



11.02.2022

JulkICT-osasto
Tuija Kuusisto**Digitaalisen turvallisuuden strateginen johtoryhmä**Aika 11.02.2022 klo 13-15
Paikka Skype

Osallistujat alivaltiosihteeri Päivi Nerg, valtiovarainministeriö, puheenjohtaja
ICT-johtaja, ylijohdaja Jarkko Levasma, valtiovarainministeriö, varapuheenjohtaja
budjettineuvos, yksikön päällikkö Tomi Hytönen, valtiovarainministeriö
osastopäällikkö Janne Kerkelä, valtioneuvoston kanslia
alivaltiosihteeri Pekka Puustinen, ulkoministeriö
tietohallintopäällikkö Mikko Soikkeli ylijohdaja Raimo Jyväsjärven sijaisena,
puolustusministeriö
ylijohdaja Jukka Aalto, sisäministeriö
osastopäällikkö, ylijohdaja Laura Eiro, liikenne- ja viestintäministeriö
kyberturvallisuusjohtaja Rauli Paananen, liikenne- ja viestintäministeriö
johtaja Minna Saario, sosiaali- ja terveysministeriö
hallitusneuvos Kari Klemm, työ- ja elinkeinoministeriö
tietoyhteiskunta-asiain johtaja Tommi Karttaavi, Kuntaliitto
pääsihteeri Petri Toivonen, Turvallisuuskomitea
varautumispäällikkö Jarna Hartikainen, Huoltovarmuuskeskus
pääjohtaja Janne Viskari, Digi- ja väestötietovirasto
tietohallintoneuvos Tuija Kuusisto, valtiovarainministeriö, sihteeri
johtava erityisasiantuntija Kimmo Rousku, Digi- ja väestötietovirasto, sihteeri

Erikseen kutsutut esittelijät: turvallisuusjohtaja Hannu Naumanen, Valtori, kohta 3
tietoturva-asiantuntija Karoliina Kemppainen, Liikenne- ja viestintävirasto, kohta 4
erityisasiantuntija Marième Korhonen, liikenne- ja viestintäministeriö, kohta 5
erityisasiantuntija Niko Mäkilä, valtiovarainministeriö, kohta 6
JUDO-hankepäällikkö Erja Kinnunen, Digi- ja viestintävirasto, kohta 6

Poissa kaupunginjohtaja Ritva Viljanen, Vantaa
työelämäprofessori Jarno Limnell, Aalto-yliopisto**1 Kokouksen avaus**

Puheenjohtaja avasi kokouksen. Todettiin, että Huoltovarmuuskeskuksen johtaja Sauli Savisalonen seuraajana ryhmässä on jatkossa varautumispäällikkö Jarna Hartikainen Huoltovarmuuskeskuksesta.

2 Edellisen kokouksen pöytäkirjan hyväksyminen

Hyväksyttiin edellisen kokouksen 8.10.2021 pöytäkirja.

3 Valtorin tietoturvallisuuden kehittäminen, ja edistämiseksi tarvittavat toimet

Turvallisuusjohtaja Hannu Naumanen Valtorista kertoi Valtorin tietoturvallisuuden kehittämiseksi toteutetuista toimenpiteistä. Hän korosti, että tuki viranomaisten tiedonvaihdolle tilannekuvan ylläpitämiseksi sekä havainnointi- ja reagointikyvyn kasvattamiseksi olisi tärkeää. Tietoturvallisuuden arviointitoiminnassa on vähän hyväksytyjä arviointilaitoksia. Keskustelussa todettiin, että osaavan työvoiman saatavuuskysymys nousee usein esille. Rauli Paananen kertoi, että Kyberturvallisuusstrategian kehittämisohjelman kautta on rahoitettu harjoittelua, sekä turvallista mobiiliratkaisua. Valtorin rooli on nähty tärkeänä harjoituksissa. Janne Kerkelä totesi, että hyväksytyin arviointilaitoksen suorittama minimietoturvatason arviointi tulisi olla saatavilla palvelujen osalta. Hannu Naumanen kertoi, että uudet palvelut noudattavat määrämuotoista käyttöönottoprosessia, johon kuuluu hyväksytyin arviointilaitoksen suorittama palvelun tietoturvallisuusvaatimusten todentaminen. Jarkko Levasma tähdensi, että pilvipalveluissa käsiteltävä tietoja koskevat päätökset ovat EU:n tietosuoja-asetuksen mukaisesti viranomaiskohtaisia. Jukka Aalto totesi, että yhteiset palvelut sekä havainnointikyvyn kehittäminen ovat merkittäviä.

Tomi Hytösen totesi, että viranomaisten väliseen tietojenvaihtoon pitäisi saada parempi malli: esimerkiksi Valtorin ja Kyberturvallisuuskeskuksen välille, jotta Valtorin tilannekuvatieto paranisi ja Valtorin toimintaa voitaisiin parantaa ja ennakkollistaa. Tätä voisi selvittää ja tutkia Titukrin Kyber-PTR-selvityksessä. Pekka Puustinen totesi, että uusien palvelujen ja viime kädessä kaikkien palvelujen tietoturvallisuuden todentaminen on merkittävää. Hän myös korosti asiakaslähtöisyyttä. Merkittiin tiedoksi Valtorin tietoturvallisuuden kehittämiseksi toteutettavat toimet, ja niistä käyty keskustelu. Liite 1, salassa pidettävä.

4 Kuntien tietoverkkoskannausten tulokset ja jatkoaskeleet

Tietoturva-asiantuntija Karoliina Kemppainen Liikenne- ja viestintävirastosta kertoi kuntien tietoverkkoskannauspilotointien toteuttamisesta, tuloksista ja jatkotoimenpiteistä. Pilottikunnilla oli haasteita skannauksessa tarvittavien lähtötietojen keräämisessä. Skannausten automaatioastetta olisi perusteltua nostaa jatkossa. Pilottikunnat kokivat skannaukset hyödyllisiksi, ja niille toivottiin jatkoa. Pilottikunnat suorittivat skannausten perusteella digitaalisen turvallisuuden korjaavia toimenpiteitä, ja kykenivät toteuttamaan ICT-palvelutuottajien valvontaa ja vastuuttamista skannaustulosten perusteella. Uusintaskannausten tulosten perusteella vahvistui käsitys siitä, että pilottikunnat olivat toteuttaneet korjaavia toimenpiteitä. Karoliina Kemppainen korosti, että kunnilla itsellään on vastuu riskienarvioinnista ja toimenpiteistä skannaustietojen perusteella. Liikenne- ja viestintävirastolla on tavoitteena lisätä julkisen hallinnon tietoverkkoskannausten toteuttaminen jatkuvien palvelujen palveluvalikoimaan.

Puheenjohtaja totesi, että palvelun jatkopohdinnoissa on perusteltua tarkastella myös hyvinvointialueiden tarpeita skannauspalvelun osalta. Minna Saario kertoi, että siirtymäaikana riskialttius ja tarve tämän kaltaisille palveluille on tunnistettavissa. Tommi Karttaavi sanoi, että olisi hyvä, että palvelua saataisiin laajennuttua kaikille ja se saataisiin pysyväksi palveluksi. Hän myös totesi, että pitäisi pystyä paneutumaan niihin syihin, joiden johdosta haavoittuvuuksia skannauksissa löytyy. Janne Viskari totesi, että kunnat tarvitsevat skannausten kaltaista käytännön konkreettista tukea. Hän myös sanoi, että Vahti-toiminnan piirissäkin voitaisiin pohtia kuntien saattamista käytännön asiantuntijatuen piiriin paremmin. Kimmo Rousku kertoi, että skannuspilotointien tuloksia on käsitelty myös Vahti-johtoryhmässä. Pilotoinnin kokemusten perusteella keskimäärin joka sadas palvelu on sisältänyt haavoittuvuuden. Merkittiin tiedoksi kuntien tietoverkkoskannausten tulokset ja niistä käyty keskustelu. Liite 2.

5 EU:n päivitetyn verkko- ja tietoturvadirektiiviehdotuksen NIS2.0 kansallinen toimeenpano

Erityisasiantuntija Marième Korhonen liikenne- ja viestintäministeriöstä kertoi verkko- ja tietoturvadirektiiviehdotuksen NIS2.0 käsittelytilanteesta sekä kansallisen toimeenpanon suunnitelmista. Euroopan Komissio antoi 16.12.2020 ehdotuksensa direktiiviksi (COM(2020) 823 final) kyberturvallisuuden korkean tason varmistamiseksi Euroopan unionin alueella ja verkko- ja tietoturvadirektiivin (EU) 2016/1148 kumoamisesta, tuttavallisemmin NIS-direktiivi. Uusi direktiiviehdotus kyberturvallisuuden korkean tason varmistamiseksi EU:n alueella, ns NIS2.0, perustuu nykyiseen verkko- ja tietoturvadirektiiviin NIS.

Marième Korhonen nosti esille, että uuden direktiivin myötä ei ole enää välttämätöntä tarvetta kansalliselle toimijoiden identifiointiprosessille. Soveltamisala myös laajenee merkittävästi, ja mukaan tulee uusia soveltamisaloja kuten julkishallinto. Euroopan neuvoston kompromissiehdotuksessa valtiotoimijat kuuluisivat soveltamisalaan, ja kansallisen harkintavallan perusteella myös mahdollisesti alueelliset ja paikalliset julkisen hallinnon toimijat. Toimijat jaetaan keskeisiin ja tärkeisiin. Keskeisiin toimijoihin sovellettaisiin ennako- ja jälkivalvontaan, tärkeisiin ainoastaan jälkivalvontaa. Toimijoilta edellytetään uusien riskienhallintatoimenpiteiden käyttöönottamista, koskien myös tuotantoketjuja. Toimijoilla on velvollisuus raportoida poikkeamista valvovalle viranomaiselle. Valvontaviranomainen voi määrätä sanktioita. Kansallisessa harkintavallassa on sanktioiden määrääminen julkisen hallinnon toimijoille.

Suomi on pitänyt ehdotusta ja sen velvoitteita kannatettavana. Yhteistyön tiivistäminen on nähty tärkeänä, samoin kansallisen liikkumavaran säilyttäminen. Direktiiviehdotuksen käsittely on pääpiirteissään edennyt Suomen kannan mukaiseen suuntaan. Direktiivin laajentaminen julkiseen hallintoon on herättänyt keskustelua. Kokoperustaisen kriteeristön ja riskiperustaisuuden välinen suhde on ollut keskeinen kysymys. Samoin direktiiviehdotuksen suhde muuhun relevanttiin säätelyyn, kuten CER-direktiivi ja DORA on ollut keskustelussa. Direktiiviehdotus on trilogineuvottelujen vaiheessa. Ranska tähtää siihen, että trilogineuvottelut saataisiin päätökseen tämän vuoden kesäkuuhun mennessä.

Uusi direktiivi on laajempi kuin NIS, joten kansallinen täytäntöönpanokin on laajempi. Kansallinen täytäntöönpano alkaa aikaisintaan syksyllä 2022. Tarkoituksena on täytäntöönpanossa tehdä tiivistä yhteistyötä eri hallinnonalojen kanssa. Kansallisen täytäntöönpanon valmisteluryhmässä on tarkoitus joko päivittää sektorilaisääntöä tai valmistella uusi säädös. Kyberturvallisuusstrategian päivistytyö on tarkoitus toteuttaa uuden direktiivin täytäntöönpanon yhteydessä. Uuden direktiivin siirtymäajaksi on suunniteltu 18 tai 24 kuukautta.

Keskustelussa korostettiin riskilähtöisyyttä ja kansallista liikkumavaraa. Merkittiin tiedoksi NIS2.0 kansallinen toimeenpano ja siitä käyty keskustelu. Liite 3.

Pekka Puustinen, Laura Eiro ja Jarkko Levasma poistuivat kokouksesta.

6 Haukka ja Judo-hankkeiden työsuunnitelma 2022 ja tehtävien edistämiseksi tarvittavat toimet

Tietohallintoneuvos Tuija Kuusisto valtiovarainministeriöstä kertoi yleisesti Haukka-hankkeen tehtävistä Valtiovarainministeriössä, Digi- ja väestötietovirastossa sekä Liikenne- ja viestintävirastossa, ja hankkeen valtiovarainministeriössä toteuttavat tuotokset vuonna 2022. Judo-hankepäällikkö Erja Kinnunen Digi- ja väestötietovirastosta kertoi Judo-hankkeen tehtävistä ja tuloksista vuonna 2022. Vahti-pääsihteeri Kimmo Rousku Digi- ja väestötietovirastosta kertoi digiturvatietoisuuden lisäämisen vaikuttavuudesta vuonna 2021 sekä

vuoden 22 tehtävistä. Minna Saario totesi, että digiturvavartit ovat hyvä toimintamalli. Hyväksyttiin Haukka-työsuunnitelma 2022 ja merkittiin tiedoksi Judo-työsuunnitelma 2022 ja siitä käyty keskustelu. Liite 4 ja 5.

7 Mahdolliset muut asiat

Seuraavat kokoukset:

- 21.4.2022 klo 14-16
 - Titukri, keskeiset toimenpiteet ja niiden edistämiseksi tarvittavat toimet
 - Kyberturvallisuusstrategian kehittämisohjelma, keskeiset toimenpiteet ja niiden edistämiseksi tarvittavat toimet
 - Digitaalisen turvallisuuden alueen syötteitä seuraavan hallitusohjelman valmisteluun
- 17.6.2022 klo 13-15
 - Valtorin tietoturvallisuuden edistyminen
 - Kuntien digitaalisen turvallisuuden palvelujen tiekartta, ja palvelujen edistämiseksi tarvittavat toimet
 - Haukka ja Judo-hankkeiden tehtävien edistyminen ja keskeiset tulokset
 - Hyvinvointialueiden digitaalisen turvallisuuden katsaus, STM:n kanssa sovitaan

Tiedoksi:

Haukka-hankkeen kuntien digiturvapalvelujen koordinaatioryhmä hyväksyi 26.1.22 Kuntien digiturvan tiekarttasuunnitelman, liite 6.

Tiedonhallintalautakunnan suositus Turvallisuusluokiteltavien asiakirjojen käsittelystä pilvipalveluissa on julkaistu 10.1.2022 ([VM 2022:4](#)).

Liitteet	Liite 1	Valtorin tietoturvallisuuden kehittäminen, valmistuu myöhemmin
	Liite 2	Kuntien tietoverkkoskannausten tulokset ja jatkoaskeleet
	Liite 3	NIS2.0 kansallinen toimeenpano
	Liite 4	Haukka-hankkeen työsuunnitelma 2022
	Liite 5	Judo-hankkeen työsuunnitelma 2022
	Liite 6	Kuntien digiturvan tiekarttasuunnitelma
	Liite 7	Haukka-hankeen edistymisen seuranta-excel