VALTIONEUVOSTO
STATSRÅDET

Muistio
Asianumero: VN/3501/2021
Päivämäärä: 10.6.2021

Valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla

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 on tärkeää tehdä aktiivisesti toimia tietoturvallisuuden ja tietosuojanparantamiseksi ja tunnistaa turvallisuuskokonaisuuden merkitys palveluiden laadulle ja turvallisuudelle 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.

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 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. Julki-

sen 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, tietosuojan ja valvonnan taso ei ole riittävällä tasolla siten kuin EU:n tietosuojalainsäädäntö ja toimialan erityislainsäädäntö edellyttävät. Osa näistä järjestelmistä on yhteiskunnan toiminnan kannalta kriittisillä toimialoilla. Myöskään näiden järjestelmien valvonta ei ole ollut ajan tasalla ja siksi 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. Valtion tehtävänä on vastata riittävästä tietoturvallisuuden valvonnasta.

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.

Pääasiallinen sisältö

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 määräyksillä. Aikaisempien selvitysten mukaan sääntelyllä on ollut positiivinen vaikutus tietoturvan toteutukseen.[1] 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.

8. Käynnistetään toimet kansalaisten digiturvaosaamisen vahvistamiseksi eri toimijoiden laajana yhteistyönä.

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

Nykytilan arviointi

Periaatepäätöksen linjausten taustalla olevaa nykytilaa on tarkasteltu kattavasti tietoturvan ja tietosuojan parantamista yhteiskunnan kriittisillä toimialoilla selvittäneen poikkihallinnollisen työryhmän loppuraportissa[2]. 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. 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,

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

toimintojen ja tietojärjestelmien tietoturvallisuuden taso voi vaihdella merkittävästi eri toimialoilla. Prosessien ja toimintojen auditoinnin pitäisi olla luonnollinen osa kriittisten toimialojen riskinhallintaa.

Keskeisimmät linjaukset

Periaatepäätöksen linjaukset pohjautuvat liikenne- ja viestintäministeriön johtaman poikkihallinnollisen työryhmän selvitykseen, joka julkaistiin 1.2.2021. Periaatepäätöksessä on esitetty yhteensä 37 poliittista linjausta, joiden toteuttamisen on arvioitu parantavan tietoturvan ja tietosuojan tasoa yhteiskunnan kriittisillä toimialoilla. Linjaukset rakentuvat seuraavien otsikoiden varaan:

1. Viranomaiset toimivat yhdessä, Kyberturvallisuuskeskus tukee ja vahvistaa viranomaisia
2. Kaikilla kriittisillä toimialoilla on lakisääteiset tietoturvavaatimukset
3. Kriittisten toimintojen ja järjestelmien vaatimustenmukaisuutta arvioidaan säännöllisesti
4. Kriittisten toimialojen erityispiirteet tunnistetaan ja huomioidaan
5. Julkisen sektorin merkitys kriittisenä toimialana tunnistetaan ja huomioidaan
6. Tietosuojasääntelyllä pystytään tehokkaasti puuttumaan oikeudenloukkauksiin
7. Etsitään uusia toimintatapoja tietoturvauhkista ja –loukkauksista viestimiseksi ja ilmoittamiseksi

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 oli tarkoitus varmistaa resurssien riittävyys vastaamaan kyberturvallisuuden kasvavaan työmäärään ja painoarvoon yhteiskunnassa. Henkilötyövuosien lisäys kustantaisi arvion mukaan yhteensä noin 10,2 miljoonaa euroa vuodessa. Lisäksi hallinnonaloille on arvioitu syntyvän muun muassa ICT-järjestelmäkustannuksia ja hankintakustannuksia, joiden suuruusluokka voi vaihdella suuresti toteutustavasta ja -ajankohdasta riippuen.

Periaatepäätöksen linjaukset on jaoteltu sen mukaan, tarvitaanko niihin lisärahoitusta valtion budjetista vai pystytäänkö ne hoitamaan pääosin nykyisillä resursseilla. Linjaukset 1, 8, 9, 12, 15, 16, 17, 19, 20, 22, 23, 24, 27, 28, 34 ja 36 pystytään arvion mukaan toteuttamaan nykyisillä resursseilla. Tästä huolimatta näistäkin toimenpiteistä saattaa tulla välillisiä resurssivaikutuksia viranomaisten toimintaan esimerkiksi toteutuneiden lainsäädäntömuutosten myötä. Linjaukset 2, 3, 4, 5, 6, 7, 10, 11, 13, 14,18, 21, 25, 26, 29, 30, 31, 32, 33, 35 ja 37 vaativat lisärahoitusta, eivätkä siten järjesty nykyisten resurssien puitteissa.

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.

Periaatepäätöksen linjauksia toteutetaan valtion budjettiraamien sekä olemassa olevien määrärahojen puitteissa. Esitetyistä lisäresurssitarpeista tai muista budjettivaikutuksia vaativista toimenpiteistä päätetään erikseen valtiontalouden kehyksissä ja vuosittaisissa talousarvioissa. Tässä periaatepäätöksessä esitetyt lisäresurssitarpeet ovat siis ehdollisia ja niitä voidaan toteuttaa vain, jos periaatepäätöksen kohteena olevan tietoturvan ja tietosuojan parantamisen kokonaisrahoitusta lisätään eri hallinnonaloilla budjettivarojen kautta. Tästä on päätettävä ja sovittava erikseen.

Periaatepäätöksen valmisteluprosessi

Periaatepäätöksen linjaukset pohjautuvat Liikenne- ja viestintäministeriön johtaman poikkihallinnollisen työryhmän 9.11.2020-31.1.2021 selvitykseen, joka julkaistiin 1.2.20213. Suomessa kyberturvallisuuden kehittämistä on tarkasteltu laajasti vuonna 2019 valmistuneessa Suomen kyberturvallisuusstrategiassa ja sen toimeenpano-ohjelmassa, joka valmistuu keväällä 20214. 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.

Periaatepäätöksen luonnos oli lausuttavana 2.3.-3.3.2021. Lausuntoja antoi 20 tahoa ja periaatepäätöstä päivitettiin saatujen palautteiden pohjalta. Lyhyt lausuntokierros oli mahdollinen, koska lähes vastaavat linjaukset olivat lausuttavana poikkihallinnollisen työryhmän selvitysluonnoksen yhteydessä 15.12.2020-6.1.2021.

Periaatepäätösluonnos käsitellään raha-asiainvaliokunnassa ennen periaatepäätöksen antamista.

Periaatepäätöksen seuranta ja raportointi

Liikenne- ja viestintäministeriö vastaa periaatepäätöksen linjausten toteuttamisen seurannasta yhteistyössä toimenpiteissä mainittujen toimijoiden kanssa ja lisäksi liikenne- ja viestintäministeriön koordinaatioroolia äkil-

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

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

listen tai poikkeuksellisten tietoturva- ja tietosuojatapausten hoitamisessa vahvistetaan. Linjauksissa vastuutetut tahot raportoivat toimenpiteen edistymisestä liikenne- ja viestintäministeriölle. Jokaiselle linjaukselle on määritelty kiireellisyysluokka, joka määrittää toimenpiteen toteuttamisaikataulun.

Esitys

Edellä olevan perusteella esitetään, että valtioneuvosto tekee periaatepäätöksen tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla.

Esittelijä

Osastopäällikkö, Laura Vilkkonen, liikenne- ja viestintäministeriö