Valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla

xx.3.2021

Sisällys

1. Johdanto

Yhteiskunnan eri sektorit ovat yhä riippuvaisempia digitaalisten palveluiden käytöstä niin Suomessa kuin maailmanlaajuisesti. Yhteiskunnan keskeiset palvelut, kuten sähkön ja juomaveden jakelu sekä terveydenhuollon palvelut, tarvitsevat luotettavia yhteyksiä ja tietojärjestelmiä toimiakseen. Eri toimialoilla tulee viimeistään nyt ottaa huomioon, että tietoturvallisuuden ja tietosuojan merkitys palveluiden laadulle ja turvallisuudelle on perusedellytys digitaalisessa yhteiskunnassa.

Lainsäädännössä on asetettu yleisiä tietoturvallisuutta ja tietosuojaa koskevia velvollisuuksia, joita on erityisesti henkilötietosääntelyssä ja viranomaisia koskevissa yleislaeissa. Lisäksi Suomessa on useilla toimialoilla sektorikohtaisia velvoitteita huolehtia palveluiden ja tietojärjestelmien tietoturvasta ja tietosuojasta. Hyviä esimerkkejä tällaisista toimialoista ovat viestintä- ja finanssisektorit. Eri sektoreiden kyvykkyydet vastata kasvaviin tietoturva- ja tietosuojahaasteisiin vaihtelevat kuitenkin suuresti. Yhteiskunnan eri sektoreilla asetetaan toisistaan poikkeavia tietoturva- ja tietosuojavaatimuksia, joissa on pyritty huomioimaan kunkin toimialan erityispiirteitä. Myös lainsäädännön yhtenäistäminen EU:n tietosuojalainsäädännön vaatimusten kanssa on vielä kesken, vaikka usea ministeriö on jo toteuttanutkin uudistuksia. Yksin lakisääteiset velvoitteet ja määräykset eivät kuitenkaan ole riittäviä tietoturvallisuuden ja tietosuojan parantamisessa, vaan velvoitteita täydentävät eri toimialojen toimintakulttuuri, yhteinen tilannekuva, ymmärrys toimintaympäristön muutoksista sekä vapaaehtoinen yhteistyö viranomaisten sekä palveluiden tarjoajien välillä.

Tietoturvaa koskevat häiriöt ja loukkaukset sekä tietosuojaa koskevat loukkaukset voivat vaikuttaa merkittävästi toimialojen toimintaan ja palveluihin. Tämä pätee nykyään myös esineisiin, laitteisiin ja kulkuneuvoihin, joista yhä suurempi osa on yhteydessä internetiin, ja joiden toimintaa ohjataan digitaalista tietoa käsittelemällä. Käytössä olevien yhteyksien, palveluiden ja laitteiden tietoturvallisuuden taso vaikuttaa suoraan kansalaisten digitaalisia palveluita ja tuotteita kohtaan kokemaan luottamukseen. Tuotteet, palvelut ja tietojärjestelmät on suunniteltava, valmistettava ja ylläpidettävä siten, että tietoturva ja tietosuoja muodostavat niiden erottamattoman ja sisäänrakennetun osan. Toisin sanoen tietosuoja ja tietoturva on huomioitava toiminnan koko elinkaaren aikana tuote-, järjestelmä- ja palvelukehityksen lähtökohtana, eikä jälkikäteen päälle liimattavana tarrana tai laastarina.

Digitaalista toimintaympäristöä koskevan tiedon ja ymmärryksen lisääminen sekä toimivien ja turvallisten toimintamallien opastaminen yksityisille ja julkisille organisaatioille sekä yksittäisille käyttäjille on tärkeässä asemassa digitaalisessa yhteiskunnassa ja kansalaisten luottamuksen saavuttamisessa. Kyseessä on vahvasti myös riskien hallintaa koskeva kysymys, johon toimijoiden tulee vastata säilyttääkseen verkko- ja tietojärjestelmiensä turvallisuuden eheyden ja häiriönsietokyvyn. Yritystasolla häiriöt ja loukkaukset voivat aiheuttaa merkittäviä taloudellisia vahinkoja ja laajemmassa mittakaavassa häiriöillä voi olla vaikutusta koko yhteiskunnan huoltovarmuudelle ja peruspalveluiden saatavuudelle.

Psykoterapiakeskus Vastaamoon kohdistunut tietomurto osoitti, miten tietomurto tai kyberhyökkäys voi vaikuttaa merkittävästi tavallisten ihmisten arkeen ja paljastaa erittäin arkaluonteisia tietoja ihmisten elämästä. Tietomurrot ja tietosuojaloukkaukset voivat taloudellisten vaikutusten lisäksi aiheuttaa myös syvää inhimillistä kärsimystä, jonka merkitystä yhteiskunnallisena ja oikeudellisena epäkohtana ei pidä väheksyä. Julkisen vallan tehtävänä on perustuslain nojalla turvata kansalaisten yksityiselämän suoja ja muut perusoikeudet. Yksin viranomaistoimilla riittävää turvallisuustasoa ei kuitenkaan ole mahdollista saavuttaa, vaan tietoturvan ja tietosuojan merkitys on tunnistettava kaikkialla yhteiskunnassa ja myös yksityisen sektorin toimijoiden on sitouduttava siihen.

Vastaamon tietomurtotapaukseen liittyvien näkökohtien selvittäminen on osoittanut, että Suomessa on tietojärjestelmiä, joiden tietoturvan ja tietosuojan taso ei ole riittävällä tasolla siten kuin EU:n tietosuojalainsäädäntö ja toimialan erityislainsäädäntö edellyttävät. Osa näistä järjestelmistä on yhteiskunnan toiminnan kannalta kriittisillä toimialoilla. Lähtöoletuksena voidaan pitää, että tällaisia tietojärjestelmiä koskevaa sääntelyä ja valvontaa on vahvistettava. Tuloksekas toiminnan kehittäminen

edellyttää sääntelyn, ohjeistuksen ja valvonnan rinnalla, että taloudelliset voimavarat suunnataan tehokkaasti niin julkisella sektorilla kuin elinkeinoelämässä. Viime kädessä yritykset ja viranomaiset kuitenkin vastaavat omien palveluidensa, tuotteidensa ja tietojärjestelmiensä tietoturvan ja tietosuojan tasosta.

Tietosuojan osalta on keskeistä huomata, että tietoturva on vain yksi keino suojata henkilötietoja. Tietoturvan lisäksi henkilötietoja suojataan esimerkiksi minimoimalla käsiteltävien henkilötietojen määrä vain välttämättömään tai käsittelemällä tiedot siten, etteivät ne ole suoraan yhdistettävissä yksittäiseen henkilöön. Tässä periaatepäätöksessä tietosuojaa on käsitelty pääasiassa tietoturvan näkökulmasta. Tämä ei kuitenkaan vähennä muiden henkilötietojen käsittelyä ohjaavien periaatteiden ja säännösten merkitystä kansalaisten tietosuojan ja tiedollisen itsemääräämisoikeuden turvaamisessa. Periaatepäätöksessä käytettyjen termien osalta on syytä huomata, että periaatepäätöksessä käytetään synonyymeina termejä kyberturvallisuus ja tietoturvallisuus.

Periaatepäätöksen linjaukset pohjautuvat Liikenne- ja viestintäministeriön johtaman poikkihallinnollisen työryhmän selvitykseen, joka julkaistiin 1.2.2021[1]. Suomessa kybertuvallisuuden kehittämistä on tarkasteltu laajasti vuonna 2019 valmistuneessa Suomen kyberturvallisuusstrategiassa ja sen toimeenpano-ohjelmassa, joka valmistuu keväällä 2021[2]. Kyberturvallisuusstrategian toimeenpanossa keskitytään erityisesti pitkän aikavälin toimiin kyberturvallisuuden kehittämiseksi, kuten osaamisen- ja tietoturvakulttuurin parantamiseen. Tästä syystä vastaavia, esimerkiksi kansainväliseen yhteistyöhön, osaamiseen tai harjoitustoimintaan kohdistuvia, pitkän aikavälin toimenpiteitä ei ole tarkasteltu tässä periaatepäätöksessä. Toimenpide-ohjelman ja tämän periaatepäätöksen toimenpiteiden on tarkoitus muodostaa yhdenmukainen ja toisiaan tukeva kokonaisuus, joilla tietoturvan ja tietosuojan toteutumiseen liittyviin haasteisiin pystytään puuttumaan sekä pitkällä että lyhyellä aikavälillä. Tavoitteena on yhteiskunta, jossa on maailman luotettavimmat ja turvallisimmat digitaaliset palvelut kaikille yhteiskunnan toimijoille.

2. Poliittiset linjaukset

2.1. Viranomaiset toimivat yhdessä, Kyberturvallisuuskeskus tukee ja vahvistaa viranomaisia

1. Viranomaisten väliselle yhteistyölle tietoturvaloukkaustilanteissa luodaan yhtenäinen säädöspohja. Laki viranomaisten yhteistoiminnasta tietoturvaloukkausten ehkäisemisessä ja selvittämisessä sisältäisi säännökset yhteistyöryhmän perustamisesta tietoturvaloukkaustilanteissa, viranomaisten välisestä ennakoivasta ja tapahtumakohtaisesta keskinäisestä tiedonvaihdosta sekä välineistön, tilojen ja henkilöstön tilapäisestä luovuttamista toisen viranomaisen käyttöön. Säädöspoh-

[1] Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla : Työryhmän loppuraportti (LVM:n julkaisuja 1/2021), http://urn.fi/URN:ISBN:978-952-243-614-6

[2] https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia-2019/.

jan valmistelussa arvioidaan lisäksi nykyisten toimivaksi todettujen yhteistyömenettelyjen vahvistamista ja yhteistyötä yksityisen sektorin kanssa. Viranomaisille taataan riittävät resurssit yhteistoimintaan.

Vastuutaho: LVM, muut yhteistyöviranomaisten hallinnonalat

Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

2. Varmistetaan valtion budjetista riittävät viranomaisvalvonnan resurssit tämän raportin linjausten toteuttamiseen.

   Vastuutaho: LVM, VM, STM, TEM, OM, MMM, SM

   Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa

3. Lisätään liikenne- ja viestintäministeriön resursseja vastaamaan kyberturvallisuuden kasvavaa työmäärää ja painoarvoa yhteiskunnassa.

   Vastuutaho: LVM

   Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa

4. Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen resursseja vahvistetaan, jotta se pystyy tukemaan ja antamaan toimialakohtaista neuvontaa muille hallinnonaloille. Kyberturvallisuuskeskukseen perustetaan jokaiselle kriittiselle toimialle oma asiantuntijapalvelu, joiden vastuuvirkamiehet tukevat päätoimisesti tietyn yksittäisen toimialan tietoturvasta vastaavaa sektoriviranomaista.

   Vastuutaho: LVM, Liikenne- ja viestintävirasto, NIS-sektoriviranomaiset

   Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

5. Liikenne- ja viestintäviraston Kyberturvallisuuskeskus tarjoaa koulutusta NIS-sektoreiden tietoturvaa valvoville viranomaisille. Työnantajavirastot sitoutuvat siihen, että Kyberturvallisuuskeskuksen koulutus tai muu vastaava tietoturvakoulutus on tietoturvavalvonnan parissa työskenteleville virkamiehille pakollinen. Työnantajavirastojen tulee kyetä esittämään koulutuksen perusteella, että tietoturvavalvonnan parissa työskentelevien asiantuntijoiden tietotaito on riittävällä tasolla.

   Vastuutaho: Liikenne- ja viestintävirasto, NIS-sektoriviranomaiset

   Toimenpiteen kiireellisyys: Kiireellisyysluokka 2 (toteutettava 2-4 vuoden kuluessa)

6. Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen tarjoama tietoturvallisuuden kartoituspalvelu mahdollistetaan kaikille kriittisille toimialoille. Palvelun

avulla on mahdollista löytää ja korjata ulkoverkon tietoturvahaavoittuvuuksia. Tehdään tarvittavat lainsäädäntömuutokset. Varmistetaan, että kriittisten toimialojen viranomaisilla on riittävä osaaminen kartoituspalvelujen tulosten tulkitsemiseksi.

Vastuutaho: LVM, Liikenne- ja viestintävirasto

Toimenpiteen kiireellisyys: Kiireellisyysluokka 2 (toteutettava 2-4 vuoden kuluessa)

7. Selvitetään viranomaisten tarpeet teknologisille ratkaisuille salassa pidettävän ja turvaluokitellun tiedon käsittely-ympäristöjen luomiseen. Selvityksen kohteena ovat muun muassa viranomaisten yhdenmukainen salattu sähköpostiviestintä, turvalliset neuvotteluyhteydet ja -palvelut sekä turvallinen tiedonsiirtopalvelu. Selvitys tehdään vuonna 2021 ja selvityksen pohjalta haetaan ja toteutetaan nykyaikaiset ratkaisut vuosina 2022-2023. Selvityksessä arvioidaan myös tiedonvaihdon yhteentoimivuutta kolmansien tahojen kanssa.

   Vastuutaho: VM

   Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

8. Varmistetaan, että tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä Havaro on laajasti kriittisten toimialojen käytettävissä. Tehdään tarvittavat lainsäädäntömuutokset, jotka mahdollistavat Havaro-palvelun tarjoamisen nykyistä laajemmalle joukolle.

   Vastuutaho: LVM ja Liikenne- ja viestintävirasto

   Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

2.2. Kaikilla kriittisillä toimialoilla on lakisääteiset tietoturvavaatimukset

9. Kriittisille toimialoille määritellään selkeät ja oikeasuhtaiset tietoturvavaatimukset lainsäädännössä. Määrittely tehdään riskiperusteisesti. Viranomaisilla on oltava laissa riittävät valtuudet antaa tietoturvaa koskevia sitovia määräyksiä kriittisille toimialoille. Olemassa olevat määräykset käydään läpi ja varmistetaan, että ne ovat ajan tasalla. Tietoturvavaatimusten valmistelussa huomioidaan kansainvälinen lainsäädäntö ja sen asettamat rajoitteet ja vaatimukset.

   Vastuutaho: LVM, TEM, MMM, STM, VM,

   Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

10. Tietoturvavaatimusten laatimisesta vastaaville viranomaisille säädetään velvoite pyytää Liikenne- ja viestintäviraston Kyberturvallisuuskeskukselta lausunto tietoturvaa koskevista vaatimuksista ennen niiden hyväksymistä ja tarvittaessa myös vaatimusten toimeenpanosta.

    Vastuutaho: LVM, TEM, MMM, STM, VM

    Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

11. Liikenne- ja viestintäviraston Kyberturvallisuuskeskus, Tiedonhallintalautakunta sekä Tietosuojavaltuutettu laativat ennakollisen ohjeen yleisistä tietoturvavaatimuksissa huomioitavista asioista.

    Vastuutaho: Liikenne- ja viestintävirasto, Tiedonhallintalautakunta, Tietosuojavaltuutetun toimisto

    Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

2.3. Kriittisten toimintojen ja järjestelmien vaatimustenmukaisuutta arvioidaan säännöllisesti

12. Kriittisille toimialoille säädetään velvoite määritellä kriittiset tieto- ja tietoliikennetekniset prosessit ja toiminnot. Määrittelyssä huomioidaan erityisesti prosesseissa ja toiminnoissa käsiteltävien tietojen ja tietoaineistojen sekä käytettävien tietojärjestelmien kriittisyys sekä prosessien ja toimintojen merkitys yhteiskunnan keskeisille toiminnoille ja arkaluontoisille henkilötiedoille. Kriittisyyden määrittelyn reunaehdot määritellään lainsäädännössä. Määrittelyssä huomioidaan myös EU:ssa tehtävä työ kriittisten toimintojen ja infrastruktuurin tunnistamiseksi. Määrittelyssä huomioidaan taloudelliset vaikutukset.

    Vastuutaho: LVM, TEM, MMM, STM, VM

    Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

13. Kriittisille toimialoille säädetään velvoite säännöllisesti auditoida kriittiset tieto- ja tietoliikennetekniset prosessit ja toiminnot. Auditointimalli määräytyy laissa riskiperusteisesti sen mukaan, kuinka kriittistä tietoa sisältävästä järjestelmästä tai prosessista tai toiminta ohjaavasta on kyse. Auditointimallissa voidaan ottaa huomioon toimialakohtaisia erityispiirteitä. Määrittelyssä huomioidaan taloudelliset vaikutukset ja toimenpiteiden oikeasuhtaisuuseri kokoisten toimijoiden osalta.

    Vastuutaho: LVM, TEM, MMM, STM, VM

    Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

14. Kriittisten toimialojen suurimpien ja yhteiskunnan keskeisten toimintojen kannalta merkittävimpien toimijoiden tulee osoittaa käyttävänsä tietoturvallisuuden hallintajärjestelmää ISO 27001 –sertifioinnilla tai sitä vastaavalla yleiseen tietoturvastandardiin perustuvalla sertifioinnilla vuoden 2025 loppuun mennessä. Kyseessä olevat toimijat määritellään sektorikohtaisesti toimenpiteen täytäntöönpanovaiheessa.

    Vastuutaho: NIS-direktiivissä määritellyt toimialat

    Toimenpiteen kiireellisyys: Kiireellisyysluokka 2 (toteutus aloitettava 2-4 vuoden kuluessa)

15. Tietoturvallisuuden arviointilaitosten määrää lisätään tehostamalla arviointilaitosten hyväksymismenettelyä ja valmistelemalla tämän mahdollistavat lakimuutokset. Lakimuutoksien yhteydessä varmistetaan, että arviointilaitoksien toiminnan korkea laatu ja ammattitaito säilyvät.

    Vastuutaho: VM

    Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

2.4. Kriittisten toimialojen erityispiirteet tunnistetaan ja huomioidaan

16. Säädetään tietoturva täsmällisemmin osaksi sähköverkkoyhtiöiden varautumisvelvoitetta ja varautumissuunnitelmaa.

    Vastuutaho: TEM

    Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

17. Varmistetaan ydinvoimaloiden tietoturvallisuusvaatimuksia koskevan ohjeistuksen velvoittavuus.

    Vastuutaho: TEM ja Säteilyturvakeskus (STUK)

    Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

18. Varmistetaan, että tietoturvallisuus on otettu huomioon vesihuoltolaitosten suunnitelmissa häiriötilanteisiin varautumiseksi. Laaditaan vesihuoltolaitoksia koskevia tietoturvaohjeistuksia ja varmistetaan, että vesihuoltolaitokset noudattavat niitä toiminnassaan.

Vastuutaho: MMM

Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

19. Tehdään lainsäädäntömuutokset, joilla varmistetaan, että Liikenne- ja viestintävirastolla on mahdollisuus antaa määräyksiä kaikkien liikennemuotojen tietoturvasta.

    Vastuutaho: LVM

    Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

20. Tietoverkkorikoksiin liittyen poliisin toimivaltuuksia selvitetään pakkokeinolainsäädännön tarkastelutarpeita koskevassa työryhmässä kysymyksen eri näkökannat huolellisesti punniten.

    Vastuutaho: OM:n työryhmä

    Toimenpiteen kiireellisyys: Työryhmälle annetussa aikataulussa

21. Lisätään poliisin tietoverkkorikostorjunnan resursseja, jotta se voi tehokkaasti ennalta estää, selvittää ja tutkia kriittisiin toimialoihin kohdistuvia tietoverkkorikoksia.

    Vastuutaho: SM

    Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

22. Valvovat viranomaiset ohjeistavat toimijoita tekemään tietoturvaloukkauksista rikosilmoituksen poliisille aina, kun epäilevät, että kyseessä on rikos.

    Vastuutaho: NIS-sektoriviranomaiset

    Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

23. Vaikutetaan NIS-direktiivin uudelleenarviointityössä EU:ssa, jotta tulevassa sääntelyssä otetaan huomioon Suomen kannalta keskeiset toimijat.

    Vastuutaho: LVM

    Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

2.5. Julkisen sektorin merkitys kriittisenä toimialana tunnistetaan ja huomioidaan

24. Valtion tieto- ja viestintätekniikkakeskus (Valtori) auditoi järjestelmänsä ja prosessinsa valtiovarainministeriön marraskuussa 2020 antaman ohjauksen mukaisesti[3]. Lisäksi Valtorin on vuoden 2021 loppuun mennessä varmistettava, että tietosuojaa koskevat vaikutusarvioinnit on yleisen tietosuoja-asetuksen mukaisesti tehty siltä osin, kun käsittely todennäköisesti aiheuttaa korkean riskin ihmisten oikeuksille ja vapauksille.

    Vastuutaho: Valtori ja VM

    Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

25. Arvioidaan valtion yhteisten tieto- ja viestintäteknisten palveluiden tuottajien tietosuojaa ja tietoturvaa koskevia vastuita ja velvoitteita. Lähtökohtana on, että yhteisille kriittisille palveluille asetetaan palvelukohtaisesti turvallisuus, tietosuoja sekä toimintavarmuusvaatimukset ja palvelujen vaatimuksenmukaisuus arvioidaan hyväksytyn arviointityökalun kriteerien mukaisesti arviointityökalun määräytyessä kunkin palvelun luonteen perusteella (esim. Tiedonhallintalaissa (906/2019) säädetyt vaatimukset, ISO 27001, Katakri TL IV –tason vaatimukset)

    Vastuutaho: VM

    Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

26. Arvioidaan Valtorin tietoturvan ja tietosuojan vaatimia resursseja ja arvioinnin pohjalta tehdään tarvittavat resursoinnit. Resurssit tulee kohdistaa nimenomaisesti tietoturva- ja tietosuojaosaamiseen.

    Vastuutaho: VM, Valtori

    Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

27. Varmistetaan Tiedonhallintalautakunnan vuoden 2020 suositusten toimeenpano hyödyntämällä Haukka-hankkeessa vuonna 2021 laadittavaa Julkri-kriteeristöä, jota julkisen sektorin toimijat käyttävät pilvipalveluiden tietoturvallisuusvaatimusten määrittämisessä sekä pilvipalveluntarjoajien ja pilvipalveluihin perustuvien valmistuotteiden tietoturvallisuudentason arvioimisessa hankintoja tehdessään.

    Vastuutaho: VM, Liikenne- ja viestintävirasto, Digi- ja väestötietovirasto

[3] Valtiovarainministeriön ohjauskirje Valtorille 20.11.2020, VN/1411/2020

Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

28. Selvitetään, miten tietoturvaan ja tietosuojaan liittyvää osaamista voidaan vahvistaa julkisissa hankinnoissa esimerkiksi yhteishankintayhtiö Hansel Oy:n kautta.

    Vastuutaho: VM

    Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

29. Selvitetään Suomen 15 suurimman kunnan tietoturvan ja tietosuojan taso terveydenhuollossa, sosiaalihuollossa, energiahuollossa ja vesihuollossa. Selvityksessä hyödynnetään toimenpiteessä 4 mainittua Kyberturvallisuuskeskuksen tarjoamaan tietoturvallisuuden kartoituspalvelua.

    Vastuutaho: VM, Liikenne- ja viestintävirasto

    Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

2.6. Tietosuojasääntelyllä pystytään tehokkaasti puuttumaan oikeudenloukkauksiin

30. Selvitetään kriittisten toimialojen tietosuojaa koskeva kyvykkyystaso samaan tapaan kuin kyberturvallisuudessa.

    Vastuutaho: Tietosuojavaltuutetun toimisto, Huoltovarmuuskeskus (siltä osin kun kytkös huoltovarmuuteen)

    Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

31. Kriittisten toimialojen rekisterinpitäjien on varmistettava vuoden 2021 loppuun mennessä, että tietosuojaa koskevat vaikutusarvioinnit on yleisen tietosuoja-asetuksen mukaisesti tehty siltä osin, kun käsittely todennäköisesti aiheuttaa korkean riskin ihmisten oikeuksille ja vapauksille.

    Vastuutaho: Kriittisten toimialojen rekisterinpitäjät, Tietosuojavaltuutetun toimisto

    Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

32. Tietosuojan sertifiointielinten toiminta käynnistetään tehostamalla sertifiointielinten hyväksymismenettelyä.

Vastuutaho: Tietosuojavaltuutetun toimisto

Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

33. Sertifiointielimet luovat kriteerit tietosuojasertifioinnille ja tuovat ne tietosuojavaltuutetulle hyväksyttäväksi. Työssä huomioidaan olemassa olevat kansainväliset standardit. Arvioidaan mahdollisuudet hyväksyä kriittisiä toimialoja valvovien viranomaisten tietoturvamääräykset tai olemassa olevat tietoturvan arviointikriteerit yleisen tietosuoja-asetuksen mukaisiksi sertifiointikriteereiksi.

    Vastuutaho: Tietosuojavaltuutetun toimisto

    Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

34. Kannustetaan laajasti erityisiin henkilötietoryhmiin kuuluvia tai valtiosääntöoikeudellisesti arkaluonteisia tietoja käsitteleviä kriittisten toimialojen rekisterinpitäjiä osoittamaan keskeisen toimintansa tietosuojasääntelyn mukaisuus tietosuojasertifioinneilla.

    Vastuutaho: Tietosuojavaltuutetun toimisto

    Toimenpiteen kiireellisyys: Kiireellisyysluokka 2 (toteutettava 2-4 vuoden kuluessa)

35. Varmistetaan Tietosuojavaltuutetun toimistolla riittävät resurssit valvoa sektoreita tehokkaasti ja puuttua henkilötietojen tietoturvaloukkauksiin. Lisäksi Tietosuojavaltuutetun ratkaisukäytäntöä pyritään saattamaan nykyistä paremmin saataville.

    Vastuutaho: OM, Tietosuojavaltuutetun toimisto

    Toimenpiteen kiireellisyys: Kiireellisyysluokka 1 (toteutettava 1-2 vuoden kuluessa)

36. Seurataan tietosuojalain mukaisen seuraamusjärjestelmän soveltamista ja toimivuutta.

    Vastuutaho: OM

    Toimenpiteen kiireellisyys: Kiireellisyysluokka 2 (toteutettava 2-4 vuoden kuluessa)

2.7. Etsitään uusia toimintapoja tietoturvauhkista ja -loukkauksista viestimiseksi ja ilmoittamiseksi

37. Kehitetään yksityishenkilöille ja organisaatioiden edustajille palvelu (esimerkiksi mobiilipäätelaitteeseen asennettava sovellus), jonka kautta on mahdollista saada kohdennetusti ajankohtaista tietoa tietoturvauhkista ja -loukkauksista ja tietoturvallisuutta koskevista ohjeista sekä ilmoittaa tietoturvauhkista ja -loukkauksista Kyberturvallisuuskeskukselle, kriittisen toimialan valvovalle viranomaiselle ja/tai poliisille. Lisäksi palvelun avulla voisi ilmoittaa henkilötietojen tietoturvaloukkauksesta Tietosuojavaltuutetun toimistolle. Palvelu (sovellus ja palveluun liittyvät järjestelmät) toteutetaan turvallisen ohjelmistokehityksen sekä hyvän tietoturvan ja -suojan periaatteita noudattaen.

    Vastuutaho: Liikenne- ja viestintävirasto

    Toimenpiteen kiireellisyys: Kiireellisyysluokka 2 (toteutettava 2-4 vuoden kuluessa)

3. Tavoitteet ja keinot

Tietoturvan ja tietosuojan tasoa on kehitettävä kaikilla yhteiskunnan kriittisillä sektoreilla. Lisäksi sektoreiden välisiä osaamis- ja kyvykkyyseroja on kavennettava. Digitaalinen yhteiskunta koostuu suuresta joukosta toisistaan riippuvaisia toimijoita. Esimerkiksi useat kriittiset toimialat tarvitsevat energiahuoltoa tai viestintäverkkoja oman sektorinsa perustoimintoihin. Yhteiskunnan toiminnan jatkuvuuden kannalta on välttämätöntä varmistaa kaikkien keskeisten toimialojen toimintaedellytykset myös erilaisten häiriöiden varalta. Kriittisten toimintojen osalta yksikään toimiala ei voi olla heikko lenkki.

Riittävästä tietoturvasta ja tietosuojasta huolehtimisella vahvistetaan myös kansalaisten luottamusta digitaaliseen yhteiskuntaan. Ihmisten tietojen siirtyessä yhä enenevässä määrin digitaaliseen muotoon on kansalaisten kyettävä luottamaan siihen, että tietoja käsitellään asianmukaisesti ja ne ovat turvassa tietomurroilta ja muilta oikeudenloukkauksilta. Ilman luottamusta yhteiskunnan digitaaliset palvelut eivät kehity ja digitalisaation hyödyt menetetään.

Tavoitteisiin pääsemiseksi tarvitaan toimenpiteitä, joilla saadaan aikaan sektorirajat ylittäviä vaikutuksia. Tällaisia toimenpiteitä ovat esimerkiksi viranomaisten välisen yhteistyön ja yhteisen tilannekuvan kehittäminen, joka vaatii sekä lainsäädännön vahvistamista että riittävää resursointia. Tietoturva- ja tietosuojaloukkausten ehkäisemiseksi ja selvittämiseksi viranomaisille tulisi säätää nykyistä vakiintuneemmat yhteistyörakenteet. Yhteistyön osalta korostuu myös viranomaisten yhteistyö yksityisen sektorin toimijoiden kanssa. Lisäksi Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen tarjoamat asiantuntija- ja tietoturvapalvelut on saatava entistä laajemmin kaikkien kriittisten toimialojen käyttöön.

Toiminnan kehittäminen ja sektoreiden välisten erojen kaventamien vaatii kattavaa sääntelyä ja sen tehokasta valvontaa. Lainsäädännössä on oltava riittävät tietoturvaa ja tietosuojaa koskevat vaatimukset ja määräyksenantovaltuudet, joita voidaan täydentää velvoittavilla alemman asteen mää-

räyksillä. Aikaisempien selvitysten mukaan sääntelyllä on ollut positiivinen vaikutus tietoturvan toteutukseen.[4] Lainsäädännön tasolla korostuu lisäksi vähimmäisvaatimusten määritys. Eri sektoreilla tarkemmat tietoturvavaatimukset asetetaan tyypillisesti määräyksissä tai ohjeistuksissa. Riittävän tietoturvallisuuden ja tietosuojan tason varmistamiseksi vaatimusten tulisi perustua velvoittaviin määräyksiin.

Sääntelyn vahvistamien ei yksin riitä, vaan myös sääntelyn toimeenpanoon ja valvontaan sekä toimijoiden ohjaamiseen ja neuvontaan tarvitaan riittävät resurssit. Tällä hetkellä useilla yhteiskunnan kriittisillä toimialoilla tietoturvaan ja tietosuojaan osoitetut resurssit ovat riittämättömiä. Resurssien riittämättömyys koskee myös toimialakohtaista viranomaisvalvontaa, eikä viranomaisilla ole edes mahdollisuutta käyttää lainsäädännössä annettuja toimivaltuuksia. Toiminnan kehittäminen ja resurssien kohdentaminen tietoturvan ja tietosuojan kehittämiseen edellyttää uskallusta johtotasolta.

Vaikka tehokkaalla viranomaisvalvonnalla voidaan katsoa olevan merkittävä vaikutus tietoturvan ja tietosuojan parantamiseen yhteiskunnassa, ensisijainen vastuu tietoturvan ja tietosuojan toteutumisesta on jokaisella toimijalla itsellään. Mikään määrä valvontaa ei yksin riitä tekemään yhteiskunnasta ja sen kriittisisät toiminnoista turvallisia. Tietoturvan ja tietosuojan on jo lähtökohtaisesti oltava sisäänrakennettuna kriittisten toimialojen toimintakulttuuriin ja toimijoiden on itse kannettava siitä vastuu.

Yhteenvetona voidaan todeta, että tietoturvan ja tietosuojan parantaminen kriittisillä toimialoilla vaatii, että:

1. Lainsäädännössä on riittävät tietoturva- ja tietosuojavaatimukset ja –velvoitteet, joita toimialoilla noudatetaan, sekä säännökset antaa tarkempia määräyksiä tietoturvan ja tietosuojan toteuttamisesta.
2. Toimijoilla on riittävä tietämys ja osaaminen velvoitteiden noudattamisessa.
3. Viranomaisilla on riittävät toimivaltuudet valvoa tietoturvan ja tietosuojan toteutumista ja tehdä sektorirajat ylittävää yhteistyötä.
4. Viranomaisilla on riittävä osaaminen ja uskallus käyttää niille lainsäädännössä annettua toimivaltaa ja ohjata toimialaansa.
5. Viranomaisilla on riittävät tosiasialliset aineelliset ja henkilöresurssit käyttää toimivaltaansa.
6. Jokainen toimija kantaa itse vastuun oman toimintansa tietoturvasta ja tietosuojasta.
7. Pidetään yllä yhteistä tietoturvaa ja tietosuojaa koskevan toimintaympäristön tilannekuvaa ml. säännöllisellä koordinaatiolla, tiedonvaihdolla ja tilannekatsauksilla.

[4] Huoltovarmuuskeskuksen raportti kyberturvallisuuden nykytilasta eri toimialoilla: https://cdn.huoltovarmuuskeskus.fi/app/uploads/2020/10/05091400/Kyberturvallisuuden-nykytila-eri-toimialoilla.pdf

4. Nykytilan arviointi

Periaatepäätöksen linjausten taustalla olevaa nykytilaa on tarkasteltu kattavasti tietoturvan ja tietosuojan parantamista yhteiskunnan kriittisillä toimialoilla selvittäneen poikkihallinnollisen työryhmän loppuraportissa[5]. Nykytilan osalta keskeiset havainnot on tiivistetty alla:

1. Suomessa vastuu tietoturvan ja tietosuojan viranomaisvalvonnasta on jakautunut useiden viranomaisten kesken. Tietoturvan osalta kriittisten toimialojen sektoriviranomaiset vastaavat muun valvonnan ohella myös oman sektorinsa tietoturvan valvonnasta. Tietosuojalainsäädännön ja muiden henkilötietojen käsittelyä koskevien lakien noudattamista valvoo Tietosuojavaltuutetun toimisto. Rikosten selvittämisestä vastaa poliisi.

2. Liikenne- ja viestintäviraston Kyberturvallisuuskeskus tukee suoraan yhteiskunnan eri sektoreiden toimijoita omien sektorikohtaisten valvontatehtäviensä lisäksi. Eri toimialojen riittävä tukeminen vaatii Kyberturvallisuuskeskukselta riittävää ymmärrystä niiden toiminnasta ja toimintaympäristöstä. Toimintaa on resursoitava riittävästi, jotta mahdollistetaan tilannekuvan jatkuva tuottaminen ja analysointi kunkin toimialan tarpeet huomioiden. Nykyresursoinnilla Kyberturvallisuuskeskus ei pysty tarjoamaan riittäviä palveluita kaikille yhteiskunnan kriittisille toimialoille.

3. Viranomaisten keskinäisen yhteistyön lähtökohtana on, että tietoturvallisuudesta huolehtivien viranomaisten on oltava yhteistyössä, silloin kun niiden tehtävät sitä edellyttävät. Myös NIS-direktiivi edellyttää, että tietoturvallisuudesta vastaavat viranomaiset tekevät tarvittavaa yhteistyötä direktiivin mukaisten velvoitteiden valvomiseksi. NIS-direktiivin ulkopuolella viranomaisyhteistyö ilmenee esimerkiksi rikosten selvittämistä koskevassa yhteistyössä. Psykoterapiakeskus Vastaamon tapauksessa toimivaltaisia viranomaisia olivat poliisin lisäksi ainakin Valvira, aluehallintovirastot, tietosuojavaltuutettu ja Liikenne- ja viestintävirasto.

4. Viranomaisten välisestä yhteistyöstä on säädettävä lailla aina, jos kyse on virka-avusta, jolla puututaan yksittäisen oikeussubjektin perustuslailla suojattuihin oikeuksiin tai kyse on perustuslaissa tarkoitetusta julkisen vallan käytöstä. Myös viranomaisyhteistyöhön liittyvä tietojen vaihto saattaa edellyttää laintasoista sääntelyä. Jos viranomaisyhteistyötä varten perustetaan päätösvaltaa käyttävä yhteistyöelin, on tästäkin säädettävä laissa. Lisäksi viranomaisyhteistyöstä voi olla tarkoituksenmukaista säätää, vaikka se ei olisi oikeudellisesti välttämätöntä. Erityiset lain tasoiset säännökset yhteistyöstä korostavat yhteistyön merkitystä siihen osallistuville viranomaisille ja saattavat ohjata sen järjestäytyneisiin muotoihin. Viranomaisten välisen yhteistyön tehostamista on pidetty keskeisenä keinona tietoturvan ja tietosuojan parantamiseksi.

[5] Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla : Työryhmän loppuraportti (LVM:n julkaisuja 1/2021), http://urn.fi/URN:ISBN:978-952-243-614-6

5. Yhteiskunnan kriittisten toimialojen välillä on merkittäviä eroja sen suhteen, kuinka tarkkoja tietoturva- ja tietosuojavaatimuksia on säädetty lain nojalla. Sekä tietoturvaa valvovat viranomaiset että tietoturva-arviointeja tekevät toimijat ovat tuoneet esille tarpeen nykyistä yksityiskohtaisemmille tietoturvavaatimuksille. Etenkin energia-, liikenne- ja vesihuoltosektorilla lain nojalla annettuja vaatimuksia on vähän tai ei lainkaan. Laissa ei myöskään kaikissa tapauksessa ole valtuutusta antaa alemman aseista sääntelyä tai vaihtoehtoisesti valtuutusta ei ole käytetty. Vastaava tilanne on julkisen sektorin tiedonhallinnassa erityisesti alemman asteisen sääntelyn osalta.

6. Vain osa yhteiskunnan kriittisen toimialan toimijoista tilaa auditointipalveluja tai omaa tietoturvaa koskevia sertifikaatteja. Auditointien vähäinen käyttöaste osalla toimialoista on vaikuttanut siihen, että prosessien, toimintojen ja tietojärjestelmien tietoturvallisuuden taso voi vaihdella merkittävästi eri toimialoilla. Prosessien ja toimintojen auditoinnin pitäisi olla luonnollinen osa kriittisten toimialojen riskinhallintaa.

5. Lisäresurssitarpeet

Periaatepäätöksen valmistelun yhteydessä on arvioitu konkreettiset lisäresurssitarpeet kultakin hallinnonalalta sektoriviranomaisten tehokkaan tietoturvavalvonnan mahdollistamiseksi. Arviossa on hyödynnetty poikkihallinnollisen työryhmän aikaisempia arvioita tarvittavista lisäresurssitarpeista. Tarkasteltavia toimialoja ovat olleet NIS-direktiivin mukaisesti erityisesti terveydenhuolto, rahoitusmarkkinat, energiahuolto, vesihuolto, liikenne ja digitaalinen infrastruktuuri, sekä viestintäverkot. Tarkasteltavana ovat olleet myös valtion ja kuntien merkittävät tietojärjestelmät, joiden osalta lisäresurssiarvioita on tarkasteltu erityisesti valtion järjestelmien osalta. Lisäksi tarkastelussa ovat olleet poliisin resurssit erityisesti tietoverkkorikosten torjunnan näkökulmasta. Turvallisuusviranomaisten verkkoja ja järjestelmiä ei ole tarkasteltu tämän työryhmän työn puitteissa, koska katsottiin, että tällaisia erittäin turvallisuuskriittisiä toimintoja on tarkoituksenmukaista tarkastella erikseen.

Periaatepäätöksen valmistelun aikana tehdyn arvion mukaan mainituilla toimialoilla tarvitaan yhteensä 115 henkilötyövuotta lisää viranomaistoiminnoissa, jotta periaatepäätöksen linjaukset voitaisiin toteuttaa ja tietoturvan sekä tietosuojan valvonnan, ohjauksen ja neuvonnan tasoa voitaisiin kehittää tarvittavalle tasolle. Arvio sisältää myös liikenne- ja viestintäministeriölle esitetyn 6 henkilötyövuoden lisäyksen, jolla varmistetaan resurssien riittävyys vastaamaan kyberturvallisuuden kasvavaan työmäärään ja painoarvoon yhteiskunnassa. Henkilötyövuosien lisäys kustantaisi arvion mukaan yhteensä noin 10,5 miljoonaa euroa vuodessa.

Sekä linjaukset että niihin kohdistetut resurssit on tarkoitettu toisiaan tukeviksi ja niitä tulisi tarkastella kokonaisuutena. Tämä tarkoittaa sitä, että yksittäisen toimenpiteen tehokkuus on usein riippuvainen muiden ehdotettujen toimenpiteiden toteutumisesta.

Linjauksien resurssitarpeet katetaan valtiontalouden kehyksen puitteissa ja mahdollisia määrärahatarpeita arvioidaan tarvittaessa tarkemmin vuosien 2022-2025 julkisen talouden suunnitelman yhteydessä

6. Seuranta ja raportointi

Liikenne- ja viestintäministeriö vastaa periaatepäätöksen linjaustentoteuttamisen seurannasta yhteistyössä toimenpiteissä mainittujen toimijoiden kanssa. Linjauksissa vastuutetut tahot raportoivat toimenpiteen edistymisestä liikenne- ja viestintäministeriölle. Jokaiselle linjaukselle on määritelty kiireellisyysluokka, joka määrittää toimenpiteen toteuttamisaikataulun.