Eduskunnan hallintovaliokunta

Poliisihallituksen asiantuntijalausunto asiassa HE 57/2024 vp Hallituksen esitys eduskunnalle kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi

1 Lausuntopyynnöstä

Eduskunnan hallintovaliokunta on pyytänyt Poliisihallituksen asiantuntijalausuntoa ja asiantuntijan kuulemista asiassa HE 57/2024 vp Hallituksen esitys eduskunnalle kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi. Poliisihallituksen asiantuntijalausunnossa on huomioitu Keskusrikospoliisin Poliisihallitukselle toimittaman lausunnon pääkohdat.

2 Yleistä

NIS2 direktiivi ja sen täytäntöönpanoa tukeva lainsäädäntö on valmistelu vastaamaan kybertoimintaympäristön kasvaviin uhkiin mm. tehostamalla tiedonvaihtoa viranomaisten sekä yritysten välillä ja lisäämällä velvollisuuksia ilmoittaa haitallisista kybertapahtumista ja tätä kautta vahvistaa kyberturvallisuutta etenkin yhteiskunnan toiminnan kannalta keskeisillä aloilla. Lainsäädännön valmistelussa on huomioitu kyberturvallisuuden parantaminen ensisijaisesti kyberturvallisuus ja tietosuojaviranomaisten toiminnan kautta ja jossain määrin sivuutettu kyberrikollisuuden yhteiskunnalle aiheuttamat haitat ja niiden torjunta. Lausunnon pykäläkohtaisissa huomioissa nostetaan esiin myös ehdotetun täytäntöönpanolainsäädännön direktiivin vaatimuksia laajempi ulottuvuus, jota voi olla joissain tapauksissa tarpeen tarkastella.

Hallituksen esityksen sivulla 61 todetaan, että lainsäädännössä kansallista liikkumavaraa ei käytetä NIS2-direktiivin soveltamiseksi paikallistason julkishallinnon toimijoihin tai opetus- ja koulutusalan laitoksiin. Poliisihallitus nosti tähän kokonaisuuteen liittyvän haasteen esille jo hallituksen esityksen luonnoksen kommentoinnissa, joka tapahtui ennen Helsingin kaupunkiin ja mm. sen opetustoimen tietoihin kohdistunutta tietomurtoa. Kyseisellä tietomurrolla vaikutettiin kymmeniin tuhansiin kansalaisiin ja sen ennalta estäminen liittyi mitä suurimmassa määrin kyberturvallisuuteen. Mikäli NIS2 direktiivin täytäntöönpanoa koskevassa lainsäädännössä ei ole mahdollista

huomioida paikallishallinnon toimijoita, niin näiden toimijoiden velvollisuudet sekä kyberturvallisuuden ja poikkeamien tiedonjakaminen olisi varmistettava muilla keinoin, jotta haitallisia kyberrikoksia voidaan ennalta estää ja selvittää.

3 Pykäläkohtaiset huomiot kyberturvallisuuslakiin

3.1 17 § Poikkeamailmoitusten käsittely

Pykälän 3 momenttiin kirjattu valvontaviranomaisen velvollisuus ilmoittaa poliisille tapahtumista, joissa on syytä epäillä rikosta, voidaan pitää hyvänä muutoksena. Suuri osa kyberympäristön tahallisista teoista on kyberrikoksia, jolloin on luontevaa, että valvovalla viranomaisella on velvollisuus ilmoittaa törkeistä tieto- ja viestintärikoksista poliisille. Asetettu kynnys epäillyistä rikoksista ilmoittamisen velvollisuudelle on oikealla tasolla, eli ilmoitusvelvollisuus koskee tapahtumia, joissa on syytä epäillä rikoksia joiden enimmäisrangaistus on vähintään kolme vuotta vankeutta. Sen sijaan ilmoitusvelvollisuuden perusteena olevaa *syytä epäillä rikosta* -muotoilua tulisi harkita, jotta ilmoitusta käsittelevältä henkilöltä ei edellytettäisi oikeudellista harkintaa sen osalta, ylittyykö kyseisessä teossa syytä epäillä rikosta -kynnys vai ei. Samalla on kuitenkin todettava, että vastaavaa muotoilua on käytetty myös laissa sähköisen viestinnän palveluista (917/2014) 316 §:ssä, jossa säädetään liikenne- ja viestintäviraston oikeudesta saada viestintää koskevia tietoja. Mikäli edellä mainittua lainkohtaa muutettaisiin, niin syytä epäillä rikosta -ilmaisun sijaan voitaisiin käyttää ilmaisua, *voidaan olettaa rikoksen tapahtuneen.* Sama ilmaisu on käytössä myös esitetyn lain 16 §:ssä, jonka muuttamista tulisi vastaavasti harkita. Poliisin ja muiden toimijoiden välisissä keskusteluissa on noussut esiin huoli siitä, että julkishallinnon ja yksityisen sektorin toimijoilla voi olla vaikeaa arvioida, mitä syytä epäillä -ilmaisulla tarkoitetaan ja miten sitä tulisi arvioida suhteessa havaittuun tapahtumaan.

3.2 20 § CSIRT-yksikön tehtävät

Lainkohdassa säädettäisiin CSIRT-yksikön tehtävistä ja sen 1 momentin 4. kohdassa uhkatietojen ja tietoturvaloukkausten tietojen käsittelystä. Tätä kohtaa on perustelu esityksen sivun 179 toisessa kappaleessa, jossa on todettu, että *yksikön tehtävänä olisi kerätä ja analysoida uhkatietoja ja tietoturvaloukkausten tutkintaa koskevia tietoja eli forensisia tietoja.* Poliisin osalta forensisten tietojen käsittelyssä puhutaan laissa säädetyn laite-etsintään liittyvästä toiminnasta ja sen osalta on säädetty oma toimivaltuus, jota käytetään myös silloin kun kyseessä on asianomistajan suostumuksella tehtävästä toimenpiteestä kuten tässäkin yhteydessä CSIRT-yksikön toiminnassa. Olennaista on se, että toiminnassa voidaan käsitellä laajastikin viestinnän liikennetietoja.

Vastaava havainto liittyy 4 momentissa säädettyyn tietoturvaloukkausten havainnointipalveluun. Vaikka palvelu perustuu vapaaehtoisuuteen, mikäli se

käytännössä kuitenkin mahdollistaa CSIRT:lle suhteellisen itsenäisen pääsyn esimerkiksi liikennetietoihin palvelun ollessa säännöksen mukaan reaaliaikaista tai lähes reaaliaikaista, ilman, että toimija itse viestinnän osapuolena seuloo ja toimittaa tiedot CSIRT:lle. Pykälässä olisi tarpeen tuoda esiin, onko kyse tiedon luovuttamisesta vai reaaliaikaisesta pääsystä tietoon. Poliisin osalta reaaliaikainen tietoon pääsy tarkoittaa käytännössä tuomioistuimen myöntämää lupaa suorittaa telekuuntelua laissa säädettyjen rikosten ennalta estämiseksi, paljastamiseksi tai selvittämiseksi, joten kyseessä on varsin merkittävästä toimenpiteestä.

3.3 21 § Yleisten viestintäverkkojen ja tietojärjestelmien verkkopohjainen haavoittuvuuskartoitus

Pykäläkohtaisessa perustelussa sivulla 180 on kerrottu, että 21 §:llä pantaisiin täytäntöön NIS2-direktiivin 11 artiklan 3 kohdan 1 alakohdan e-luetelmakohdassa ja saman artiklan 3 kohdan 2 alakohdassa CSIRT-yksiköille säädetyt tehtävät. Viitatussa direktiivin kohdassa lukee seuraavasti:

> e) suorittaa keskeisen tai tärkeän toimijan pyynnöstä asianomaisen toimijan verkko- ja tietojärjestelmien ennakoiva skannaus sellaisten haavoittuvuuksien havaitsemiseksi, joilla voi olla merkittävä vaikutus;

Esitetyssä 21 §:ssä ei kuitenkaan säädetä pääsääntönä siitä, että haavoittuvuuskartoitus tehtäisiin keskeisen tai tärkeän toimijan pyynnöstä ja sen vuoksi kyseessä on merkittävä laajennus direktiivissä kuvattuihin CSIRT-yksikön tehtäviin. Pykälän 4 momentissa säädettäisiin pyynnöstä tehtävistä toimenpiteistä, jotka kuitenkin poikkeaisivat 1-3 momentissa säädetystä tavanomaisesta menettelystä. Edellä olevasta johtuen ns. *ei intrusiivinen* haavoittuvuuskartoitus voitaisiin tehdä viestintäverkon tai tietojärjestelmän haltijan suostumuksetta ja tietämättä. Kyse on merkittävästä viranomaisen toimivaltuudesta, jolla voi olla vaikutusta kolmannen tahon tietojärjestelmiin ja luottamukselliseen viestintään. Vähimmillään pykälää olisi muutettava siten, että sinänsä kannatettava haavoittuvuuskartoitus perustuu kohteena olevan verkon tai tietojärjestelmän haltijan suostumukseen, jolloin voidaan selvittää myös viestinnän luottamuksellisuuden suojaan liittyvät kysymykset. Koska haavoittuvuuskartoituksen yhtenä tarkoituksena on pykälän mukaan varoittaa asianomaisille tahoja tietoturvaa vaarantavista seikoista, niin kartoituksesta olisi sovittava verkon tai tietojärjestelmän haltijan kanssa.

Kyseessä olisi säädetty oma-aloitteinen toimivaltuus, joka on laajempi ja yleisempi kuin NIS 2 direktiivin soveltamisala, koska se koskee yleisesti koko viestintäverkkoa ja kaikkia tietojärjestelmiä eikä rajaudu tiettyihin toimijoihin tai toimialoihin. Kyseessä vaikuttaisi olevan siten yleinen haavoittuvuuskartoitustoimivaltuus eikä direktiivin rajaama toimivaltuus. Perusteluissa ei ole kuvattu sitä, miksi tällainen kansallinen laajennus on tarpeen. Viitatun direktiivin kohdan mukaan, vain 4 momentin mukainen haavoittuvuuskartoitus vaikuttaisi olevan direktiivin edellyttämää

Haavoittuvuusskannauksen tuloksena voidaan saada varsin yksityiskohtaista tietoa luottamuksellisesta viestinnästä, mutta laissa ei säädettäisi kenellä olisi oikeus tehdä päätös haavoittuvuusskannauksesta tai kenellä olisi sellaisen toteuttamiseen oikeus. Koska kyseessä voi olla varsin merkittävästäkin luottamuksellisen viestinnän suojaan kajoavasta toimenpiteestä olisi syytä vähimmillään säätää siitä, millä virkamiehellä on oikeus tehdä päätös ja kenellä on toimenpiteen suorittamisen oikeus kuten on toimittu rikostorjunta- tai tiedusteluviranomaisten osalta heidän tiedonhankintaa koskevassa lainsäädännössä. Haavoittuvuuskartoituksesta päättävällä taholla ja sen suorittajalla tulisi olla virka-aseman lisäksi riittävä perehtyneisyys asiaan liittyvään lainsäädäntöön ja suoritettavaan toimenpiteeseen.

Pykäläkohtaisessa perustelussa (sivu 181 viimeinen kappale) sallituksi menetelmäksi on kuvattu esimerkiksi oletuskäyttäjätunnuksen ja salasan yhdistelmän kokeileminen, mutta ei tämän jälkeen jatkuvat toimenpiteet järjestelmässä. Poliisihallitus kiinnittää huomiota rikoslain (39/1889) 38 luvun 8 §:n tietomurtoon, jonka teonkuvaus on seuraava.

> Joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa, taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava *tietomurrosta* sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Vaikka tunnusmerkistöön liittyy oikeudeton tunkeutuminen, niin esitetty lainsäädäntö ei kuitenkaan välttämättä poistaisi tunkeutumisen oikeudettomuutta. Tietoverkkodirektiivissä (2013/40/EU) 2 artiklan d-kohdassa oikeudettomuus määritelty seuraavasti

> d) ilmaisulla ’oikeudettomasti’ tässä direktiivissä tarkoitettua toimintaa, mukaan lukien järjestelmään tunkeutuminen, sen häirintä tai tietojen hankkiminen, johon ei ole järjestelmän tai sen osan omistajan tai muun oikeudenhaltijan lupaa tai joka ei ole sallittua kansallisen lain nojalla

CSIRT-yksikön oikeudesta tunkeutua järjestelmään esimerkiksi oletuskäyttäjätunnusta ja salasanaa käyttäen tulisi säätää lainsäädännössä tai lainkohtaa koskevia perusteluita tulisi muuttaa ja poistaa esimerkki (sivu 181), jossa järjestelmään tunkeutuminen oletustunnuksia käyttämällä mahdollistetaan ei intrusiivisena toimenpiteenä.

Kuten aiemmin on todettu, niin suostumus haavoittuvuusskannaukseen tietojärjestelmän tai verkon haltijalta olisi oleellinen seikka myöskin teon rangaistavuuden poistamisen osalta.

Käsiteltävien tietojen osalta ehdotuksessa todetaan, että haavoittuvuuskartoituksessa ei olisi sallittua käsitellä viestintäverkkoon tai tietojärjestelmään tallennettua henkilötietoa. Kun viestintä sisältää useimmiten esimerkiksi ip-

osoitteen, joka useassa yhteydessä on henkilötietoa, niin haavoittuvuuskartoituksen suorittaminen käytännössä voisi olla hankalaa tai mahdotonta siten, ettei toiminnassa käsiteltäisi henkilötietoja.

Onko näin laaja toimivaltuus ja sen vaikutukset riittävästi arvioitu? Laissa ei ole asetettu toimivaltuuden käytölle tai valvonnalle myöskään mitään menettelyllisiä vaatimuksia tai takeita (päätöksenteko, dokumentointi, ilmoittaminen, suostumuksen merkitys, valvonta, raportointi). Sama päätöksentekijää koskeva huomio liittyy myös 28 §:ssä säädettyyn tiedonsaantioikeuteen, johon liittyen ei ole säädetty siitä, kuka voi pyytää varsin laajastikin salassa pidettäviä tietoja eri tahoilta.

3.4 25 § CSIRT-yksiköllе vapaaehtoisesti luovutettu tieto

CSIRT-yksikölle vapaaehtoisesti luovutettua tietoa ei saisi käyttää tiedon luovuttajaan kohdistuvassa rikostutkinnassa eikä hallinnollisessa tai muussa tiedon luovuttajaan kohdistuvassa päätöksenteossa ilman tiedon luovuttaneen suostumusta (s. 188) Kysymys ei olisi tietoon pääsystä, vaan tiedon käyttämisestä. Käytännön esimerkki voisi olla tilanteesta, jossa joku luovuttaa tiedon merkittävään tietomurtoon liittyvästä tapahtumasta, jossa henkilön tai yrityksen oma toiminta on johtanut tietomurtoon. Koska pykälässä tai sen perusteluissa ei ole avattu sitä, keneen tiedon käytön suoja ulottuisi, on pykälä huonosti muotoiltu ja täytyisi muuttaa ensimmäiseksi tämän kohdan osalta. Lainsäädännön tarkkarajaisuus edellyttää vähimmillään sitä, että tiedon käyttämisen suojaa saava taho pystytään määrittelemään.

Muu päätöksenteko perustelu voi käytännössä tarkoittaa mitä tahansa, joka tarkoittaisi esimerkiksi sitä, että kansallisen turvallisuuden viranomaiset eivät voisi hyödyntää heillä olevaa tietoa esimerkiksi turvallisuusselvitysmenettelyssä, joka on hallinnollista päätöksentekoa.

Perusteluista ei ilmene luottamuksellisuuden suhteen vaatimuksen perusteluita eikä kansallista tai kansainvälistä tutkimusta asiasta ole esitetty, vaan väite luottamuksellisen suhteen muodostumisesta tätä kautta jää vain arvailujen varaan.

Ehdottomasti, vähintään hyödyntämiskiellon tulisi olla väistyvä ja siten harkinnanvarainen rikoksen vakavuuden perusteella. Esimerkiksi valvovan viranomaisen ilmoituskynnys poliisille on tässä lakiehdotuksessa asetettu rikoksiin, joista voi seurata kolme vuotta vankeutta ja tämä kattaa tieto- ja viestintärikosten törkeät tekomuodot.

3.5 Muita huomioita ehdotetusta lainsäädännöstä

3.6 Salaus

Kansallista lainsäädäntöä valmisteltaessa ei ole tuotu käsittelyyn NIS2-direktiivin (98) täsmennystä salaukseen liittyen. Resitaalissa tuodaan esiin päästä päähän tapahtuvan salauksen merkitys viestinnän luottamuksselli-

suudelle, mutta samalla huomioidaan jäsenvaltioiden oikeus varmistaa keskeisten turvallisuusetujensa ja yleisen turvallisuuden suojelu ja mahdollistaa rikosten ennalta estäminen, tutkiminen, paljastaminen ja rikoksiin liittyvät syytetoimet unionin oikeuden mukaisesti.

3.7 Lain voimaantulo

Poliisihallitus kiinnittää huomiota siihen, että vaikka NIS2 direktiivin osalta jäsenvaltioiden on saatettava vaaditut muutokset voimaan direktiivissä säädetyssä aikataulussa, niin eri toimijoille on taattava mahdollisuus tosiasiallisesti toteuttaa direktiivissä ja lainsäädännössä säädetyt toimet.

3.8 Vaikutukset poliisin resursseihin

Kuten kohdassa 3.1 on todettu kyberturvallisuuslain 17 §:n poikkeamailmoituksissa valvontaviranomaisen velvollisuus on ilmoittaa poliisille törkeistä tieto- ja viestintärikoksista. Vastaavaa ilmoitusvelvollisuutta ei ole voimassa olevassa lainsäädännössä ja tässä vaiheessa muutoksen resurssivaikutuksia poliisiin on vaikea arvioida. Muutoksen arvioidaan lisäävän jonkin verran poliisin tietoon tulevia vakavia tietoverkkorikoksia ja rikoksiin liittyvä rikosilmoitusten kirjaaminen, esikäsittely ja esitutkinta tulevat sitomaan poliisin resursseja. Vakavien tietoverkkorikosten esitutkinta vaatii erityistä asiantuntemusta ja esitutkinta on usein pitkäkestoista, jonka vuoksi on oletettavaa, että ko. ilmoitusvelvollisuuden pysyvä resurssivaikutus poliisiin on muutama henkilötyövuosi.

Poliisitarkastaja Kimmo Ulkuniemi

Asiakirja on sähköisesti allekirjoitettu asianhallintajärjestelmässä. Poliisi 03.09.2024 klo 20:59. Allekirjoituksen oikeellisuuden voi todentaa kirjaamosta.