden jakautuminen tiedonhallintayksikössä ja toisaalta ne osuudet tehtävistä, jotka voidaan hankkia ostopalveluna ulkopuoliselta toimijalta.

2 TIETOTURVALLISUUSTEHTÄVIEN VASTUISTA

Tietoturvallisuustehtävien kuvauksen muodostamisessa on sovellettu tietosuojavastaavan nimittämiseen, asemaan ja tehtäviin liittyviä kuvauksia[5] sekä julkisesti saatavilla olevia tietoturvapolitiikkoja, joissa tietoturvallisuuden kehittämisen ja ylläpidon vastuita ja tehtäviä on kuvattu.

2.1 Tietoturvallisuustehtävien organisoinnista

Tiedonhallintalain tiedonhallintayksiköille asettamien velvoitteiden toimeenpanemiseksi tiedonhallintayksikkö voi hyvien alan käytänteiden mukaisesti organisoida tietoturvallisuuteen liittyviä tehtäviä yhdelle tai useammalle henkilölle. Erilaisten yhteistoiminnan muotojen tueksi tiedonhallintayksikön tulisi julkistaa sellaiset yhteystiedot, joiden kautta yhteistyötä voidaan koordinoida muiden tiedonhallintayksiköiden, viranomaisten ja yksityissektorin toimijoiden kanssa. Tiedonhallintayksikön tulisi huolehtia tietoturvatyön kokonaisuudesta johdon osoittamien resurssien ja toimintavaltuuksien puitteissa.

Tietoturvallisuustehtävien hoitaminen voidaan antaa tehtäväksi joko tiedonhallintayksikön henkilöstöön kuuluvalle yksittäiselle henkilölle (esimerkiksi tietoturva- tai IT-päällikölle), tai tehtävät voidaan hajauttaa osaksi useamman henkilön tehtäviä; uusien virkojen perustaminen ei ole välttämätöntä. Lisäksi ainakin osa tehtävistä on mahdollista osoittaa palvelusopimuksen perusteella tehtäviä hoitavalle henkilölle. Tärkeintä on, että kaikki oleelliset tietoturvallisuustehtävät toteutetaan, niiden toteuttamisen vastuut on selkeästi kuvattu ja tehtävien toteutumisen seuranta on määritelty. Tietoturvallisuustehtävien hoitaminen edellyttää kuitenkin ymmärrystä tiedonhallintayksikön toiminnasta ja toimintaympäristöstä sekä tehtävien edellytyksiin nähden riittävää hallinnollisen ja teknisen tietoturvan osaamista.

Tietoturvallisuustehtäviä voidaan osoittaa tiedonhallintayksikön toimihenkilölle tai virkamiehelle. Jos tehtäviä osoitetaan viranhaltijalle, on varmistettava, ettei tehtävän kuvaus ole valtion virkamieslain (750/1994), kunnan tai hyvinvointialueen viranhaltijoista annetun lain (304/2003) ja kuntalain (410/2015) kannalta ristiriitainen. Jos tietoturvatehtävistä säädettäisiin lailla tai muulla velvoittavalla määräyksellä, tulisi määrittää, mitkä tehtävät tiedonhallintayksikön on hoidettava itse ja mitkä sen on mahdollista hankkia ostopalveluna.

Vastuuhenkilölle annetut tietoturvallisuustehtävä eivät saa aiheuttaa eturistiriitoja henkilön muiden mahdollisten tehtävien kanssa. Sama henkilö voi hoitaa tietoturvatehtäviä useammassa tiedonhallintayksikössä, mutta tällöin tulee huolehtia siitä, että henkilöllä on tosiasialliset mahdollisuudet hoitaa tehtävää eli siten, että työaikaa, välineitä ja osaamista koskevat edellytykset täyttyvät jokaisessa näistä tiedonhallintayksiköistä.

Tietoturvavastaavan tehtävää voi hoitaa myös ulkoa hankittuna palveluna, jota voi tuottaa joko toinen tiedonhallintayksikkö tai yksityisen sektorin palveluntarjoaja. Ulkoista tietoturvavastaavaa käytettäessä tiedonhallintayksikön on varmistettava, että vastuut, velvoitteet ja palvelutasot kirjataan selkeästi

[5] https://www.kuntaliitto.fi/yleiskirjeet/2018/tietosuojavastaavan-nimittaminen-tehtavat-ja-asema

sopimuksiin. Tietoturvavastaavan tehtävää ulkoistettaessa on kuitenkin huomioitava, että vastuu tiedonhallintalain vaatimusten sekä muiden tietoturvavaatimusten toteutumisesta on aina tiedonhallintayksiköllä, eikä vastuuta voi ulkoistaa.

2.2 Vastuuhenkilöiden toimintaedellytyksistä ja osaamisvaatimuksista

Tietoturvallisuustehtävistä vastuussa olevien henkilöiden toimintaedellytyksiin vaikuttavat edellisessä kappaleessa kuvatun vastuiden organisoinnin lisäksi käytettävissä olevat resurssit sekä tehtävää hoitavan henkilön osaaminen. Täsmällisten osaamisvaatimusten asettamiseen vaikuttavat tiedonhallintayksikön koko, tehtävä ja toimiala, toimintaympäristön kompleksisuus sekä ulkoistettujen ja itse tuotettujen digitaalisten palvelujen laatu ja määrä. Kun tietoturvallisuustehtäviä annetaan jonkun tehtäväksi, tulisi ottaa huomioon henkilön ammattipätevyys ja erityisesti asiantuntemus tietoturvallisuutta koskevasta lainsäädännöstä ja alan käytänteistä. Ammatillista pätevyyttä tulisi arvioida kokonaisuutena hakijan työkokemuksen ja aiempien tehtävien perusteella, koulutustaustan avulla, esimerkiksi kyber- tai tietoturvallisuuden koulutusohjelmat, sekä erilaisten kurssien suorittamisen ja henkilökohtaisten sertifiointien perusteella, kuten CISSP, CISM, Comp TIA Security+. Tietoturvallisuustehtävien hoitamisessa edellytetään kykyä soveltaa tietoturvaosaamista tiedonhallintayksikön toimialalle, jolloin myös sosiaalisten taitojen ja toimialaosaamisen merkitys korostuu.

Jotta tietoturvallisuustehtävien lisääminen yhden tai useamman henkilön tehtäväkuvauksiin ei jäisi vain pelkäksi kirjaukseksi, on vastuullisilla oltava riittävästi työaikaa, -välineitä ja osaamista tehtävän suorittamiseen. Tärkeä osa tehtävän hoitamista on vaadittavan ammatillisen osaamisen kehittäminen, jota voi toteuttaa esimerkiksi osallistumalla koulutuksiin, seminaareihin tai yhteistyöryhmiin. Tietosuojavastaavan asemasta on säädetty, ettei tietosuojavastaava ole henkilökohtaisesti vastuussa tietosuojaa koskevan lainsäädännön rikkomisesta ja siksi suositellaan, ettei tietoturvallisuudesta vastaavien henkilöiden tulisi olla henkilökohtaisesti vastuussa tietoturvallisuutta koskevan lainsäädännön rikkomisesta.

3 TIETOTURVALLISUUSTEHTÄVISTÄ

Tietoturvallisuustehtäviä hoitavat vastuuhenkilöt ovat tiedonhallintayksikön sisäisiä asiantuntijoita, joiden tehtäviin tulisi kuulua tietoturvallisuuden koordinointi, kartoittaminen, toteuttamisen valvonta sekä tietoturvallisuustietouden edistäminen. Tiedonhallintayksikön tulisi määrittää tietoturvallisuustehtävät kirjallisiin tehtäväkuvauksiin. Kuvauksia voidaan hyödyntää rekrytoinnissa ja ne tulisi liittää työsopimukseen tai viran kuvaukseen. Lisäksi tiedonhallintayksikkö voi kuvauksen perusteella laatia rajauksia tietoturvallisuuden ulkoistukselle. Tässä ohjeessa määriteltyjen tehtävien lisäksi tiedonhallintayksikkö voi asettaa muita tietoturvallisuustehtäviä, kunhan ne eivät ole ristiriidassa tässä esitettyjen suositusten kanssa.

Tiedonhallintayksikön tietoturvallisuuden onnistumisen kannalta on tärkeää, että tietoturvallisuutta käsiteltäisiin ainakin ICT-hankinnoissa, järjestelmäprojekteissa sekä tarkastuksissa ja arvioinneissa. Vastuuhenkilön tulisi olla mukana aina, kun tehdään tietoturvallisuuteen vaikuttavia päätöksiä ja hänellä tulisi olla käytettävissään kaikki olennaiset tiedot asianmukaisten neuvojen antamiseksi.

Tietoturvallisuustehtävistä vastaavilla tulisi olla mahdollisuus raportoida tietoturvallisuuteen liittyvistä asioista suoraan johdolle ja tietoturvallisuuden asiantuntijoita olisikin hyvä kutsua säännöllisesti ylemmän ja keskitason johdon kokouksiin ja näiden tietoturvallisuutta koskeville näkemyksille tulisi antaa asianmukainen painoarvo. Mahdollisissa erimielisyystilanteissa on suositeltavaa dokumentoida perusteet, joiden vuoksi asiantuntijan neuvoa, ohjeita tai näkemyksiä ei noudateta.

Koska erilaisia tietoturvauhkia tai kyberhyökkäyksiä ei voida täysin eliminoida, tulisi tiedonhallintayksikön pystyä reagoimaan tietoturvaloukkauksiin tai muihin tietoturvaongelmiin mahdollisimman nopeasti ja tehokkaasti. Tästä syystä tiedonhallintayksikössä tulisi olla menettelytavat, joiden mukaan kaikista havaituista tietoturvallisuuden puutteista, tietoturvallisuutteen liittyvästä väärinkäytöksistä tai epäillyistä tietoturvarikkomuksista raportoidaan välittömästi tiedonhallintayksikön määrittämällä tavalla. Kun tietoturvaloukkaus tai muu tietoturvaongelma on havaittu, tulisi tietoturvallisuuden asiantuntijoita kuulla mahdollisimman nopeasti ongelman rajaamiseksi ja asianmukaisten korjaavien toimenpiteiden aloittamiseksi.

Liitteenä 2 olevassa taulukossa on lueteltu tietoturvallisuustehtäviä sekä niihin liittyviä säädösperusteita. Tehtävät on pyritty liittämään tiedonhallintalain vaatimuksiin, mutta kaikkia kuvattuja tehtäviä ei voi yksiselitteisesti velvoittaa tiedonhallintalain perusteella. Jos tietoturvallisuustehtävistä halutaan tehdä velvoittavia, tulisi lainsäädäntöä kehittää tukemaan tätä tavoitetta.

4 HUOMIOITA

Tietoturvallisuuden vastuiden selkeyttäminen tiedonhallintalain vaatimusten toteuttamiseksi koetaan tärkeäksi, mutta nimikettä ”tietoturvavastaava” ei pidetä onnistuneena. Nimikkeen tulisi paremmin kuvata vastuuta tietoturvallisuuden kehittämisestä ja koordinoinnista. Useissa organisaatioissa käytössä oleva ”tietoturva-asiantuntija” ei välttämättä anna kuvaa riittävän vahvasta toimijasta, kun taas ”tietoturvapäällikkö” herätti ajatuksen uuden viran välttämättömyydestä, mitä pidettiin epärealistisena ajatuksena. Tärkeänä pidettiin, että tiedonhallintayksiköissä on käytettävissä riittävästi tietoturvaosaamista, ja yhden tietoturvavastaavan katsottiin muodostavan avainhenkilöriskin. Digitaalisen turvallisuuden eri osa-alueiden hallinta edellyttää laajaa osaamista, eikä tehtävien osoittaminen yhdelle henkilölle ole välttämättä mahdollista tai tarkoituksenmukaista. Esimerkiksi sovelluskehitys, johtaminen, tietoaineistojen käsittely ja hankinnat edellyttävät tiedonhallintayksikön yhteistä digiturvallisuudesta huolehtimista.

Tietosuojavastaavan tehtävien velvoittavuuden nähtiin parantaneen tietosuojaa organisaatioissa. Tästä näkökulmasta tietoturvavastaavan roolin säätämistä velvoittavaksi kannatettiin ja nähtiin velvoittavuuden helpottavan tietoturvallisuuden vähimmäistason saavuttamista. Toisaalta haastatteluissa todettiin, että velvoittavuuden sijaan tarvittaisiin yhtenäisiä käytäntöjä esimerkiksi riskienhallintaan. Lisäksi todettiin, ettei tietosuojavastaavankaan tehtävää pystytä kaikissa organisaatioissa hoitamaan velvoitteiden edellyttämällä tavalla. Erityisesti pienissä kunnissa on vaikea osoittaa tehtävää henkilölle, jolla olisi kuvauksessa edelletyllä tavalla riittävästi resursseja ja osaamista tehtävän hoitamiseksi. Käytännössä tietosuojavastaaville on annettu tehtäväksi myös vastuu tietoturvallisuuden kokonaisuudesta, mikä on ristiriidassa tietosuojavastaavan tehtävän riippumattomuuden kanssa. Suurissa kaupungeissa, hyvinvointialueilla ja muissa isoissa organisaatioissa voi olla helpompi määritellä tietoruvallisuuden kokonaisuudesta vastaava rooli ja löytää siihen tekijä. Ostopalvelun käyttö kuvauksen mukaisten tietoturvallisuustehtävien hoitamisessa nähtiin tärkeänä apuvälineenä.

Ulkoistuksissa haasteeksi tunnistettiin esimerkiksi tiedonhallintayksikön toiminnan ja toimintaympäristön tuntemuksen puutteet, vastuiden määrittely. Kuvauksessa esitettyjä tehtäviä pidettiin enimmäkseen hyvinä, mutta samalla korostettiin, että roolin ja tehtävän kuvauksessa tulisi keskittyä hallintamallin ja tietoturvallisuuden määrittelyyn yksittäisten, operatiivisten tehtävien sijaan. Yleisesti todettiin, että tietoturvavastuita ulkoistetaan paljon, mutta tiedonhallintayksiköillä ei ole yhtenäistä käsitystä siitä, mitkä tehtävät tulisi pystyä hoitamaan itse ja mitkä voidaan hankkia ostopalveluina.

Tietoturvallisuustehtävien hoitamiselle tulisi määritellä selkeä mandaatti tehtävien hoitamiseksi. Tietoturvavastaavalle tulisi määritellä vastaava selkeä ja riittävän vahva mandaatti, jotta tietoturvallisuutta voi käytännössä edistää. Erityisesti kaivattiin selkeää vastuunjakoa johdon ja tietoturvallisuudesta vastaavien henkilöiden välille. Tietoturvallisuuden ja tietosuojan toteuttamisella on erilaiset tavoitteet, mutta tehtävät edellyttävät kuitenkin läheistä yhteistyötä .

LIITE 1: TIETOTURVALLISUUSTEHTÄVIIN JA NIIDEN ORGANISOINTIIN LIITTYVIÄ SÄÄDÖKSIÄ

- Laki julkisen hallinnon tiedonhallinnasta (906/2019)
- Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019)
- Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011)
- Valtion virkamieslaki (750/1994)
- Valtion virkaehtosopimuslaki (664/1970)
- Laki kunnan ja hyvinvointialueen viranhaltijasta (304/2003)
- Laki kunnan ja hyvinvointialueen virkaehtosopimuksista (669/1970)
- Kuntalaki (410/2015)
- Työehtosopimuslaki (436/1946)

LIITE 2: EHDOTUS TIETOTURVATEHTÄVISTÄ

Tehtävä	Säädökset
Yleiset tehtävät	
tiedonhallintayksikön ja sen toimintaympäristön tietoturvallisuuden tilan seuranta	906/2019 4.2 § 5 k, 13.1 §
tiedonhallintayksikön tietoturvasäännösten noudattamisen seuranta ja havaitsemiensa puutteiden raportointi	906/2019 4.2 § 5 k 1101/2019 1406/2011 3 §, 6 §, 8 a §
tiedonhallinnan muutosten arvioinnin tekemiseen liittyvien neuvojen antaminen pyydettäessä	906/2019 5 §, 8 §
viranomaisten yhteyshenkilönä toimiminen tietoturvallisuuteen liittyvissä asioissa	906/2019 7 §
tietoturvallisuutta koskevien tietojen ja neuvojen antaminen johdolle ja henkilöstölle	906/2019 4.2 § 2 k, 13.1 §
Vastuut	
tietoturvallisuustoimenpiteiden mitoittaminen tiedonhallintayksikön tietoturvalinjausten mukaisesti	906/2019 13.1 §, 13.3 §
tietoturvallisuuden arviointi ja ulkoisten arviointien koordinointi	906/2019 13.5 §
tietoturvallisuusdokumenttien laatiminen ja päivittäminen	906/2019 4.2 § 2 k, 18 §, 28 §
tietoturvatietouden edistäminen ja tietoturvallisten toimintatapojen noudattaminen tiedonhallintayksikössä ja sen ostamissa palveluissa	906/2019 4.2 § 3 k, 13.1 §, 13.4 §
tietoturvallisuuden yleisen tilanteen seuraaminen	906/2019 4.2 § 5 k, 13.1 §
laitteisto- ja ohjelmistoturvallisuuden periaatteiden määrittäminen	906/2019 13.1-4 §, 14 §, 15 §
hankintojen tietoturvallisuusvaatimusten määrittely niiden noudattamisen seuranta	906/2019 13.4 §
tietoturvallisuuden mittaamisen määrittäminen ja tulosten raportointi	906/2019 5.3 §, 8 §
tietoturvallisuuden kehittämissuunnitelmien tekeminen	906/2019 4.2 §, 13.3 §, 15-18 §§
tietoturvallisuuden toimeenpanon koordinointi	906/2019 4.2 § 1-2 k, 13 §
merkittävien tietoturvapoikkeamien käsittely johdon kanssa käyttäen tarvittaessa ulkopuolista asiantuntemusta	906/2019 4.2 § 5 k, 13.1 §
Tukitehtävät	
tiedonhallintayksikön riskienhallinnan tukeminen selvittämällä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoittamalla tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti	906/2019 13.1 §

Tehtävä	Säädökset
tietojärjestelmien omistajien ja vastuuhenkilöiden tukeminen tietoturvatoimenpiteiden suunnittelussa	906/2019 4.2 § 1-4 k
säännöllinen keskustelu tiedonhallintayksikön toimintojen kanssa tietoturvallisuuskysymyksistä	906/2019 13.1 §
tiedonhallintayksikön tietosuojavastaavan tukeminen tietoturvallisuutta koskevissa asioissa	906/2019 17 §
osallistuminen tiedonhallintayksikön ICT-varautumiseen ja toiminnan jatkuvuuden hallintaan	906/2019 4.2 § 2 k, 13.2 §