



Mari Starck
Tieto- ja turvallisuusosasto,
Digitaalinen luottamus -yksikkö

Liikenne- ja viestintäministeriön lausunto ehdotuksesta turvallisuustutkintalain ja kyberturvallisuuslain 17 §:n muuttamisesta

Oikeusministeriö on pyytänyt liikenne- ja viestintäministeriön lausuntoa ehdotuksesta turvallisuustutkintalain ja kyberturvallisuuslain 17 §:n muuttamisesta. Liikenne- ja viestintäministeriö kiittää mahdollisuudesta lausua esityksestä.

Hankkeessa Onnettomuustutkintakeskukselle ehdotetaan säädettävän toimivalta tutkia erittäin vakavia kyberturvallisuuspoikkeamia. Lisäksi esityksellä ehdotetaan pantavan kansallisesti täytäntöön Euroopan unionin merionnettomuustutkintadirektiiviin tehty lainsäädäntötoimenpiteitä edellyttävät muutokset. Lisäksi turvallisuustutkintalakia ehdotetaan tarkistettavaksi joidenkin muiden sääntelykysymysten osalta. Näitä ovat mm. määritelmät, turvallisuustutkinnan asiantuntijarekisteristä säätäminen sekä selvitys ja yhteenvetoraportti. Kyberturvallisuuslain muuttamisen osalta kyse olisi informatiivisesta viittauksesta turvallisuustutkintalakiin.

Ehdotus turvallisuustutkintalain muuttamisesta pohjautuu kansallista turvallisuutta ja yhteiskunnan kriisinkestävyyttä vahvistavaan kirjaukseen Petteri Orpon hallituksen ohjelmassa ”Selvitetään mahdollisuus lisätä Onnettomuustutkintakeskuksen toimialaan kyberturvallisuuteen kohdistuneiden vakavien häiriöiden turvallisuustutkinta. Hallitus valmistelelee tarvittaessa säädösmuutokset turvallisuustutkintalakiin ja tekee siihen muut tarvittavat tarkistukset.”

Liikenne- ja viestintäministeriö toteaa, että on saanut mahdollisuuden osallistua vain yksittäisten pykälien osalta alustaviin keskusteluihin mutta ei ole ennen lausuntokierrosta nähnyt esitettäviä muutoksia tai hallituksen esitystä kokonaisuutena.

Kyberturvallisuuspoikkeamien syiden tutkiminen ja niistä oppiminen on tärkeää. Liikenne- ja viestintäministeriö kuitenkin katsoo, että esitystä tulisi tietyin osin kehittää ja täydentää, jotta saavutettaisiin toimiva malli toteuttaa turvallisuustutkintaa ja samalla turvata nykyisellään hyvin toimiva kyberturvallisuuden yhteistoimintamallin viranomaisten ja toimijoiden työ.

Liikenne- ja viestintäministeriö lausuu seuraavaa keskittyen lausunnossaan erityisesti Onnettomuustutkintakeskukselle ehdotettuun toimivaltaan tutkia erittäin vakavia kyberturvallisuuspoikkeamia. Euroopan unionin merionnettomuustutkintadirektiivin kansallisesta täytäntöönpanosta johtuvat turvallisuustutkintalakiin ehdotetut muutokset ovat perusteltuja eikä niiden osalta ole huomioitavaa.

Nykytila ja sen arviointi

Liikenne- ja viestintäministeriö katsoo, että nykytilan kuvausta tulisi merkittävästi täydentää ja osin myös korjata.



Kyberturvallisuuden kansallinen yhteistoimintamalli ja eri viranomaisten tehtävät

Nykytilan kuvauksesta puuttuu kokonaan kuvaus kyberturvallisuuden kansallisesta yhteistoimintamallista ja eri viranomaisten tehtävistä. Kyberturvallisuuden yhteistoimintamalli Suomessa on hajautettu ja vastaa periaatteiltaan kokonaisturvallisuuden yhteistoimintamallia. Yhteistyön perustana ovat lakisääteiset tehtävät, yhteistyösopimukset ja yhteiskunnan turvallisuusstrategia, jonka jokaisessa strategisessa tehtävässä otetaan huomioon kyberturvallisuus. Kyberturvallisuuden yhteistoimintamallissa ja kyberturvallisuudirektiivin tarkoittamassa kyberkriisitilanteessa toimivaltaiset viranomaiset johtavat häiriötilanteen hallintaa kukin tehtävänsä ja toimivaltansa puitteissa. Toimivaltaiset viranomaiset, toiminnan yhteensovittaminen sekä tukeminen määritetään tarvittaessa yhteiskunnan kriisijohtamisen mallin mukaisesti.

Kyberturvallisuuspoikkeamiin reagoiminen ja niiden tutkiminen perustuu tällä hetkellä selkeisiin eri viranomaisten lakisääteisiin tehtäviin ja toimivaltoihin sekä viranomaisten väliseen kattavaan yhteistyöhön. Jokaisella viranomaisella on omat tehtävänsä, joita toisen viranomaisen toimenpiteet eivät voi korvata. Poikkeaman selvitys on usein samanaikaisesti usean viranomaisen vastuulla.

Kybertoimintaympäristön turvallisuutta vaarantava tapahtuma voi olla samanaikaisesti tietoturvapoikkeama tai sen uhka, rikos taikka kansallista turvallisuutta ja maanpuolustusta vaarantava tapahtuma, jolla voi olla ulko- ja turvallisuuspoliittisia vaikutuksia. Turvallisuutta vaarantava tapahtuma voi lisäksi olla myös esimerkiksi muun sektorikohtaisen lainsäädännön rikkomus tai GDPR:n mukainen henkilötietorikkomus.

Tietoturvapoikkeaman hallintaa koordinoi Liikenne- ja viestintäviraston Kyberturvallisuuskeskus, esitutkinnasta vastaa poliisi, ulko- ja turvallisuuspoliittisen päätöksenteon valmisteluun tietoa tuottavat tiedusteluviranomaiset ja puolustusjärjestelmän turvallisuudesta vastaa Puolustusvoimat. Lisäksi kyberturvallisuuden tuottamiseen osallistuu laaja joukko muita viranomaisia sekä julkisia ja yksityisiä toimijoita. Kyberturvallisuuden toimijakenttä on laaja ja se perustuu laajaan yhteistyöhön ja luottamukseen niin yksityisen kuin julkisenkin sektorin välillä. Toimijakentän kuvaaminen on tärkeää, jotta voidaan turvata jokaisen viranomaisen lakisääteisten tehtävien toteuttaminen poikkeaman selvittämisessä.

Liikenne- ja viestintäministeriö pitää tärkeänä, että nykytilan kuvausta täydennetään kuvaamalla kyberturvallisuuden kansallinen yhteistoimintamalli eli eri viranomaisten tehtävät kyberturvallisuudessa. Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen ja muiden viranomaisten toimintaa on kuvattu mm. Suomen kyberturvallisuusstrategiassa 2024–35 kyberturvallisuuden kansallisen yhteistoimintamallin yhteydessä sekä Selvityksessä viranomaisten toimintaedellytyksistä kyberturvallisuudessa (VN2023:31). Lisäksi yhteiskunnan turvallisuusstrategiassa (YTS) liikenne- ja viestintäministeriön vastuulla on kyberturvallisuuden kansallisen toimintamallin ylläpitäminen yhteistyössä muiden ministeriöiden kanssa (YTS:n strateginen tehtävä 35). Eri viranomaisten tehtävien kuvauksia on sisällytetty laajasti myös Onnettomuustutkintakeskuksen julkaisemaan Helsingin kaupungin tietomurto 2024-tutkintaselostukseen (P2024-01). Lisäksi Suomen kyberturvallisuusstrategiassa on avattu siinä käytettyä sanastoa, joka on tarkentunut ja täydentynyt verrattuna kyberturvallisuuden vuonna 2018 laadittuun sanastoon.

Liikenne- ja viestintäministeriön hallinnonalan osalta nykytilan kuvauksen tulisi sisältää kuvaus Liikenne- ja viestintäviraston sekä sen kyberturvallisuuskeskuksen ja ensivasteen antavan CSIRT



(Computer Security Incident Response Team) -yksikön lakisääteisistä tehtävistä sekä kyberturvallisuuden liittyvien tapahtumien havainnoinnista sekä ilmoittamisesta. Olisi tärkeää kuvata myös Kyberturvallisuuskeskuksen jo nykyisellään tekemä ns. lesson learned työ, eri toimijoita palveleva tilannekuvatyö sekä kansallisten ja kansainvälisten ISAC (Information Sharing and Analysis Centre)-yhteistyöverkostojen toiminta. Nykytilassa kyberturvallisuuden liittyvistä haitallisista ja vahingollisista tapahtumista sekä kerätään että jaetaan oppeja erittäin tehokkaasti, minkä vuoksi virheellinen on nykytilan kuvauksen lause, jossa todetaan, että merkittävänä puutteena voidaan pitää, että vakavistakaan kyberturvallisuuden liittyvistä haitallisista tai vahingollisista tapahtumista ei riittävästi kerätä ja jaeta oppeja vastaavanlaisten tapahtumien ennalta ehkäisemiseksi ja vahinkojen välttämiseksi. Liikenne- ja viestintäministeriö ehdottaa, että em. lause poistetaan ja nykytilanne tältä osin kuvataan tarkemmin.

Kyberturvallisuuskeskuksen keskeinen tehtävä on vastata kansallisen kyberturvallisuuden tilannekuvan ylläpidosta ja kansallisesta haavoittuvuuskoordinaatiosta. Se kerää ja analysoi tietoa Suomessa tapahtuvista tietoturvahaukista ja -loukkauksista sekä selvittää osaltaan Suomeen kohdistuvia teknisiä tietoturvapoiikkeamia. Sen tehtäviin kuuluu myös yleisen kyberturvallisuustietoisuuden lisääminen. Kyberturvallisuuskeskuksen asiakkaat voivat hyödyntää tilannekuvatietoa oman varautumisensa järjestämisessä ja priorisoinnissa. Lisäksi Kyberturvallisuuskeskus tekee laajaa luottamukseen perustuvaa operatiivista yhteistyötä ja tiedonvaihtoa keskeisten kansallisten ja kansainvälisten verkostojen kanssa.

Kyberturvallisuuden vakavien häiriöiden tutkinta ja Helsingin kaupungin tietomurron tutkintaselostuksesta saadut kokemukset

Nykytilan kuvauksessa on todettu, että hallitusohjelman kyberturvallisuuden vakavien häiriöiden turvallisuustutkintaa koskevan kirjauksen toteuttaminen edellyttää uutta sääntelyä turvallisuustutkintalakiin. Samalla on todettu, ettei lain nykyinen sääntely ole riittävää sen osalta, että Onnettomuustutkintakeskuksella olisi toimivalta suorittaa mainittujen kyberturvallisuuden vakavien häiriöiden turvallisuustutkintaa.

Liikenne- ja viestintäministeriö pitää tärkeänä, että nykytilan kuvausta korjattaisiin myös tältä osin, sillä jo nykyisellään kyberturvallisuuden vakavien häiriöiden tutkinta on mahdollista tehdä turvallisuustutkintalain (525/2011) 5 luvun mukaan poikkeuksellisen tapahtuman tutkintana valtioneuvoston päätöksellä, kuten tehtiin Helsingin kaupunkiin kohdistuneen tietomurron tutkinnan osalta. Hallituksen esitykseen olisikin tärkeää tarkentaa, miksi uutta lainsäädäntöä pidetään tästä huolimatta tarpeellisena, mitä nykyinen sääntely ei mahdollista ja mitä kehitettävää lainsäädännössä on havaittu keväällä 2025 valmistuneen Helsingin kaupungin tietomurron turvallisuustutkinnasta saatujen havaintojen pohjalta. Hallituksen esityksen luonnoksessa ei nyt mainita lainkaan Helsingin kaupungin tietomurron tutkintaa, vaikka se, ollessaan ensimmäinen kyberturvallisuuspoikkeaman tutkinta, antaisi hyvän mahdollisuuden tarkastella lainsäädännön muuttamisen tarpeita ja myös avata tarkemmin, mitä kyberturvallisuuspoikkeamien tutkinnalla tavoitellaan.

Turvallisuustutkinnan laajentaminen poikkeamiin

Nykytilan kuvauksessa todetaan lisäksi, että turvallisuustutkintalaki on vastannut tarkoitustaan lakina, jolla säädetään Onnettomuustutkintakeskukselle toimivalta suorittaa onnettomuuksien ja vaaratilanteiden tutkintaa. Nyt ehdotettujen muutosten myötä turvallisuustutkintalaki mahdollistaisi lisäksi erittäin vakavien kyberturvallisuuspoikkeamien tutkinnan, jolloin kyse ei välttämättä olisi vain



joko onnettomuudesta tai vaaratilanteesta vaan näiden lisäksi vaikuttaisi siltä, että kyseeseen voisi tulla muu poikkeamaksi luettava tilanne, joka voisi jopa olla edelleen käynnissä tutkinnan alkaessa.

Liikenne- ja viestintäministeriö pitää tärkeänä, että esityksessä kuvattaisiin selkeämmin tarvetta laajentaa Onnettomuustutkintakeskuksen toimivalta kyberturvallisuuspoikkeamien tutkintaan ja kuvattaisiin miltä osin vakavien kyberturvallisuuspoikkeamien tutkinta tuo lisäarvoa jo nykyisellään kattavalle kyberturvallisuuspoikkeamien tutkinnalle. Käynnissä olevan tietoturvallisuuspoikkeaman ulkopuolinen turvallisuustutkinta saattaa vaikuttaa jopa haitallisesti niihin poikkeaman hallintakeinoihin, joiden tarkoituksena on onnettomuuden ja vahinkojen ehkäiseminen.

Salassa pidettävät ja turvallisuusluokitellut tiedot

Liikenne- ja viestintäministeriö korostaa, että erittäin vakavassa kyberturvallisuuspoikkeamassa saattaa olla kyse tiedoista, jotka ovat julkisuuslain 24 §:n 1 momentin mukaisten salassapitoperusteiden nojalla salassa pidettäviä tai turvallisuusluokiteltuja. Kyberturvallisuuspoikkeama saattaa samanaikaisesti koskea toimivaltaisia viranomaisia, julkisia organisaatioita ja yksityistä sektoria, ja salassapitoa tulee näin ollen arvioida useasta eri näkökulmasta. Liikenne- ja viestintäministeriö korostaa, että erityisesti turvallisuusluokitellun tiedon osalta korostuu sen viranomaisen arvio, jolla on edellytykset arvioida tiedon luonnetta suhteessa salassapitosäännöksellä suojattuun etuun. Lisäksi on huomioitava, että koska Onnettomuustutkintakeskus tutkii erittäin vakavan kyberturvallisuuspoikkeaman niin teknisiä kuin prosessuaalisiakin syitä sekä mahdollisia kehittämisen kohteita kohdeorganisaatioiden ja ensivasteen antavien kyberturvallisuusviranomaisten toiminnassa, erittäin vakavasta kyberturvallisuuspoikkeamasta kerätty tieto saattaa muodostaa hyvinkin kattavaa tietoa kyberturvallisuusviranomaisten kyvykkyyksistä ja valmiuksista.

Pääasialliset vaikutukset

Liikenne- ja viestintäministeriö katsoo, että vaikutusten arviointia tulisi merkittävästi täydentää.

Viranomaiset

Esityksen vaikutuksissa tulisi arvioida esityksen vaikutukset kyberturvallisuuden kansalliseen yhteistoimintamalliin ja eri viranomaisten toimintaan poikkeaman selvittämisessä, mikäli tutkinta kohdistuisi käynnissä olevaan häiriötilanteeseen. Liikenne- ja viestintäviraston tehtäviin esityksellä voisi olla merkittävää vaikutusta, mikäli tutkinta alkaisi poikkeaman ja siinä avustamisen ollessa vielä käynnissä. Vaikutusten arvioinnissa tulisi lisäksi tarkastella vaikutuksia kyberturvallisuuslain valvovien viranomaisten tehtäviin ainakin heille asetettavan ilmoitusvelvollisuuden osalta ottaen huomioon, että kyberturvallisuuslaki on vielä uutta lainsäädäntöä.

Resurssit ja osaaminen

Vaikutusten arvioinnissa on todettu, että erittäin vakavien kyberturvallisuuspoikkeamien tutkinta merkitsisi Onnettomuustutkintakeskukselle uudenlaisia tehtäviä mutta ei vaatisi lisäresursointia. Onkin epäselvää, mistä resurssit kyberturvallisuuspoikkeamien tutkintaan voitaisiin saada ja on mahdollista, että erittäin vakavien kyberturvallisuuspoikkeaminen tutkiminen voisi aiheuttaa lisätehtäviä Kyberturvallisuuskeskukselle tai muulle viranomaiselle tutkinnassa avustamisen osalta. Tämän osalta on kuitenkin huomioitava, että voisi olla mahdollista, että esimerkiksi Kyberturvallisuuskeskuksen resursseja ei välttämättä voisi käyttää lakiluonnoksen 14 §:n esteellisyyteen perustuen kyberturvallisuuspoikkeamien tutkinnassa silloin, kun



Kyberturvallisuuskeskuksen asiantuntija on osallistunut tapauksen tutkintaan lakisääteisen tehtävän hoitamiseksi.

Vaikutusten arviointia tulisi täydentää arkaluontoisen tiedon käsittelyyn liittyvien vaikutusten osalta. Erittäin vakavien kyberturvallisuuspoikkeamien tutkiminen voi edellyttää mm. liikesalaisuuksia, kansallista turvallisuutta, yhteiskunnan varautumista ja/tai ulkosuhteita koskevien tietojen käsittelyä. Näiden tietojen luovuttaminen Onnettomuustutkintakeskukselle ei Liikenne- ja viestintäministeriön näkemyksen mukaan saa vaarantaa niitä etuja, joita salassapitosäännöksellä suojataan. Tämän huomioiminen korostuu erityisesti julkisen tutkintaselostuksen kohdalla. Lisäksi on huomioitava, että merkittäviin intresseihin liittyvät tiedot tekevät niin Onnettomuustutkintakeskuksesta kuin myös sen henkilöstöstä potentiaalisen vaikuttamisen ja luvattoman tiedonhankinnan kohteena.

Esityksessä ei myöskään ole tuotu ilmi, millaista teknistä osaamista tai järjestelmiä Onnettomuustutkintakeskuksella on käytössään. Erittäin vakavien kyberturvallisuuspoikkeamien tutkiminen voisi edellyttää Onnettomuuskeskukselta jopa TL II -luokitellun tiedon suojaamiseen tarvittavia prosesseja sekä mahdollisesti tietojärjestelmiä ja tiloja ja mahdollisesti myös henkilöstön luotettavuuden arviointien kehittämistä. Onnettomuustutkintakeskus käyttää tutkinnoissa ulkopuolisia asiantuntijoita ja avustajia sekä tuntipalkkaisia avustajia. Nykyisen käytännön jatkaminen edellyttäisi turvallisuusluokitellun tietoon liittyvien käytäntöjen tarkistamista toiminnan luottamuksellisuuden korostuessa merkittävästi. Liikenne- ja viestintäministeriö katsoo, että tämä voi tarkoittaa merkittäviä lisäkustannuksia Onnettomuustutkintakeskukselle eikä siten voisi olla toteutettavissa nykyresurssein.

Vaikutukset yrityksiin

Liikenne- ja viestintäministeriö haluaa korostaa, että nykyisellään kyberturvallisuuden toimialalla ja niin yksityisten kuin julkisten toimijoiden välillä vallitsee kansainvälisestikin poikkeuksellinen luottamus. Käsillä olevan lakiuudistuksen vaikutusten osalta olisi syytä huomioida, että valvoville viranomaisille tehtyjen merkittävien poikkeamailmoitusten määrä saattaa vähentyä sen myötä, että valvova viranomainen on veloitettu ilmoittamaan poikkeamista Onnettomuustutkintakeskukselle. Tämä pätee pitkälti sellaisissa tilanteissa, joissa toimija ilmoittaa pakollisena ilmoituksena poikkeamista, jotka eivät ylitä merkittävyyden kynnyksiä. Valittavien sääntelykeinojen tulee olla sellaisia, etteivät ne vaaranna vapaaehtoisuuteen perustuvaa yhteistyötä ja yritysten ja kyberturvallisuuskeskuksen välistä luottamuksellista suhdetta.

Välttämättömien toimien ja ensivasteen lisäksi olisi syytä huomioida, että Onnettomuustutkintakeskuksen tutkintaedellytyksien turvaamisella kuten kyberturvallisuuspoikkeamaan liittyvän paikan eristämällä saattaa olla merkittäviä taloudellisia vaikutuksia sille toimijalle, johon poikkeama on kohdistunut. Tämä saattaa lisätä osaltaan kyberturvallisuuspoikkeaman myötä syntyneitä kustannuksia.

Muut toteuttamisvaihtoehdot

Liikenne- ja viestintäministeriö pitää tärkeänä, että esitysluonnoksessa arvioitaisiin muita toteutusvaihtoehtoja huomioiden Helsingin kaupungin tietomurron tutkinnasta saadut kokemukset. Siitä huolimatta, että Onnettomuustutkintakeskukselle lisättäisiin turvallisuustutkintalakiin toimivalta tutkia vakavia kyberturvallisuuspoikkeamia, on kuitenkin valittavissa erilaisia keinoja tämän toteuttamiseen.



Erityisesti liikenne- ja viestintäministeriö toivoo vaihtoehtojen tarkastelussa huomioitavaksi erilaiset vakavan poikkeaman määritelmät (kyberturvallisuuslain mukainen poikkeama, merkittävä poikkeama ja näitä korkeamman kynnyksen erittäin vakava kyberturvallisuuspoikkeama) sekä vaihtoehto tutkia kyberturvallisuuspoikkeamat jälkikäteen. Lisäksi arvioida tulisi vaihtoehto, jossa kyberturvallisuuspoikkeamien tutkinta tapahtuisi edelleen poikkeuksellisen tapahtuman tutkintana.

Turvallisuustutkintalaki; pykäläkohtaiset huomiot

1 a § Määritelmät

Turvallisuustutkintalakiin ehdotetaan uutta 1 a §:ä, jossa määriteltäisiin, mitä tarkoitetaan mm. onnettomuudella, suuronnettomuudella, vaaratilanteella ja erittäin vakavalla kyberturvallisuuspoikkeamalla.

Onnettomuus, suuronnettomuus ja vaaratilanne

Liikenne- ja viestintäministeriö toivoo, että esitykseen tarkennettaisiin, mikä 1 a §:n määritelmien suhde on 2 §:ssä kuvattuihin tutkittaviin onnettomuuksiin ja vaaratilanteisiin, joissa viitataan EU-säädöksiin. Esimerkiksi ilmailun ja merenkulun osalta määritelmät perustuvat globaaleihin, Kansainvälisessä siviili-ilmailujärjestössä (ICAO) ja Kansainvälisessä merenkulkujärjestössä (IMO) tuotettuihin määritelmiin ja olisi erittäin tärkeää, että näistä määritelmistä edelleen pidetään kiinni.

Erittäin vakavat kyberturvallisuuspoikkeamat

Nyt ehdotettavassa turvallisuustutkintalain muutoksessa Onnettomuustutkintakeskukselle ehdotetaan säädettäväksi toimivalta tutkia *erittäin vakavia kyberturvallisuuspoikkeamia*. Erittäin vakavalla kyberturvallisuuspoikkeamalla tarkoitetaan ehdotetun 1 a §:n 4 kohdan mukaan tapahtumaa, jonka seurauksena on yhteiskunnan toimintoja tai strategisia tehtäviä merkittävästi vaarantava viestintäverkkojen tai tietojärjestelmien häiriytyminen tai vahingoittuminen. Turvallisuustutkintalakia koskevan hallituksen esityksen perusteluissa on todettu, että ehdotettu termi vastaisi pääpiirteittäin kyberturvallisuuslaissa olevaa määritelmää poikkeamalle, mutta todettu myös, että yksityiskohtainen määrittely on haasteellista.

Kyberturvallisuuslain (124/2025) 2 §:n määritelmässä kohdassa 11 määritellyllä *poikkeamalla* tarkoitetaan tapahtumaa, joka vaarantaa viestintäverkoissa ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden. Näiden ilmoittaminen valvovalle viranomaiselle perustuu vapaaehtoisuuteen.

Kyberturvallisuuslain 11 §:ssä on säädetty viranomaiselle tehtävistä poikkeamailmoituksista. Toimijan on viipymättä ilmoitettava valvovalle viranomaiselle *merkittävästä poikkeamasta*, jolla tarkoitetaan poikkeamaa, joka on aiheuttanut tai voi aiheuttaa vakavan palvelujen toimintahäiriön tai huomattavia taloudellisia tappioita asianomaiselle toimijalle, sekä poikkeamaa, joka on vaikuttanut tai voi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa.

Liikenne- ja viestintäministeriö on hallituksen esitystä koskevissa alustavissa keskusteluissa nostanut esiin riittävän tutkintakynnyksen ylittävän poikkeaman määrittelyn haasteet ja ehdottanut,



että poikkeamamääritelmä perustuisi esimerkiksi kyberturvallisuuslain (124/2025) 11 §:n mukaiseen merkittävän poikkeaman määritelmään, jota tarkennettaisiin lisämäärittelyin riittävän korkean ilmoitus- ja tutkintakynnyksen varmistamiseksi. Käsityksemme mukaan riittävän korkea ilmoituskynnys on ollut tavoitteena myös esitystä valmisteltaessa. Erittäin vakava kyberturvallisuuspoikkeama tulisikin määritellä siten, että kyse on poikkeamaa ja merkittävää poikkeamaa vakavammasta tilanteesta.

Liikenne- ja viestintäministeriö toteaa, että erittäin vakavan kyberturvallisuuspoikkeaman ehdotettu määrittely voi aiheuttaa haasteita valvoville viranomaisille. Tulkinnan haasteellisuutta lisää merkittävästi usean erilaisen määritelmän käyttäminen eikä valvovan viranomaisen ole helppoa tunnistaa, mikä on erittäin vakava kyberturvallisuuspoikkeama ja milloin ilmoitusvelvollisuus ylittyy. Valvovia viranomaisia on lisäksi useita, mikä edellyttää yhteistyötä ja koordinaatiota yhtenäisen tulkintakäytännön luomiseksi.

Liikenne- ja viestintäministeriö on alustavien keskustelujen aikana ehdottanut, että tutkintakynnyksen ylittävällä kyberturvallisuuspoikkeamalla tarkoitettaisiin:

Kyberturvallisuuslain (124/2025) 11 §:n mukaista merkittävää poikkeamaa, jolla on poikkeuksellisen vakavia tai laajamittaisia haitallisia vaikutuksia:

- 1) julkisen vallan päätöksentekokykyyn tai viranomaisten toimintaedellytyksiin;*
- 2) kansalliseen turvallisuuteen tai maanpuolustukseen;*
- 3) välttämättömiin sosiaali- ja terveydenhuollon tai pelastustoimen palveluihin;*
- 4) energia-, vesi, elintarvike- tai lääkehuoltoon taikka muihin välttämättömiin hyödykkeisiin;*
- 5) välttämättömiin maksu- ja arvopaperipalveluihin;*
- 6) yhteiskunnan kriittisiin liikenne- ja viestintäpalveluihin;*
- 7) edellä 1 – 6 kohdassa tarkoitettuja toimintoja ylläpitäviin tieto- ja viestintätekniisiin palveluihin tai tietoaaineistoihin;*
- 8) yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain (320/2025) nojalla määritettyihin kriittisiin toimijoihin; tai*
- 9) henkilötietojen suojaan.*

Kyberturvallisuuspoikkeamien luonteen vuoksi on lisäksi muistettava, että ilmoituskynnys Onnettomuustutkintakeskukselle ei välttämättä ylitä ensimmäisissä saaduissa poikkeamailmoituksissa vaan vasta saataessa lisää tietoa tilanteesta ja vahingoista. On yleistä, että kyberturvallisuuspoikkeamien vakavuus paljastuu vasta myöhemmin ja jatkoilmoitusten aikana, mutta poikkeaman tilanne on silti käynnissä. Helsingin kaupungin tietomurrosta tehdyn tutkinnan perusteella olisi mahdollista arvioida määritelmän toimivuutta sekä ilmoituskynnyksen ylittymistä. Hallituksen esitykseen tulisi kuvata esimerkkejä tapauksista, joiden voidaan katsoa olevan erittäin vakavia kyberturvallisuuspoikkeamia ja siten ylittävän ilmoituskynnyksen ja turvallisuustutkinnan aloittamisen kynnyksen.

2 § Tutkittavat onnettomuudet, vaaratilanteet ja erittäin vakavat kyberturvallisuuspoikkeamat

Liikenne- ja viestintäministeriö pitää kannatettavana sitä, että vakavien kyberturvallisuuspoikkeamien tutkinnan suorittaminen olisi harkinnanvaraista.

Tutkittaviksi otettavat erittäin vakavat kyberturvallisuuspoikkeamat tulisi kuitenkin kuvata hallituksen esityksessä tarkemmin, sillä ne eroavat merkittävästi fyysisen maailman, kuten esimerkiksi ilmailun ja raideliikenteen, onnettomuuksista ja vaaratilanteista. Liikenne- ja



viestintäministeriö pitää erittäin tärkeänä, että tutkinta ei kohdistu käynnissä olevaan poikkeamaan, jotta voidaan turvata poikkeaman selvittäminen ja ehkäistä lisävahinkojen syntyminen.

Turvallisuustutkintalain 5 §:n mukaan turvallisuustutkinnassa selvitetään tapahtumien kulku, syyt ja seuraukset sekä tarvittaessa kaikkien pelastustoimiin osallistuneiden toiminta ennen tapahtumaa, tapahtuman aikana ja sen jälkeen. Liikenteen osalta (turvallisuustutkintalain 2 §) tutkitaan tapahtuneita onnettomuuksia ja vaaratilanteita. Olisikin siten johdonmukaista, että kyberturvallisuuspoikkeamien osalta samoin tutkittaisiin vain tapahtuneita poikkeamia – ei käynnissä olevia. Näin on mahdollista tarkastella myös pelastustoimia ja niihin osallistuneiden toimintaa.

Hallituksen esitykseen olisi tärkeää kuvata, mikä on hetki, jolloin vakavan kyberturvallisuuspoikkeaman tutkinta voidaan aloittaa. Liikenne- ja viestintäministeriö katsoo, että onnettomuustutkinnan tulisi alkaa vasta kyberpoikkeaman aktiivisen käsittelyn päätyttyä, ja ehdottaa, että Onnettomuustutkintakeskuksen toimivalta tutkia vakava kyberturvallisuuspoikkeama alkaisi vasta, kun kyberturvallisuuspoikkeaman kohteeksi joutunut organisaatio on toimittanut valvovalle viranomaiselle KTL 13 §:n mukaisen loppuraportin.

5 § Tutkinnan sisältö

Esityksessä ehdotetaan lisättäväksi tutkinnassa erityisesti selvitettävän, onko turvallisuus otettu huomioon kyberturvallisuuteen johtaneessa toiminnassa. Ehdotuksessa lisättäisiin tutkittavien kohteiden luetteloon järjestelmä ja ohjelmisto. Esitykseen tulisi kuitenkin tarkentaa, millaista tutkintaa sen pohjalta järjestelmiin ja ohjelmistoihin on tarkoitus kohdentaa. Järjestelmiin ja ohjelmistoihin kohdistettava tutkinta edellyttää teknistä osaamista ja voi sisältää pääsyn arkaluonteisiin tietoihin.

Kyberhäiriötilanteista palautuminen on hyvin keskeinen päämäärä, onhan käytettävyyksi yksi tietoturvan suojattava intressi. Ympäristöt pyritään saamaan mahdollisimman pian käyttöön teknisten näytteen oton jälkeen ja kun on todennettu, ettei hyökkääjällä ole enää jalansijaa ympäristössä. Tästä näkökulmasta pitkään kestävä onnettomuustutkinta voi merkittävästi haitata yhteiskunnan toiminnan kannalta kriittistä palvelua.

6 § Alueellinen toimivalta

Pykälän 2 momenttia ehdotetaan muutettavaksi siten, että turvallisuustutkinta voitaisiin tehdä Suomen ulkopuolella tapahtuneesta onnettomuudesta tai erittäin vakavasta kyberturvallisuuspoikkeamasta siten kuin turvallisuustutkintaa koskevassa Euroopan unionin lainsäädännössä säädetään tai Suomea sitovassa kansainvälisessä velvoitteessa määrätään.

Liikenne- ja viestintäministeriö katsoo, että perusteluissa tulisi tarkemmin kuvata, mitä tämä käytännössä voisi tarkoittaa. Millaisia Suomen ulkopuolella tapahtuneita erittäin vakavia kyberturvallisuuspoikkeamia Onnettomuustutkintakeskuksella olisi toimivalta tutkia?

16 a § Ilmoitusvelvollisuus erittäin vakavasta kyberturvallisuuspoikkeamasta

Liikenne- ja viestintäministeriö pitää perusteltuna, että ilmoitusvelvollisuus voisi olla kyberturvallisuuslain valvovalla viranomaisella. Liikenne- ja viestintäministeriö nostaa kuitenkin esiin, että hallituksen esitys ja erityisesti sen ehdotetut 16 a § ja 20 a § eivät näyttäisi kattavan kaikkia NIS 2 -direktiivin mukaisia valvovia viranomaisia. NIS 2 -direktiivin 8 artiklassa



tarkoitettuina toimivaltaisina viranomaisina toimivat kansallisesti kyberturvallisuuslain 26 §:ssä ja tiedonhallintalain 18 h §:ssä tarkoitetut viranomaiset sekä Finanssivalvonnasta annetun lain (878/2008) 50 p §:n nojalla Finanssivalvonta. Hallituksen esitykseen tulisikin tarkentaa, onko tarkoitus, että ilmoitusvelvollisuus koskisi vain kyberturvallisuuslain mukaisia valvovia viranomaisia, sillä tämä rajaisi Finanssivalvonnan valvottavien lisäksi julkishallinnon poikkeamat pois ilmoitusvelvollisuuden piiristä.

Huomioitavaa on lisäksi se, että ilmoitusvelvollisuus esityksessä on nyt kyberturvallisuuslain tarkoittamalla valvovalla viranomaisella, joka käytännössä voi tehdä ilmoituksen vain saamistaan kyberturvallisuuslain mukaisista merkittävistä poikkeamista, jotka se arvioi ylittävän ilmoituskynnyksen. Kaikkia viranomaisenaan tietoon tulleita merkittäviä poikkeamia ei siten saatettaisi ehdotuksen nojalla Onnettomuustutkintakeskuksen tietoon.

Kyberturvallisuuslain 4 §:n soveltamisalarajauksissa on todettu, että kyberturvallisuuslain säännöksiä, jotka velvoittavat antamaan tietoa, ei sovelleta, jos tiedon luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin siihen liittyvää tärkeää etua. Liikenne- ja viestintäministeriö esittää, että sama rajausta lisättäisiin turvallisuustutkintalain ilmoittamisvelvollisuutta koskevaan 16 a §:ään.

19 § Tutkintaedellytysten turvaaminen

Esitysluonnoksessa ehdotetaan säädettäväksi, että Onnettomuustutkintakeskuksella olisi 19 §:n nojalla oikeus päästä onnettomuuspaikalle tai paikkaan, joka liittyy erittäin vakavaan kyberturvallisuuspoikkeamaan. Onnettomuustutkintakeskuksen tutkintaa tekevällä olisi oikeus tutkia onnettomuuteen tai erittäin vakavaan kyberturvallisuuspoikkeamaan liittyviä esineitä, laitteita, ohjelmistoja ja rakenteita. Onnettomuustutkintakeskus ja tutkintaryhmän johtaja voivat määrätä onnettomuuspaikan tai erittäin vakavaan kyberturvallisuuspoikkeamaan liittyvän paikan eristettäväksi, jos se on turvallisuustutkinnan kannalta välttämätöntä. Lisäksi erittäin vakavaan kyberturvallisuuspoikkeamaan liittyvässä paikassa olevia esineitä, laitteita ja muuta aineistoa, joilla saattaa olla merkitystä tutkinnassa, ei saa ilman lupaa hävittää, viedä pois eikä liikutella.

Liikenne- ja viestintäministeriön näkemyksen mukaan kyberturvallisuuspoikkeaman onnettomuuspaikka ei ole suoraan rinnastettavissa fyysisen maailman kuten lento-onnettomuuden paikkaan. Onnettomuuspaikan määritelmää olisi näin ollen syytä tarkentaa. Lisäksi Liikenne- ja viestintäministeriö katsoo, että esityksessä kuvattaisiin tarkemmin, mitä pääsyllä laitteisiin, järjestelmiin ja ohjelmistoihin tarkoitetaan. Esityksen perusteluissa olisi syytä kuvata se, mitkä laitteet katsotaan kuuluvan erittäin vakavaan kyberturvallisuuspoikkeamaan liittyväksi ja miten Onnettomuustutkintakeskus arvioi tutkintatoimenpiteidensä ulottamisen.

Kyberturvallisuuspoikkeamat ja siihen liittyvät olosuhteet ovat luonteeltaan täysin erilaisia kuin reaali maailman onnettomuuspaikat, koska kyberturvallisuuspoikkeaman alkaminen ja loppuminen vaihtelee tapauskohtaisesti. Kyberturvallisuuspoikkeaman vaikutukset voivat lisäksi realisoitua myöhemmin. Näin oli esimerkiksi Vastaamon tietomurtotapauksessa, jossa varsinainen tietomurto oli tapahtunut paljon aikaisemmin kuin kiristys terveystietojen julkaisusta. Liikenne- ja viestintäministeriö katsoo, että esityksessä olisi syytä antaa esimerkkejä tilanteista, joissa tutkintaedellytysten turvaamiseen käytettäviä keinoja kohdistetaan erittäin vakavan kyberturvallisuuspoikkeamaan liittyviin paikkoihin ja laitteisiin.



Liikenne- ja viestintäministeriö pitää tärkeänä, että Onnettomuustutkintakeskuksen tutkintaedellytysten osalta on huomioitu, että muut kyberturvallisuusviranomaisten tekemät välttämättömät toimet kyberturvallisuuspoikkeaman keskeyttämiseksi ja rajoittamiseksi sekä sen vaikutusten estämiseksi on turvattu. Tämä olisi huomioitava myös toimijan tai sen lukuun toimivan tahon osalta, johon erittäin vakava kyberturvallisuuspoikkeama on kohdistunut. Toimijat palkkaavat usein kolmannen osapuolen eli ns. DFIR-toimijan, jotka tutkivat ja tekevät välttämättömät toimenpiteet, jotta tekninen ympäristö on saatu stabiloitua ja turvattua. Ennenaikainen kyberturvallisuuspoikkeaman onnettomuuspaikan tai laitteiden eristäminen saattaisi vaikuttaa näihin välttämättömiin toimiin ja osaltaan poikkeaman vaikutuksiin. Onnettomuustutkintakeskuksen tekemä turvallisuustutkinta kyberturvallisuuspoikkeamien syiden selvittämiseksi tulisi siis täten tapahtua vasta sitten, kun poikkeaman ja sen vaikutusten estämiseksi on tehty välttämättömät toimet.

Jatkovalmistelussa tulisi arvioida, onko eristämistoimivaltuus ylipäänsä asianmukainen kyberturvallisuuspoikkeamien osalta. Esimerkiksi onnettomuuspaikan rajaaminen moderneissa pilvipalveluympäristössä voi olla jopa mahdotonta, sillä tietojenkäsittely tapahtuu usein abstraktilla tasolla. Palvelut tarjoavat kapasiteettia käytön mukaan eikä ole yksiselitteisesti näytettävissä palvelin tarkkuudella, missä tietojenkäsittely kulloinkin on tapahtunut. Eristäminen voisi myös estää sellaisen yhteiskunnan toiminnan kannalta välttämättömien palvelun tuottamisen, joten mahdollisuus käyttää toimivaltuutta tulisi joka tapauksessa rajata niin, että se olisi käytettävissä vain, jos se ei aiheuta merkittävää haittaa poikkeaman hallinnalle.

Luonnoksen pykälän 3 momentti on epäselvä kyberturvallisuuspoikkeamien hallinnan kannalta. Tulisiko momentti sovellettavaksi selvityksen käynnistämispäätöksestä alkaen? Voitaisiinko sen nojalla pitää kiellettyä aineiston hävittämisenä sitä, että kyberturvallisuuspoikkeaman hallinnassa poistettaisiin esimerkiksi haittaohjelmia tai esimerkiksi järjestelmään oikeudetta luotuja käyttöoikeuksia, jotka liittyvät kyberturvallisuuspoikkeamaan? Tällaisten toimenpiteiden määräämisen tulisi kuulua poliisille.

20 a § Tiedonsaantioikeus erittäin vakavien kyberturvallisuuspoikkeamien turvallisuustutkintaa varten

Esitysluonnoksessa ehdotetaan säädettäväksi tutkintaa tekevän tiedonsaantioikeudesta erittäin vakavien kyberturvallisuuspoikkeamien turvallisuustutkintaa varten. Ehdotuksen mukaan tutkintaa tekevällä olisi salassapitosäännösten estämättä oikeus saada maksutta erittäin vakavien kyberturvallisuuspoikkeamien turvallisuustutkintaa varten tarpeellisia tietoja kyberturvallisuuslain 26 §:ssä tarkoitelta valvovalta viranomaiselta kyberturvallisuuslain 11–13 §:ssä ja 28 §:n 1 ja 2 momentissa tarkoitetuista tiedoista.

Liikenne- ja viestintäministeriö kiinnittää huomiota siihen, että kyberturvallisuuslain mukaisiin valvoviin viranomaisiin rajaa pois tilanteet, joissa poikkeama on ilmennyt Finanssivalvonnan valvomassa toimijassa tai tiedonhallintalain kattamassa toimijassa. Tämä ei välttämättä ole tarkoituksenmukaista.

Luonnoksessa ulotettaisiin tiedonsaantioikeus myös valvovan viranomaisen KTL 28 §:n 2 momentin nojalla saamiin välitystietoihin ja eräin edellytyksin tietoihin viesteistä. KTL 28 § 2 momentissa on säädetty viestinnän luottamuksellisuuden suojan edellyttämistä syistä 1 momenttia täydentävä erityissäännös valvovan viranomaisen tiedonsaantioikeudesta välitystietojen, sijaintitietojen sekä sähköisten viestien osalta. Valvovalla viranomaisella on salassapitosäännösten



tai muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada tieto välitystiedosta, sijaintitiedosta tai haitallisen tietokoneohjelman tai käskyn sisältävästä sähköisestä viestistä, jos se on välttämätöntä kyberturvallisuuden riskienhallintavelvoitteiden noudattamisen valvomista varten tai merkittävän poikkeaman selvittämiseksi.

Vaikka luonnoksessa kuvatulla tavalla kyseisten viestien voidaan eräin edellytyksin katsoa jäävän perustuslain 10.2 §:n mukaisen suojan ulkopuolelle (s. 24), näin ei ole ainakaan välitystietojen osalta. KTL 28 §:n 2 momentissa onkin säädetty viestinnän luottamuksellisuuden suojan turvaamiseksi myös erityisestä salassapitovelvoitteesta momentin nojalla saatuihin tietoihin. Salassapitovelvollisuus on tarpeen sen johdosta, että julkisuuslain salassapitoperusteet eivät riittävästi suojaa viestinnän luottamuksellisuuden alaan kuuluvien tietojen salassapitoa. Lisäksi tiedot tyypillisesti kuuluisivat tiedon luovuttajalla sähköisen viestinnän palveluista annetun lain 136 §:n 4 momentin mukaisen vaihtovelvollisuuden alaan, jolloin olisi perusteltua, että salassapito jatkuisi myös viranomaisessa viestinnän luottamuksellisuuden turvaamiseksi.

Liikenne- ja viestintäministeriö pitää välttämättömänä, että tämä salassapitovelvollisuus ulotetaan myös Onnettomuustutkintakeskuksen turvallisuustutkintaa tekeviin. Tämä olisi mahdollista tehdä säätämällä, että mitä KTL 28.2 §:ssä säädetään valvovan viranomaisen salassapitovelvoitteesta, sovelletaan myös tutkintaa tekevään, jolle on luovutettu siinä tarkoitettuja tietoja. Koska luonnoksen 20a §:n 1 momentin loppuosassa laajennettaisiin tiedonsaantioikeus muihinkin tietoihin, tulisi erikseen säädettävän salassapitovelvoitteen kattaa myös Liikenne- ja viestintäviraston SVPL 316.2 §:n nojalla saamat tiedot, mikäli tiedonsaantioikeuden katsottaisiin kohdistuvan myös niihin. Kyseisiin tietoihin kohdistuu viestinnän luottamuksellisuuden turvaamiseksi perustuslain edellyttämällä tavalla SVPL 319.1 §:n nojalla erityinen salassapitovelvollisuus, eivätkä nämä tiedot voisi tulla julkisiksi vain sillä perusteella, että ne luovutettaisiin turvallisuustutkintaa varten. KTL 28.2 §:ssä ja SVPL 316.2 §:ssä tarkoitettuja tietoja ei lain mukaan voida luovuttaa myöskään rikostutkintaan. Rajaus liittyy tietojen käyttötarkoitussidonnaisuuteen ja perustuslain asettamiin edellytyksiin näihin tietoihin pääsulle. Tämän kanssa ristiriidassa olisi, jos Onnettomuustutkintakeskus voisi luovuttaa saamansa tiedot luonnoksen 39 §:n 2 momentin nojalla mille tahansa viranomaiselle yleisen edun turvaamiseksi. Tämä mahdollisuus olisi suljettava pois. Sikäli kuin kyse olisi teleyrityksiltä saaduista tiedoista, olisi arvioitava ehdotuksia myös suhteessa sähköisen viestinnän tietosuojadirektiivin 15(1) artiklaan.

Valvovan viranomaisen tulisi lisäksi voida kieltäytyä tiedon luovutuksesta KTL 4.7 §:ssä tarkoitetuilla perusteilla eli kun siltä osin kuin tiedon luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin siihen liittyvää tärkeää etua.

21 § Oikeus saada tietoja teleyrityksiltä

Liikenne- ja viestintäministeriö ei pidä perusteltuna luonnoksen 2 momentin mukaista toimivaltuuden laajentamista erittäin vakavan kyberturvallisuuspoikkeaman kulun, syyn tai seurausten selvittämiseksi. Luonnoksessa ei ole perusteltu tiedonsaantioikeuden tarvetta saati välttämättömyyttä tältä osin. Ei ole lainkaan ilmeistä, millä tavoin teleyritysten käsittelemiä välitystietoja voitaisiin hyödyntää turvallisuustutkinnassa. Liikenne- ja viestintäministeriön käsityksen mukaan teleyrityksiltä saatavissa olevilla tiedoilla voi olla merkitystä lähinnä poikkeamaan liittyvässä rikostutkinnassa, kuten selvitettyäessä poikkeamaan liittyvän IP-osoitteen käyttäjää. Tällöin voi olla kyse sähköisen viestinnän palveluista annetun lain 19 luvussa tarkoitetuista, viranomaistarpeisiin säilytetyistä tiedoista. Tällaisten tietojen saamiseen liittyy erityisiä EU-oikeudesta, etusijassa sähköisen viestinnän tietosuojadirektiivin 15(1) artiklasta ja



siihen perustuvasta EU-tuomioistuimen käytännöstä seuraavia edellytyksiä, joihin ei ole luonnoksessa lainkaan viitattu. Lähtökohtana on, että näitä tietoja voidaan saada vain vakavan rikollisuuden torjuntaa varten.

22 § Tarkastusoikeus

Tarkastusoikeuteen ehdotetaan lisättäväksi oikeus erittäin vakavien kyberturvallisuuspoikkeamien osalta oikeus tarkastaa esineiden ja asiakirjojen ohella myös järjestelmiä ja ohjelmistoja. Liikenne- ja viestintäministeriön näkemyksiä avattu 5 §:n kohdalla.

Kuten edellä 19 §:n osalta tuotiin esille, toimivaltuuden ongelmana on se, ettei se edellyttäisi minkäänlaista suhteellisuusarviointia tutkinnan ja etenään haltuun ottamisen välillä seurausten välillä. Äärimmillään järjestelmien haltuun ottaminen voisi estää yhteiskunnan toiminnan kannalta välttämättömän palvelun tuottamisen, joten mahdollisuus käyttää toimivaltuutta tulisi joka tapauksessa rajata niin, että se olisi käytettävissä vain, jos se ei aiheuta merkittävää haittaa poikkeaman hallinnalle tai yleiselle edulle.

27 § Tutkintaselostus

Liikenne- ja viestintäministeriö esittää, että tutkintaselostuksen osalta otettaisiin huomioon se, mitä on jo lausuttu kyberturvallisuuspoikkeamiin liittyvästä salassa pidettävästä ja turvallisuusluokitellusta tiedosta. Erittäin vakavassa kyberturvallisuuspoikkeamassa voi olla pitkälti kyse salassa pidettävästä tai turvallisuusluokitellusta tiedosta, jota ei voida julkistaa millään tasolla. Kyse voi olla esimerkiksi julkisuuslain 24 §:n 1 momentin mukaisista merkittävistä intresseistä. Näin ollen olisi tärkeää, että julkinen tutkintaselostus tehtäisiin tapauskohtaisesti arvioiden tai ainakin säädettäisiin, ettei selostus saa sisältää salassa pidettävää tietoa.

Koska salassapidon laajuutta voi olla vaikea arvioida, soveltuu myös 28 §:ssä mainittu menettely (verkkoviestintäkanavien käyttö tutkintaselostuksen luonnoksesta kuulemiseen) huonosti kyberturvallisuuspoikkeamasta laadittavaan selostukseen, ainakin ellei ensivaiheen kuulemista tehdä erikseen.

39 § Salassa pidettävän tiedon luovuttaminen

Liikenne- ja viestintäministeriö viittaa edellä 20 a §:n yhteydessä esitettyihin huomioihin.

Kyberturvallisuuslaki; pykäläkohtaiset huomiot

17 § Poikkeamailmoitusten käsittely

Kyberturvallisuuslain 17 §:än ehdotetaan lisättäväksi uusi 6 momentti, jonka mukaan valvojan viranomaisen velvollisuudesta ilmoittaa salassapitosäännösten estämättä erittäin vakavista kyberturvallisuuspoikkeamista Onnettomuustutkintakeskukselle säädetään turvallisuustutkintalain (525/2011) 16 a §:ssä.

Liikenne- ja viestintäministeriö on turvallisuustutkintalakiin ehdotettujen muutosten kohdalla nostanut esiin useita haasteita erityisesti poikkeaman määrittelyn ja salassapidettävän tiedon luovuttamisen osalta sekä kysymyksen siitä, tulisiko ehdotuksen kattaa myös muut NIS 2 -direktiivin mukaiset valvovat viranomaiset. Esitystä toivotaan tarkennettavan näiltä osin. Sinänsä



perusteltuna voidaan pitää vaihtoehtoa, jossa ilmoitusvelvollisuus voisi olla kyberturvallisuuslain valvovalla viranomaisella.

Lopuksi

Liikenne- ja viestintäministeriö pitää tärkeänä, että kyberturvallisuuspoikkeamien syitä tutkitaan, häiriötilanteista opitaan ja sen myötä uusia poikkeamia voidaan ehkäistä. Erittäin tärkeää on silti myös turvata nykyisellään hyvin toimiva kyberturvallisuuden viranomaisten yhteistyö sekä luottamukseen perustuvat yhteistyö viranomaisten ja yksityisen sektorin välillä.

Turvallisuustutkinnan tarkoitus on yleisen turvallisuuden lisääminen, onnettomuuksien ja vaaratilanteiden ehkäiseminen sekä onnettomuuksista aiheutuvien vahinkojen torjuminen. Turvallisuustutkinnalla on yhteiskunnallista merkitystä sen antamien turvallisuussuositusten kautta ja siten Onnettomuustutkintakeskuksella voi olla tärkeä rooli kyberturvallisuuspoikkeamien turvallisuustutkinnassa. Tärkeää on kuitenkin tunnistaa jatkovalmistelussa kyberturvallisuuspoikkeamien ero fyysisen maailman onnettomuuksiin ja vaaratilanteisiin.

Hallituksen esityksen poikkihallinnollisella jatkovalmistelulla voitaisiin varmistaa toimiva ratkaisu vakavien kyberturvallisuuspoikkeaminen turvallisuustutkinnalle. Jatkovalmisteluun olisi tärkeää ottaa mukaan kaikki keskeiset ministeriöt ja toimijat. Näin varmistettaisiin yhteinen ymmärrys kyberturvallisuuden viranomaiskentän toiminnasta sekä valittujen sääntelykeinojen toimivuus.

Turvallisuustutkintalain kehittäminen siten, että poikkeuksellisen vakavia ja laajamittaisia haitallisia vaikutuksia aiheuttavat merkittävät poikkeamat voitaisiin tarvittaessa tutkia voi tuoda yhteiskunnallista hyötyä turvallisuussuositusten kautta. Liikenne- ja viestintäministeriön katsoo sen kuitenkin edellyttävän, että:

- poikkeaman määritelmä on riittävän selkeä ja ilmoittamisen kynnyks on riittävän korkea.
- tutkinta on jälkikäteistä tutkintaa eikä kohdistu käynnissä olevaan häiriötilanteeseen, jolloin estetään lisähaittojen syntyminen ja turvataan muille viranomaisille mahdollisuus rajata ja estää vahinkoja.
- tiedonsaantioikeuksiin liittyvät säännökset eivät vaaranna kyberturvallisuuskeskuksen luottamuksellisuuteen ja vapaaehtoisuuteen perustuvaa, maailmanlaajuisestikin korkeatasoista toimintaa eivätkä perustuslaissa ja EU:n oikeudessa turvattua viestinnän luottamuksellisuutta.
- tutkinnassa huomioidaan turvallisuusluokitellua ja salassapitoa koskevat säännökset ja niistä aiheutuvat turvallisuusluokitellun tiedon käsittelyvaatimukset ja niiden suojaamisesta aiheutuvat kustannukset.
- turvallisuustutkintalain ilmoittamisvelvollisuutta ei sovelleta, jos tiedon luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin siihen liittyvää tärkeää etua.
- tutkinta ja julkistettava tutkintaselostus eivät vaaranna kansallista turvallisuutta.



Euroopan unionin merionnettomuustutkintadirektiivin kansallisesta täytäntöönpanosta johtuvat turvallisuustutkintalakiin ehdotetut muutokset ovat perusteltuja eikä niiden osalta ole huomioitavaa.

Liikenne- ja viestintäministeriö osallistuu mielellään esityksen jatkovalmisteluun.

Timo Kievari

Osastopäällikön sijainen

Mari Starck

Hallitusneuvos

VN/27546/2023-LVM-23

Seuraavat henkilöt ovat allekirjoittaneet tämän asiakirjan sähköisesti /

Följande personer har undertecknat denna handling elektroniskt /

This document has been signed electronically by the following persons: