VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

NIS2 direktiivin kansallinen toimeenpano julkishallinnossa – webinaari 4.5.2023 klo 9-11

VM:N ALATYÖRYHMÄ

Tervetuloa

- klo 9 Tervetuloa ja aloitussanat (Tomi Hytönen, VM)

  Käytännön asioita (Sami Aalto, VM)
- klo 9.05 NIS2-direktiivi (Veikko Vauhkonen, LVM)

  Direktiivin pääasiallinen sisältö
- klo 9.30 Kansallinen toimeenpano julkishallinnon osalta (Eeva Lantto, VM)

  Valmistelu ja aikataulu

  Keskeisiä kysymyksiä toimeenpanossa julkishallinnon osalta
- klo 10 Ennakkokysymykset ja mahdollisuus esittää kysymyksiä (alatyöryhmän pj:t ja sihteeristö)
- klo 10.55 Yhteenveto ja päätös

Käytännön asioita

- Tilaisuus tallennetaan
  - Tallenne mahdollista saada pyytämällä sitä tilaisuuden jälkeen (sami.j.aalto@gov.fi)
- Materiaali lisätään hankeikkunaan https://valtioneuvosto.fi/hanke?tunnus=LVM044:00/2022
- Mikrofonit ja kamerat suljettu
  - Mahdollista esittää kysymyksiä chat-kentässä
  - Mahdollisuus esittää kysymyksiä sihteeristölle myös tilaisuuden jälkeen (sami.j.aalto@gov.fi)

NIS2 direktiivi

NIS2 direktiivin kansallinen toimeenpano

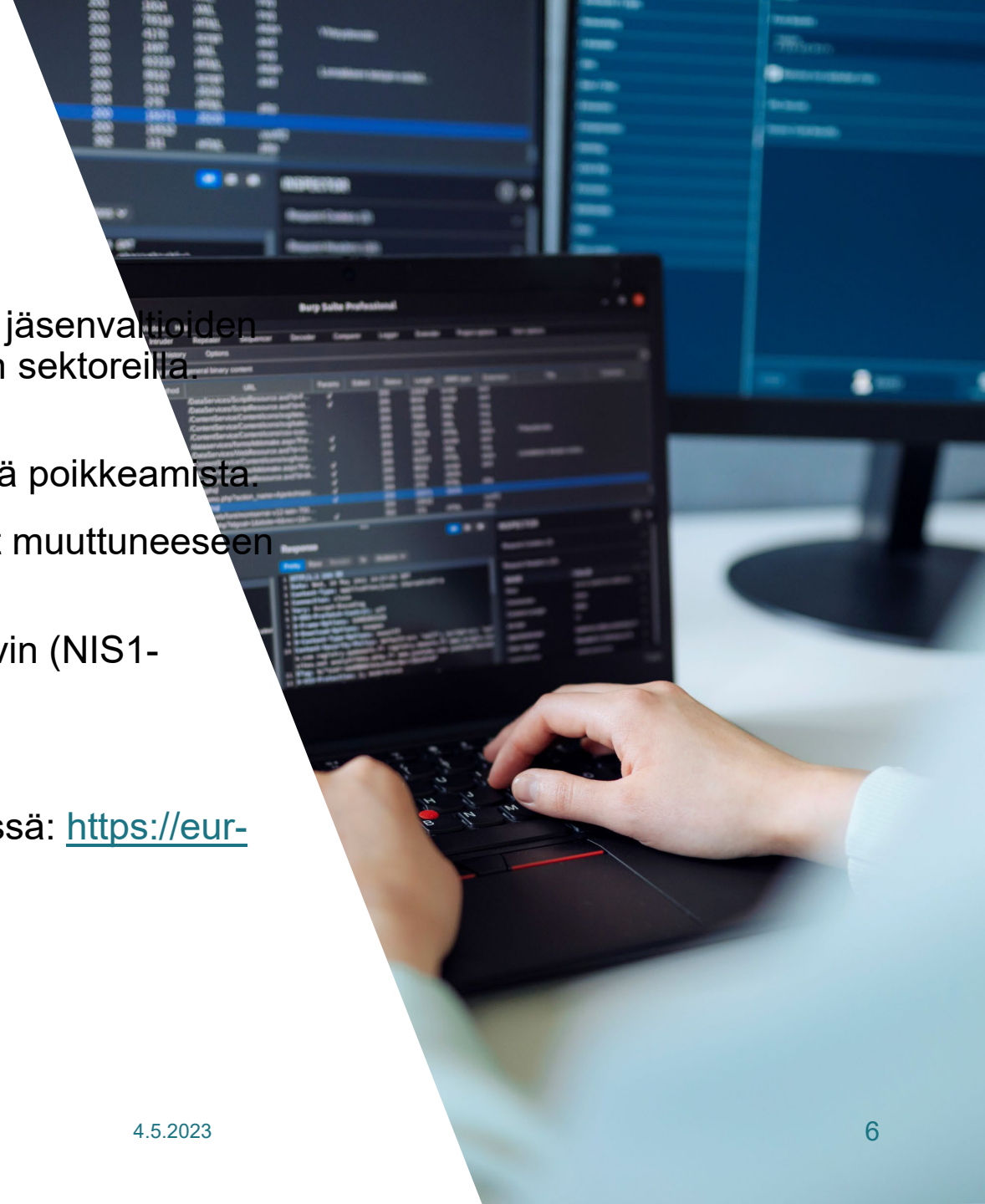
Julkishallinnon webinaari 4.5.2023

Veikko Vauhkonen
Hallitussihteeri
Tieto- ja turvallisuusosasto, turvallisuusyksikkö

LIIKENNE- JA VIESTINTÄMINISTERIÖ

Mikä on NIS2 direktiivi?

- NIS2 direktiivin tavoitteena on vahvistaa ja yhdenmukaistaa jäsenvaltioiden ja EU:n yhteistä kyberturvallisuustasoa tietyillä yhteiskunnan sektoreilla.
- Direktiivissä esitetään kyberturvallisuutta vahvistavia riskienhallintavelvoitteita ja raportointivelvoitteet merkittävistä poikkeamista.
- Velvoitteet ovat vähimmäistason velvoitteita, jotka vastaavat muuttuneeseen kybertoimintaympäristöön.
- NIS2 direktiivi kumoaa aiemman verkko- ja tietoturvadirektiivin (NIS1-direktiivi).



- NIS2 direktiivi julkaistiin 27.12.2022 EU:n virallisessa lehdessä: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
- Kansallisen täytäntöönpanon määräaika: 17.10.2024.

Mikä muuttuu?

- Suuret ja keskisuuret toimijat suoraan sääntelyn piirissä, pienet ja mikrotoimijat lähtökohtaisesti sääntelyn ulkopuolella, tietyt poikkeukset mahdollisia
- Soveltamisala laajenee
- Sektoreiden jaottelu keskeisiin ja tärkeisiin, merkityksellistä valvonnan ja seuraamusjärjestelmän kannalta (ennakko- ja jälkivalvonta)
- Tarkemmat riskienhallintavelvoitteet
- Kolmiportainen raportointivelvoite merkittävistä kyberpoikkeamista
- Ennakko- ja jälkivalvonta riippuen toimijan kategoriasta (keskeinen / tärkeä)
- Haavoittuvuuksien tunnistaminen ja varautuminen laajamittaisten kyberhäiriöiden varalle
- Seuraamukset riskienhallintavelvoitteiden laiminlyönnistä

NIS2-direktiivi sisältää lisäksi säännöksiä mm. yhteiskunnan kyberturvallisuusstrategian laatimisesta, CSIRT-yksiköistä, kv-yhteistyöstä ja Euroopan haavoittuvuustietokannasta.

NIS2 toimialat (uudet punaisella)

Liite I

- Energia (vety- ja latauspisteiden palveluntarjoajat)
- Liikenne
- Pankkitoiminta
- Finanssimarkkinoiden infrastruktuuri
- Terveys
- Juomavesi
- Jätevesi
- Digitaalinen infrastruktuuri (tele, luottamuspalvelut, CDN, konesalit)
- TVT-palvelujen hallinta (yritysten välinen)
- Julkishallinto
- Avaruus

Liite II

- Posti- ja kuriiripalvelut
- Jätehuolto
- Kemikaalien valmistus, tuotanto ja jakelu
- Elintarvikkeiden tuotanto, jalostus ja jakelu
- Valmistus (mm. lääkintälaitteet, tietokoneet, sähkölaitteet, kulkuneuvot)
- Digitaalisen palvelun tarjoajat (verkkoyhteisöalustojen tarjoajat)
- Tutkimustoiminta

Kuuluuko organisaationi NIS2 direktiivin soveltamisalaan?

- Jos organisaatiosi pääasiallinen toiminta kuuluu johonkin NIS2-direktiivin sektoriin (liitteet I-II), täyttää jonkin siinä esitetyn toimijatyyppimääritelmän ja on kooltaan vähintään keskisuuri;

Tai

- olet CER-direktiivin mukaisesti määritelty kriittinen toimija koosta riippumatta (2 artiklan 3 kohta)

Tai

- täytät NIS2 direktiivin 2 artiklan 2 tai 4 alakohtien kriteerit koosta riippumatta

Sektoreissa ei merkitystä, onko julkinen vai yksityisen taho. Julkishallinto erillinen sektori.

Keskus- ja aluetason julkishallinnon toimijat kuuluvat sekä kuuluvat soveltamisalaan koosta riippumatta, paitsi sellaisen aluetason toimijan osalta, joka riskiperusteisen arvioinnin perusteella ei tarjoa palveluja, joiden häiriintymisellä voisi olla merkittävä vaikutus yhteiskunnan tai talouden kriittisiin toimijoihin.

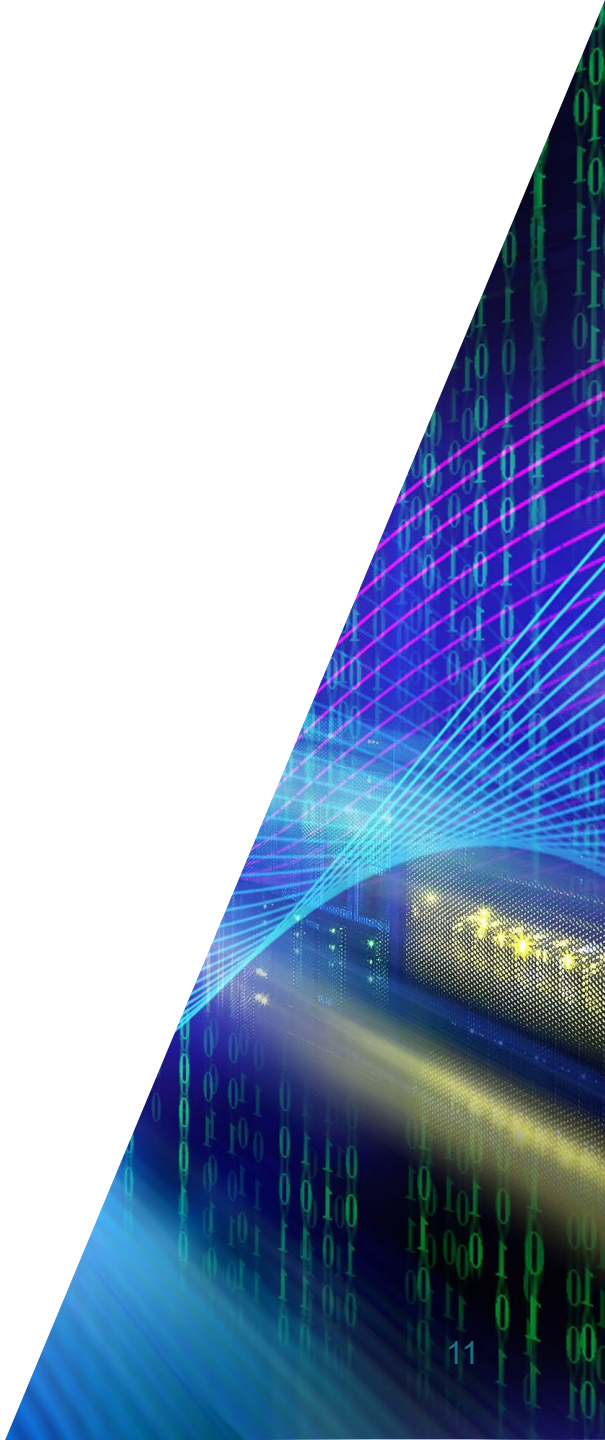
Kansallinen liikkumavara: Paikallistason julkishallinnon toimijat, opetus- ja koulutusala

Soveltamisalan ulkopuolella: kansallinen turvallisuus, yleinen järjestys ja turvallisuus, puolustus, lainvalvonta.

Riskienhallintavelvoitteet ja raportointivelvoitteet

Riskienhallintavelvoitteet

- Direktiivin 21 artiklassa esitetään riskienhallintavelvoitteet, jotka kaikkien soveltamisalaan kuuluvien toimijoiden tulee ottaa käyttöön riskiperustaisesti.
- Verkko- ja tietojärjestelmiin kohdistuvien riskien arviointi, tietyt arvioinnissa huomioitavat vähimmäisosa-alueet sekä tarpeellisten riskinhallintatoimenpiteiden tunnistaminen ja toteuttaminen organisaatiossa.
- Velvoitteiden tavoitteena on estää tai minimoida poikkeamien vaikutus palvelujen vastaanottajiin ja muihin palveluihin.
- Riskienhallintavelvoitteisiin sisältyy mm. riskianalyysit, toiminnan jatkuvuuden hallinta, poikkeamien käsittely ja havainnointi.
- Teknologianeutraali lähestymistapa, jotta velvoitteet kestävät aikaa ja soveltuisivat vähimmäistason velvoitteiksi kaikille soveltamisalaan kuuluville sektoreille.
- Jos et kuulu CER-direktiivin piiriin eikä kaikki vaaratekijät huomioiva lähestymistapa tule katettua jo sitä kautta, tulee samaa lähestymistapaa soveltaa NIS2 riskienhallintavelvoitteiden kautta.
- Vastuu ylimmällä johdolla.



Kolmiportainen raportointivelvoite merkittävistä poikkeamista

Ensi-ilmoitus 24h kuluessa

Jatkoilmoitus 72h kuluessa

Mahdollinen väliraportti

Loppuraportti 1kk kuluessa

- Valvovan viranomaisen tulee vastata ensi-ilmoitukseen 24 tunnin kuluessa ja voi toimijan pyynnöstä antaa ohjeita poikkeamatilanteeseen yhteistyössä CSIRT-yksikön (KTK) kanssa.
- Valvovalle viranomaiselle voi ilmoittaa vapaaehtoisesti myös muista kuin merkittävistä poikkeamista, kyberuhkista ja läheltä piti –tilanteista.
- Toimijan tulee tiedottaa palvelujensa vastaanottajia merkittävästä kyberuhasta.

Ennakko- ja jälkivalvonta

Keskeinen toimija (*ylittää* keskisuuren yrityksen määritelmän) CER-toimijat

- Ennakkovalvonta
- Jälkivalvonta
- Hallinnolliset seuraamusmaksut velvoitteiden laiminlyönnistä, enintään 10 milj. euroa tai 2 % vuosittaisesta liikevaihdosta.

Tärkeä toimija (*täyttää* keskisuuren yrityksen määritelmän)

- Jälkivalvonta
- Hallinnolliset seuraamusmaksut velvoitteiden laiminlyönnistä, enintään 7 milj. euroa tai 1,4 % vuosittaisesta liikevaihdosta.

NIS2 kansallisen toimeenpanohankkeen aikataulu, keskeiset ajankohdat

- Toimeenpanoaika 21 kk, määräaika 17.10.2024
- **Kansallinen soveltaminen alkaa 18.10.2024.**
- Hanke käynnistettiin virallisesti tammikuussa 2023.
  - Työryhmärakenne koostuu päätyöryhmästä (LVM pj.) ja julkishallinnon sektoria koskevasta alatyöryhmästä (VM pj.)
  - Hankkeen laaja-alaisuuden vuoksi valmisteluun osallistuu kaikki hallinnonalat, päätyöryhmätyöskentelyssä kuullaan myös keskeisten etujärjestöjen edustajia sidosryhmäkuulemisten lisäksi.
  - Sidosryhmäkuulemisia järjestetään pitkin hanketta ja kirjallinen lausuntokierros pidetään syksyllä 2023.
    - Yleinen sidosryhmätilaisuus 30.3.2023, julkishallinnon webinaari 4.5.2023.
  - Tavoitteena on, että HE annettaisiin eduskunnalle 2024 kevättalvella.

Kansallinen toimeenpano (päätyöryhmä)

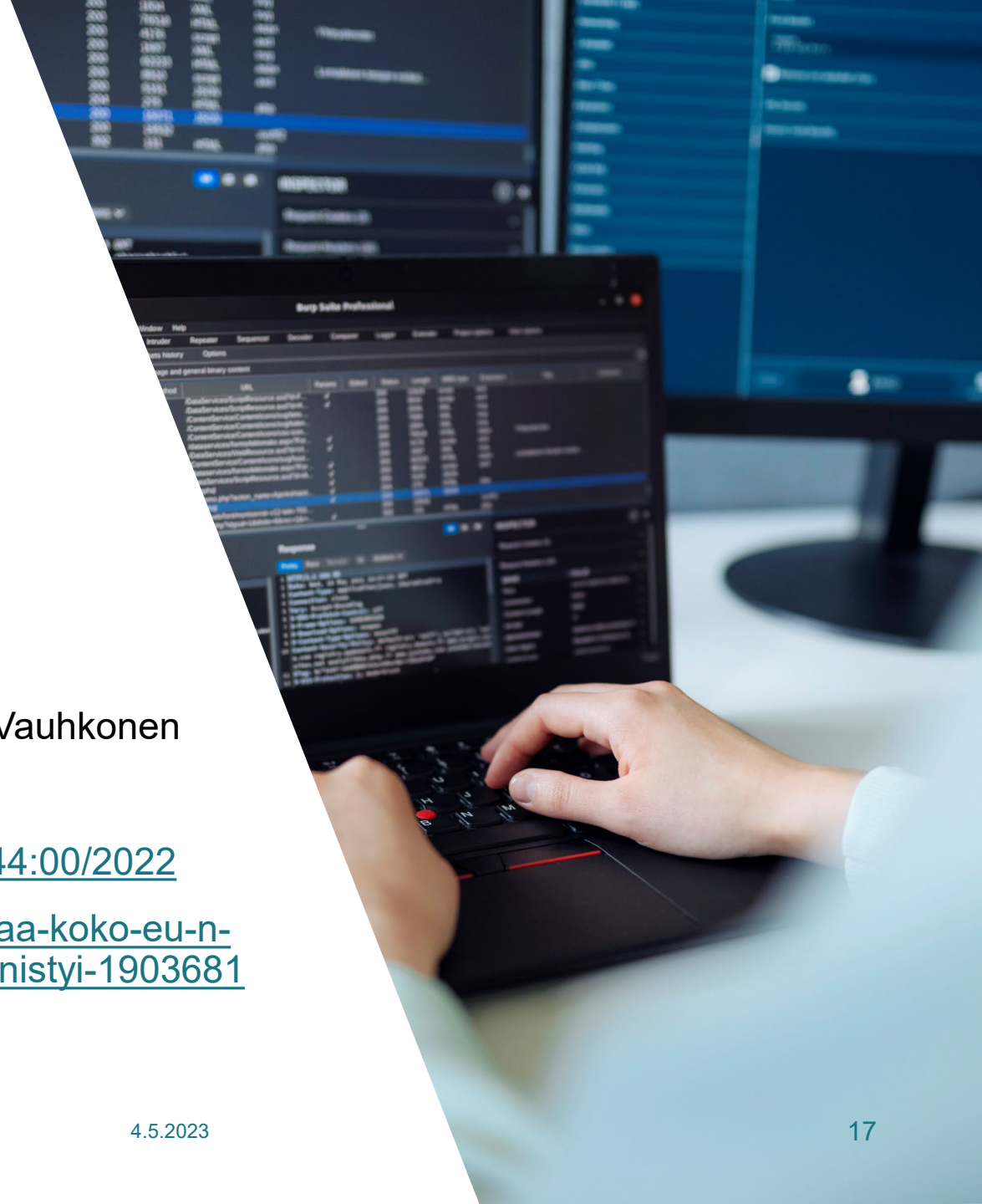
- Yleislaki, jossa pyritään säilyttämään direktiivin vähimmäistason osoittava vaikutus myös kansallisesti.
  - Riskienhallintavelvoitteita voitaisiin tarkentaa alakohtaisilla ohjeilla ja määräyksillä, joissa huomioidaan sektorikohtaiset erityispiirteet.
  - Sektorikohtaista sääntelyä voi soveltaa ensisijaisesti, jos se täyttää NIS2 velvoitteet, esim. ilmailualan sääntely, finanssialalla DORA-asetus.
- Jatketaan NIS1 aikaista jaottelua sektorikohtaisista valvovista viranomaisista + KTK keskitettynä yhteyspisteenä ja CSIRT-yksikkönä.
- Pyritään luomaan NIS2 ilmoituksia varten keskitetty sähköinen asiointilomake, rajataan toteutusmahdollisuuksien vuoksi NIS2 raportointivelvoitteisiin.
- Valmistelu yhteensovitetaan muiden relevanttien hankkeiden kanssa, kuten CER-direktiivi ja DORA-asetus.

Kansallinen toimeenpano (alatyöryhmä)

- Alatyöryhmässä ovat edustettuna kaikki ministeriöt ja Kuntaliitto. Hyvinvointialueiden edustajaa ei ole vielä nimetty.
- Julkishallinnon osalta direktiivi koskee (julkishallinnon toimialan ominaisuudessa) keskustason ja aluetason toimijoita
  - Kansallisesti harkitaan sääntelyn laajempaa soveltamista.
- Julkishallinnon toimijoiden velvoitteet lähtökohtaisesti tiedonhallintalakiin
  - Osa direktiivin edellyttämästä sääntelystä yleislaissa
- Keskeisiä kysymyksiä julkishallinnon osalta: sääntelyn soveltamisen laajuus, toimivaltainen viranomainen, vaikutukset, sääntelyn yhteensovittaminen

Mitä seuraavaksi?

- Työryhmät kokoontuvat kuukausittain
- HE luonnosta ja vaikutusarviointia valmistellaan parhaillaan
  - Hankinta vaikutustenarvioinnista
- Lausuntokierros syksyllä 2023
- Tavoite HE:n antamiselle alkuvuosi 2024



LVM:n valmistelijat: Mariéme Korhonen, Sonja Töyrylä, Veikko Vauhkonen

Lisätietoja:

- Hankeikkuna: https://valtioneuvosto.fi/hanke?tunnus=LVM044:00/2022
- LVM.fi: https://www.lvm.fi/-/kyberturvallisuusdirektiivi-vahvistaa-koko-eu-n-kyberturvallisuustasoa-kansallinen-toimeenpanohanke-kaynnistyi-1903681

Kiitos!

lvm.fi Twitter: @lvmfi

LIIKENNE- JA VIESTINTÄMINISTERIÖ

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

NIS2-direktiivi – Kansallinen toimeenpano julkishallinnon osalta

NIS2-DIREKTIIVIN KANSALLINEN TOIMEENPANO JULKISHALLINNOSSA – WEBINAARI 4.5.2023 KLO 9–11, EEVA LANTTO, VM

Kysymyskokonaisuudet

- Keskeisiä kysymyksiä toimeenpanossa julkishallinnon osalta
  - Soveltaminen julkishallinnon toimijoihin (I – IV)
  - Toimijoiden velvollisuudet
  - Toimivaltainen viranomainen – julkishallinto
  - Toimijoiden valvontatoimet

Soveltaminen julkishallinnon toimijoihin I

- Direktiiviä sovelletaan julkishallinnon toimijaan, jonka jäsenvaltio on kansallisen lainsäädäntönsä mukaisesti määritellyt (2 art 2.f))
  - keskustason julkishallinnon toimijaksi;
  - aluetason julkishallinnon toimijaksi ja joka riskiperusteisen arvioinnin perusteella tarjoaa palveluja, joiden häiriintymisellä voisi olla merkittävä vaikutus yhteiskunnan tai talouden kriittisiin toimintoihin.
- Direktiivillä ei estetä jäsenvaltioita antamasta tai pitämästä voimassa säännöksiä, joilla varmistetaan kyberturvallisuuden korkeampi taso (5 art)
- Jäsenvaltiot voivat säätää, että tätä direktiiviä sovelletaan (2 art 5.)
  - paikallistason julkishallinnon toimijoihin;
  - opetus- ja koulutusalan laitoksiin, etenkin kun niissä harjoitetaan olennaisen tärkeää tutkimus-toimintaa.

Soveltaminen julkishallinnon toimijoihin II

- 6 art 35: Julkishallinnon toimijalla [tarkoitetaan] jäsenvaltiossa kansallisen lainsäädännön mukaisesti julkishallinnon toimijaksi tunnustettua toimijaa, lukuun ottamatta oikeuslaitosta, parlamentteja ja keskuspankkeja, joka täyttää seuraavat kriteerit:

  a) se on perustettu tyydyttämään yleisen edun mukaisia tarpeita, eikä sillä ole teollista tai kaupallista luonnetta;

  b) se on oikeushenkilö tai sillä on lain nojalla oikeus toimia toisen sellaisen toimijan puolesta, joka on oikeushenkilö;

  c) sitä rahoittavat pääosin valtio, alueviranomaiset tai muut julkisoikeudelliset laitokset, sen johto on näiden viran-omaisten tai laitosten valvonnan alainen taikka valtio, alueviranomaiset tai muut julkisoikeudelliset laitokset nimittävät yli puolet sen hallinto-, johto- tai valvontaelimen jäsenistä;

  d) sillä on valtuudet osoittaa luonnollisille henkilöille tai oikeushenkilöille hallinnollisia tai sääntelyyn liittyviä päätöksiä, jotka vaikuttavat näiden oikeuksiin henkilöiden, tavaroiden, palvelujen tai pääoman rajat ylittävässä liikkuvuudessa;

  Ainakin tuomioistuimet, eduskunta ja Suomen Pankki vähimmäissoveltamisalan ulkopuolella. Kansallisesti määriteltävissä, miltä osin velvoitteita sovelletaan mainittuihin toimijoihin..

  Direktiiviä ei myöskään sovelleta julkishallinnon toimijoihin kansallisen turvallisuuden, yleisen turvallisuuden, puolustuksen tai lainvalvonnan alalla, m.l. rikosten ennalta estäminen, tutkiminen, paljastaminen ja rikoksiin liittyvät syytetoimet. (2 art 7.) – eikä tietyiltä osin näille palveluja tarjoaviin (2.art 8.)

  Kansallisesti määriteltävissä, miltä osin velvoitteita ja valvontaa sovelletaan mainittuihin toimijoihin.

Soveltaminen julkishallinnon toimijoihin III

- Direktiiviä sovelletaan myös CER-direktiivin nojalla kriittisiksi toimijoiksi määritettyihin toimijoihin (2 art 3.), jotka ovat keskeisiä toimijoita (3 art 1. f))
- Lähtökohtaisesti keskustason toimijat ovat keskeisiä, aluetason tärkeitä
  - Jäsenvaltiolla määrittelyvaraa (3 art 1. e) ja g))

Kyse vähimmäissääntelystä, jäsenvaltio voi määritellä toisin, määrittelyllä merkitystä lähinnä toimijoiden lukumäärään (ilmoitettava komissiolle) sekä valvontaan. Tärkeitä toimijoita valvotaan ainoastaan jälkikäteen.

Soveltaminen julkishallinnon toimijoihin IV

Jäsenvaltion laadittava luettelo keskeisistä ja tärkeistä toimijoista (3 art 3. ja 4.)

- Toimijan ilmoitettava
  - a) toimijan nimi;
  - b) osoite ja ajantasaiset yhteystiedot, mukaan lukien sähköpostiosoitteet, IP-osoitealueet ja puhelinnumerot;
  - c) asiaankuuluva toimiala ja toimialan osa
- Muutoksista ilmoitettava kahden viikon kuluessa muutospäivästä
- Jäsenvaltiot voivat perustaa kansallisia järjestelyjä, joilla toimijat voivat itse kirjautua luetteloon

Traficom tehnee ilmoitusjärjestelmän mainittujen tietojen keräämiseksi.

Toimijoiden velvollisuudet (20 – 23 art)

- Toimijoiden hallintoelimen tulee hyväksyä kyberturvallisuusriskien hallintatoimenpiteet (21 art) ja valvoa niiden toteuttamista. Hallintoelin voidaan saattaa vastuuseen, jos toimija rikkoo 21 artiklaa
  - Tämän kohdan soveltaminen ei rajoita kansallisen lainsäädännön soveltamista, kun on kyse julkisiin laitoksiin sovellettavista vastuusäännöistä taikka virkamiesten tai vaalilla valittujen tai nimettyjen toimenhaltijoiden vastuusta.

- Raportointivelvoite merkittävistä poikkeamista (23 art) – vapaaehtoinen raportointi (30 art)
- Jäsenvaltioiden on yksinkertaistettava teknisesti 23 ja 30 artiklassa tarkoitettujen ilmoitusten tekemistä (13 art 6.)

Toimivaltainen viranomainen - julkishallinto

- Vastaa kyberturvallisuudesta ja VII luvussa tarkoitetuista valvontatehtävistä (8 art)
- Poikkeamat ilmoitettava joko toimivaltaiselle viranomaiselle tai CSIRT:lle.
  - Valmistelussa ilmoitusjärjestelmä, jossa ilmoitukset menisivät molemmille
- CSIRT (10 – 12 art) sekä keskitetty yhteyspiste ilmeisesti Traficomissa

Toimijoiden valvontatoimet

- Valvojalla asianmukaiset toimivaltuudet ja toiminnallinen riippumattomuus valvomistaan, sanotun kuitenkaan rajoittamatta kansallisten lainsäädäntö- ja toimielinkehysten soveltamista. Jäsenvaltiot voivat päättää määrätä kyseisiä toimijoita koskevia asianmukaisia, oikeasuhteisia ja tehokkaita valvonta- ja täytäntöönpanotoimenpiteitä kansallisten lainsäädäntö- ja toimielinkehysten mukaisesti (31 art 4.)
- Toiminnan keskeyttämiseen tms. liittyviä seuraamuksia ei sovelleta julkishallinnon toimijoihin (32 art 5.)
- Johdon vastuun toteuttaminen - Virkavastuun riittävyys? (32 art 6.)
- Jäsenvaltio päättää, voidaanko julkishallinnon toimijoille määrätä hallinnollisia sakkoja ja missä määrin (34 art 7.) Tietosuoja-asetuksen osalta ei voida määrätä

Voimaan saattamisesta julkishallinnossa

- Keskus-/valtionhallinnon julkishallinnon toimijoihin sekä kriittisiin aluetason toimijoihin on sovellettava direktiivin vaatimuksia (tietyin poikkeuksin)
- On myös mahdollista laajentaa soveltamisalaa tiedonhallintalain soveltamisalalle, jolloin direktiivin sääntelyä (säädetyltä osin) sovellettaisiin esim. kunnallisiin viranomaisiin ja muina kuin viranomaisina julkista hallintotehtävää hoitaviin.
- Arvioitava myös tietojen käsittelyä poikkeamailmoitusten yhteydessä (ainakin kansalliseen turvallisuuteen ym. liittyvien tietojen osalta)
- Toimivaltainen/valvova viranomainen julkishallinnossa vielä harkinnassa.

Ennakkokysymykset ja kysymyksiä

Ennakkokysymyksiä (vastaukset punaisella)

- Ulotetaanko kansallinen sääntely koskemaan:
  - kuntia ja kuntien liikelaitoksia (paikallisia toimijoita)
  - Maakuntaliittoja
  - yliopistoja ja korkeakouluja
  - Tuomioistuimia
  - Turvallisuusviranomaisia

  Direktiivi ei edellytä näiden kuulumista soveltamisalaan. Asia on kansallisessa harkinnassa. Kuntien liikelaitokset: jos toimivat NIS2-toimialalla (muu kuin julkishallinto) ja kuuluvat yleisen soveltamisalan kautta alaan, velvoitteet voivat tulla sitä kautta, vaikka julkishallinnon velvoittava ala ei niitä kattaisikaan.
- Miten NIS2 pitää ottaa käyttöön pienempien maakuntien energia ja vesihuoltolaitoksissa? Energia ja vesihuolto ovat osa LVM:n alaisen päätyöryhmän työtä ja valmisteilla olevassa yleislainsäädännössä säädetään muun ohessa näitä aloja koskevista vaatimuksista. Jos energia- tai vesihuoltotoimija kuuluu NIS2-soveltamisalaan koon ja toimialan perusteella, NIS2-yleisen soveltamisalan osalta merkityksellistä ei lähtökohtaisesti ole se, onko omistaja julkinen vai yksityinen taho (tai niiden yhdistelmä).
- Jaetaanko hyvinvointialueet eri luokkiin ennakko- ja jälkitarkastuskyvykkyyksien suhteen? Hyvinvointialueita ei ole tarkoitus käsitellä eri tavalla julkishallinnon toimialaa koskevassa sääntelyssä.
- Mikä toimielin on vastuussa CER-direktiivin & NIS2-direktiivin kansallisesta yhteensovittamisesta ja koordinoinnista? NIS-työryhmä on ollut aktiivinen CER-valmistelun suuntaan ja lopulta CER-hankkeessa ratkaistaan, miten NIS-sääntely halutaan CER-toimijoihin ulottaa. Toki NIS2-direktiivissä on tietyt vähimmäisvaatimukset tältäkin osin. Valmisteilla oleva NIS-yleislaki tarjoaa mahdollisuuksia tähän. Yhteensovittamista toki tehdään hankkeiden välillä.

Ennakkokysymyksiä

- Onko NIS2 kansallisessa implementoinnissa tarkoitus toteuttaa vain direktiivin minimitaso VAI onko vastuuministeriön intresseissä toteuttaa direktiiviä kovempaa kansallista regulaatiota? Lähtökohtana kansallisessa sääntelyssä on direktiivin velvoitteiden minimitaso.
- Mitä pitää ottaa huomioon jos toimija kuuluu kahden eri sektorin kautta direktiiviin ja näillä on eri valvova viranomainen? Pyritään selkeyttämään hallituksen esityksessä, mitä toimijan tulee tässä tilanteessa ottaa huomioon. Tarkoituksena, että yksi taho valvoo ja ilmoitukset yhdelle taholle.
- Onko kunnille suunniteltu erityistä tukea (taloudellinen tai muu) direktiivin toimeenpanon tueksi? Ei ole tietoa, ovatko kunnat soveltamisalassa. Jos ovat, arvioidaan tarve erikseen.
- Mikä viranomaistoimija on suunniteltu valtion virastojen yhteyspisteeksi tehtäviä ilmoituksia & ja poikkeamailmoituksia varten? NIS2-direktiivi edellyttää, että ilmoitukset tehdään toimivaltaiselle valvovalle viranomaiselle ja/tai CSIRT-yksikölle. Miten tämä ratkaistaan, on selvityksessä. Traficom/KTK on ehdotettu nimettäväksi CSIRT-yksiköksi. Toimivaltainen viranomainen julkishallinnon osalta on selvityksessä.

Ennakkokysymyksiä

- Kysymys liittyen direktiivin 23 artiklan 5) kohdan soveltamiseen: artiklan sanamuoto "mahdollisuuksien mukaan" antaa ymmärtää, että vastausta ei tarvitsisi esim. viikonlopun/pyhien aikaan antaa 24 tunnin kuluessa? Tämä tarkoittaisi käytännössä virastoissa jonkinlaista varallaolomenettelyä, mikäli 24h tulee sovellettavaksi myös viraston aukioloaikojen ulkopuolella. Täsmennetään yleislaissa, mitä konkreettisesti tarkoittaa. Direktiivin juridinen edellytys on without undue delay, mutta viittaus 24 tuntiin antaa ymmärtää, että kysymys on lähempänä välitöntä vastausta kuin sitä, mihin ”ilman aiheetonta viivytystä” Suomessa yleensä tulkitaan. 24/7-reagointitoiminto olisi CSIRT-yhteydessä
- Mistä löytyy selkeä, kattava ja yksiselitteinen kriteeristö, jonka perusteella voi tarkistaa, koskeeko direktiivi omaa organisaatiota? Pyritään lainsäädännössä ja perusteluissa täsmentämään. Myös ao. sektorin valvova viranomainen voi neuvoa tarvittaessa, kunhan valmistelu on edennyt hieman pidemmälle.
- Huomioidaanko NIS2 kansallisessa toimeenpanossa valtionhallinnon tai vastaavasti laajemmin julkisen hallinnon yhteiset palvelutuottajat olivat nämä sitten viranomaisia (esim. Valtori) tai liikelaitos tai yhtiöstatuksella. Jos sääntely koskee viranomaista, viranomainen vastaa kyberturvallisuudesta, vaikka se olisi sen ulkoistanut. Valtorin osalta arvioitava esim. vastuuta poikkeamailmoituksen tekemisestä.
- Miten ilmoitusvelvollisuus henkilötietojen tietoturvaloukkausten osalta yhteensovitetaan EU:n tietosuoja-asetuksen kanssa? Kyse on kahdesta eri velvoitteesta. NIS2 direktiivissä säädetään viranomaisten yhteistyöstä ja tiedonvaihdosta. NIS2-direktiivissä on yhteensovittamista tukevia elementtejä, mm. tietosuojaa ja NIS2-velvoitteita valvovien viranomaisten välillä, jotka otetaan huomioon täytäntöönpanossa. Sääntelyn kohteet ja velvoitteet eri, mutta usein voi olla niin, että tietoturvaloukkaukseen liittyy myös tietosuojaloukkaus.
- Entä tähän liittyvät mahdolliset hallinnolliset sakot tai muut seuraamusmaksut? Tarkoitus on, ettei julkishallinnon toimijoille voisi määrätä hallinnollisia seuraamusmaksuja. Selvityksessä on vielä maksun määrääminen siinä tapauksessa, jos julkishallinnon toimija toimii jollakin muulla sektorilla (yleislaki).

Ennakkokysymyksiä

- 1. Riskienhallintaa tässä kuvattiin viime syksyn luonnoksen perusteella, mutta voitteko kertoa, minkälaisia muutoksia tähän on tullut (etenkin prosessien, periaatteiden ja muun rakenteen osalta) sen jälkeen, eli mitkä ovat olleet viimeiset muutokset? Riskienhallinnan vähimmäistason voi katsoa direktiivistä, joka edellyttää tunnistamaan riskit, tekemään arviota, tekemään riittävät riskienhallintatoimet ja huomioimaan tietyt vähimmäisosa-alueet riskienhallinnassa.
- 2. Missä määrin riskienhallinnan näkemykset ja toteutustavat on kehitetty tässä tämän säädännön "sisällä" ja mitä erityisyyksiä tähän liittyy, verrattuna muuhun tulevaan EU:n digisääntelyyn tai riskienhallinnan tapohin ja standardeihin - mitkä asiat poikkeavat (tai vain saattavat vaikuttaa poikkeavan) normaalista riskienhallinnasta? Riippuu mitä ”normaalilla riskienhallinnalla” tarkoitetaan. Tämä voidaan ymmärtää esim. eri sektoreilla hyvinkin eri tavoin. NIS2-direktiivi on vähimmäistaso, jolla ei estetä pitämästä yllä korkeampaa tai pidemmälle menevää riskienhallintaa, joka takaa paremman kyberturvallisuuden tason. NIS2-direktiivi (tai tuleva yleislaki) ei siis lähtökohtaisesti edellytä tietyn standardin noudattamista ja pyrkimyksenä on muutenkin mahdollisimman teknologianeutraali ja aikaa kestävä lähestymistapa. Tarkoituksena on ollut, että velvoitteita voidaan tarkentaa viranomaisten määräyksillä sektorikohtaiset erityispiirteet ja teknologian/käytänteiden kehitys huomioiden.
- 3. Missä ovat mahdolliset kipupisteet ja avoimet kohdat suomen julkishallinnon osalta tässä sääntelykokonaisuudessa, sen käytännön toteuttamisessa? Soveltamisala ja valvonta sekä se, että täytäntöönpanon määräaika on lyhyt.

Yhteenveto ja päätös

VM:n alatyöryhmän puheenjohtajat ja sihteeristö

- alatyöryhmän pj. budjettineuvos Tomi Hytönen
- alatyöryhmän varapj. tietohallintoneuvos Aku Hilve
- sihteeristön jäsen lainsäädäntöneuvos Eeva Lantto
- sihteeristön jäsen neuvotteleva virkamies Sami Aalto
- sihteeristön jäsen säädösvalmisteluavustaja Nikos Markou