Tuomioistuinvirasto
Domstolsverket

Lausunto

29.11.2023

TIV/1008/2023

Asia: VN/18157/2023

Lausuntopyyntö: luonnos hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Luonnoksessa hallituksen esitykseksi ehdotetaan säädettäväksi laki kyberturvallisuuden riskienhallinnasta, jossa säädettäisiin kyberturvallisuuden riskienhallinta- ja raportointivelvoitteista. Julkishallinnon osalta velvoitteista säädettäisiin lisäksi julkisen hallinnon tiedonhallinnasta annetussa laissa. Tuomioistuinvirasto kiittää mahdollisuudesta lausua tästä lakikokonaisuudesta.

Kyberturvallisuudella tarkoitetaan ulkopuolisen toimijan aiheuttamia turvallisuusuhkia, jotka kohdistuvat tietojärjestelmiin ja -verkkoihin. Kysymys on tärkeästä turvallisuuden osa-alueesta, mutta näiden uhkien tarkastelu muista riskeistä irrallaan on omiaan sirpaloittamaan riskienhallintaa ja heikentämään riskienhallinnan vaikutusta. Kyberuhkien ylikorostaminen saattaa johtaa siihen, että, että varoja ja toimintaa käytetään epätarkoituksenmukaisesti kyberuhkien minimoimiseen, vaikka kokonaisvaltaisemmin asiaa tarkasteltuna riskienhallinnan resursseista saataisiin suurempi hyöty toisaalla.

NIS2 direktiivi ja sen implementoinnin vaatimukset voivat johtaa suurin investointitarpeisiin sekä kustannusten merkittävään nousuun organisaatioissa. Kustannuksia aiheuttavan muun muassa vanhoihin järjestelmiin tehtävät muutokset sekä lisääntynyt tarve järjestää järjestelmien ylläpitoon virka-ajan ulkopuolista päivystystä. Julkishallinnon tietojärjestelmäpalveluita tuotetaan tyypillisesti ostopalveluina ja on ilmeistä, että vaatimusten implementointi tulee kertautumaan toimitusketjun eri vaiheissa.

Soveltamisalaa koskevat huomiot

Lain pohjalla olevassa NIS2 direktiivissä todetaan, ettei lakia sovelleta oikeuslaitokseen (HE s. 11 ja direktiivi). Lausunnolla olevassa ehdotetussa lakitekstissä ja hallituksen esityksen perusteluissa tuomioistuinten rajaaminen lain soveltamisalan ulkopuolelle on tehty hyvin epäselvästi.

Tiedonhallintalain muutosta käsitellään muun muassa sivulla 157, jossa mainitaan, ettei koko lukua 4a sovelleta tuomioistuimiin. Tämä ei kuitenkaan ilmene ehdotetusta 3§:stä (s.229) tai sen perusteluista.

Valittu sääntelytapa, jossa tiedonhallintalain 4 a luvun soveltaminen sidotaan siihen, että onko kysymyksessä tiedonhallinlain 4 §:n 1 momentin 1 kohdan mukaisesta valtion virastosta tai laitoksesta, on tarpeettoman vaikeaselkoinen. Tuomioistuinvirasto ehdottaa, että tuomioistuinten jäämisestä lain soveltamisalan ulkopuolelle säädettäisiin yksiselitteisesti, joko nyt ehdotetun tiedonhallintalain 3 §:n 2 momentissa tai nimenomaisesti tuomioistuimia koskevassa 3 §:n 4 momentissa. Tämä poikkeus tuomioistuinten osalta tulisi myös olla mainittuna esitetyn lain 4§:ssä.

Soveltamisalan kohdalla on syytä pohtia myös sitä, miten soveltamisalan rajoitukset heijastuvat niihin tahoihin, jotka tarjoavat palveluita soveltamisalan ulkopuolelle jääville toimijoille. Tuomioistuinviraston tehtävänä on muun ohessa ”huolehtia tuomioistuinten tietojärjestelmien ylläpidosta ja kehittämisestä” (Tuomioistuinlain 19 a luvun 2 §:n 2 mom.) Tuomioistuinvirasto vastaa siis muun muassa tuomioistuinten lainkäyttötehtävissä hyödynnettävien asianhallintajärjestelmien ylläpidosta ja kehittämisestä. Hallituksen esityksen perusteella jää epäselväksi, mikä vaikutus direktiivin mukaisella soveltamisalan rajauksella on Tuomioistuinviraston toimintaan tuomioistuinten tietojärjestelmien kehittäjänä ja ylläpitäjänä. On todettava, että lopputulos olisi erikoinen, jos Tuomioistuinviraston katsottaisiin kuuluvan lain soveltamisalaan, mutta tuomioistuimet rajattaisiin sen ulkopuolelle. Käytännössä lopputulos olisi se, että direktiivin mukainen soveltamisalan rajaus menettäisi Suomessa suuren osan merkityksestään, koska kyberuhat kohdistuvat nimenomaan tietojärjestelmin ja aiemmin kerrotulla tavalla tuomioistuimet itse eivät huolehdi käyttämiensä tietojärjestelmien ylläpidosta tai kehittämisestä. Tuomioistuinviraston lisäksi kysymys tuomioistuimia koskevan soveltamisalan rajoituksen heijastusvaikutuksesta on merkityksellinen tuomioistuimille palveluita tuottavien Oikeusrekisterikeskuksen ja Valtion tieto- ja viestintätekniikkakeskus Valtorin kannalta.

Nyt ehdotetun lain ”toimijoiden” osalta on myös syytä selkeyttää niiden suhdetta sähköisestä viestinnän palveluista annettuun lakiin (917/2014). Jo nykyisellään sähköisen viestinnän palveluista annetun lain mukaiset toimijoiden määritelmät aiheuttavat osin tulkinnanvaraisuutta sen suhteen, että kuka (SVPL 4 §:n 30, 36 ja 41 alakohta) ja millä edellytyksillä sekä mihin käyttötarkoitukseen (SVPL 136 - 138 §:t, 272 § vs. 18 luku) voi käsitellä sähköisen viestinnän tietoja (mm. sisältö- ja välitystietoja). On syytä huomata, että sähköisen viestinnän palvelulakia pidetään erityislakina suhteessa yleiseen tietosuojasääntelyyn, joten nyt ehdotetussa lain kyberturvallisuuden riskienhallinnasta 5 §:n 3 momentin mukainen maininta ”Henkilötietojen käsittelyn tietoturvallisuudesta säädetään yleisessä tietosuoja-asetuksessa ja tietosuojalaissa (1050/2018)” ei välttämättä vielä yksinään ole riittävä sähköisten viestinnän tietojen käsittelyyn. Käsittelytarpeisiin liittyvää kokonaisuutta on peilattava henkilötietojen suojan ohella viestinnän luottamuksellisuutta koskeviin vaatimuksiin, joista usein tulee vielä korkeampi kynnys kyseisten tietojen käsittelylle. Tämän ohella on huomioitava se, että toimijan ollessa mahdollisesti myös työnantajan roolissa, laki yksityisyyden suojasta työelämässä (759/2004) voi asettaa omia reunaehtojaan. Olennaista tässä yhteydessä on varmistaa, ettei nyt eri lainsäädännöistä tulevat vaatimukset, toimintamahdollisuudet ja erilaiset roolitukset johda siihen, että viestinnän luottamuksellisuutta ja henkilötietojen suojaa koskevien perusoikeuksien toteutuminen vaarantuu sääntelyn monimutkaisuuden ja tulkinnanvaraisuuden johdosta.

Todettakoon jo nyt, että nyt sääntelyn kohteena oleva lainsäädäntökehikko on poikkeuksellisen monimutkainen, kun huomioidaan nyt annettavan lain ohella sähköisen viestinnän palveluista annetun lain, tiedonhallintalain sekä tietosuojasääntelyn mukaiset vaatimukset. Kyseiset lait sisältävät monelta osin myös hyvin samankaltaista, jopa päällekkäiseltä vaikuttaa sääntelyä, mutta

jokaisessa laissa samoista toimijoista käytetään eri nimiä ja samankaltaiset toimintavaatimukset koskevat nimenomaisen sääntelyn kohteena olevaa kontekstia. Riskinä tällaisessa sääntelyssä on, että päällekkäiset vaatimukset johtavat ristiriitatilanteisiin lakien kesken. Lainsäädännön vaikeaselkoisuus aiheuttaa myös merkittävää hallinnollista taakkaa sitä soveltaville organisaatioille.

Lainsäädäntökehikon osalta on syytä vielä huomata, että viime kädessä tietosuojasääntelyllä on EU-oikeudellinen etusijaisuus suhteessa mahdolliseen direktiivipohjaiseen (nyt ehdotettu laki, SVPL) tai pelkkään kansalliseen ratkaisuun pohjautuvaan sääntelyyn (tiedonhallintalaki). Tämän vuoksi nyt ehdotetussa sääntelyssä tulee pyrkiä ennen kaikkia siihen, että se on mahdollisimman yhteensopiva ja yhdenmukainen (esim. soveltamisalarajaukset kts. tietosuoja-asetus 2 art.) tietosuojasääntelyn kanssa.

Kokoavasti voidaan todeta, että hallituksen esityksen perusteella ei muodostu selkeää kuvaa eri säännösten keskinäisistä suhteista ja niistä muodostuvasta kokonaisuudesta. Lopputuloksena on, että julkisen hallinnon toimijan on vaikea parhaallakaan tahdolla hahmottaa kaikkia toimintaan kohdistuvia vaatimuksia, kun samaa asiaa käsitellään eri tavalla eri säännöksissä. Vaarana on, että sekavuus tulee tulevaisuudessa vain lisääntymään, kun lainmuutoksia tehdään pirstaleisesti ja ilman riittävää kokonaiskoordinaatiota.

Riskienhallintavelvoitetta koskevat huomiot

Yleinen velvoite viranomaiselle huolehtia riittävästä riskienhallinnasta on kuvattu useassa, jo voimassa olevassa laissa. Tämä esityksessä oleva laki poikkeaa näistä niiltä osin, että muissa ei ole yksityiskohtaisesti kerrottu mitä riskienhallinta tulisi käsittää. Tällainen lista voi johtaa toiminnan keskittymistä vain esitetyn listan mukaisiin asioihin.

Esityksessä puhutaan, että riskienhallinnalla tulisi huomioida ”kaikki” vaaratekijät. Tällainen absoluuttinen ajattelu on riskienhallinnalle vierasta, kun itse asiassa tulisi nimenomaan keskittyä oleelliseen. Herää myös kysymys, että mikäli poikkeama tapahtuu, organisaatio ei ole huomioinut ”kaikkia” vaaratekijöitä. Esityksen sivulla 119 on listattuna laajasti alueita, joiden osalta tulisi siis ”kaikki” miettiä. Tässä herää kysymys, miksi yleensä puhua tässä kyberriskienhallinnasta, kun oikeammin voisi puhua riskienhallinnasta ja turvallisuudesta ilman etuliitteitä.

Vaatimukset riskienhallintatoimenpiteille kaikkiin tietojärjestelmiin ja tiedonkäsittelylaitteisiin lausunnolla olevassa lakiluonnoksessa kuvattavalla tavalla tulee huomattavasti lisäämään tarvetta muutoksiin sekä järjestelmissä että niiden käytössä, mutta myös asiaan liittymättömissä toiminnoissa. Näitä kustannusvaikutuksia on mahdotonta ennalta arvioida, mutta tällaisten muutosten toteuttaminen lisää sekä tietotekniikan että toiminnan kustannuksia.

5§ (sivu 115) ”Tällaiset velvoitteet voivat sisältää esimerkiksi ehdotettuun lakiin verrattuna yksityiskohtaisempia säännöksiä riskienhallinnassa huomioitavista osa-alueista, edellyttää tietyn standardin tai sertifioinnin käyttämisestä.”. Velvoittavalla sertifioinnilla tai jonkun määrätyn standardin pakollisella noudattamisella ei de facto voida sanoa olevan turvallisuutta lisäävää vaikutusta, vaan voi ennemmin olla omiaan aiheuttamaan turhia kustannuksia, kun toimenpiteitä tehdään vaatimukset edellä ”rasti ruutuun” periaatteella. Riskien odotettujen vaikutusten merkityksen tulisi olla keskeisin peruste toteutettaessa suojaavia toimenpiteitä, ei jonkin standardin tai viitekehyksen luettelo.

Raportointivelvoitetta koskevat huomiot

Raportoinnista ja sen vaikutuksesta toimintaan (mm. sopimukset):

Organisaation tulisi esityksen mukaisen lain mukaan reagoida, lähettämällä raportti poikkeamatapauksesta valvovalle viranomaiselle 24 h sisällä siitä, kun on saanut merkittävästä poikkeamasta tiedon. Organisaation tulisi sitten antaa lisätietoa poikkeamasta 72 h sisällä tiedon saannista. Nämä aikarajat eivät riipu siitä, koska tieto poikkeamasta on saatu.

Näin ollen ehdotetun lain mukanaan tuomat raportointivaatimukset tulevat aiheuttamaan uusia vaatimuksia niin toimiville organisaatioillekin kuin sopimusten kautta heidän palveluntarjoajien ja alihankkijoiden sopimuksiin. Tämä tarkoittaa päivystystä tai varallaoloa ja valmiutta tehdä ilmoituksia tietoon tulleista tapauksista. Sopimuksissa tämä tarkoittaa valvonnan ja raportointivelvoitteiden lisäystä sekä palveluntuotannon yksityiskohtaisemman tarkasteluun. Nämä toimenpiteet eivät lisää turvallisuutta mutta tulevat nostamaan palvelujen hintoja.

Tuomioistuinviraston osalta lain soveltaminen tuonee vaatimukset tarvetta muuttaa esimerkiksi Oikeusrekisterikeskuksen ja Valtorin sopimuksia, joihin mainittuja työintensiivisiä aikarajoja ei ole suunniteltu. Raportointivaatimukset tulevat vaatimaan lisääntynyttä kykyä havainnoida poikkeamia, nopeaa reagointi- ja analysointikykyä sekä kykyä raportoida näitä. Kaikkea tätä vaaditaan niin järjestelmän käyttäjiltä ja omistajilta kuin palveluntarjoajiltakin tuotantoketjun kaikilla tasoilla, riippumatta siitä onko toimintaa juuri silloin vai ei. Tällainen vaatii kohotettua valmiustasoa, ja myös vaatimusta järjestää virka-ajan ulkopuolista päivystystä niin virastoissa kuin tietoteknisten palvelujen toimittajissa. Tässä muodossa lailla tulee olla merkittäviä henkilö- ja toimintakustannuksia lisääviä vaikutuksia.

Keskeisen määritelmän epäselvyys:

Lakiehdotuksen 11§ 1 momentti kuuluu: ”Toimijan on ilmoitettava viipymättä valvovalle viranomaiselle merkittävästä poikkeamasta. Merkittävällä poikkeamalla tarkoitetaan poikkeamaa, joka on aiheuttanut tai voi aiheuttaa palvelujen vakavan toimintahäiriön tai asianomaiselle toimijalle taloudellisia tappioita taikka poikkeama on vaikuttanut tai voi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa.”. Tätä keskeistä määritelmää ei ole kirjattuna muiden määritelmien yhteyteen 2§:ään.

Merkittävä poikkeama siis määritellään lakiesityksessä siten, että se käsittää poikkeaman, ”.. jos se on aiheuttanut tai voi aiheuttaa [..] asianomaiselle toimijalle taloudellisia tappioita”. Tiedonhallintalain ehdotetussa lakimuutoksessa mainittu määritelmä on lisätty määritelmiin ja esitetään 3.1§ 25a kohdassa. Siinä edellä mainittu loppuosa on korvattu ”… aiheuttaa viranomaiselle taloudellista tappiota”.

Tämä määritelmä tekee käytännössä kaikista poikkeamista merkittäviä, koska ei ole olemassa poikkeamaa, joka ei jotenkin aiheuttaisi jotain toimenpiteitä eli kustannuksia ja siis taloudellista tappiota. Tämä tuskin lienee tarkoitus.

Kohdistuneiden poikkeamien raportointi moneen suuntaan:

Merkittävien poikkeamien raportointi on lakiesityksessä tehty raskaaksi, mikäli poikkeamalla sattuu olemaan vaikutusta toimintaan ja muihin toimijoihin. Tällöin on määritelty, että raportointiin velvoitettu tulee raportoida poikkeamasta myös kaikille toimijoille, johon poikkeama vaikuttaa sekä myös mahdollisesti ulkomaisiin viranomaisiin. Mikäli organisaatiota on kohdannut oikeasti

merkittävä ongelma, ovat tilanteen hallinta ja korjaustoimet ensisijaisia. Tällöin olisi kohtuullista, että valvova viranomainen hoitaisi raportoinnin jakamista ainakin niiltä osin, kun puhutaan muista valvovista viranomaisista tai esimerkiksi EU:n viranomaisista muissa maissa. Tutustuminen eri maiden ilmoituskohteisiin sekä -tapaan ei ole organisaatiolle tällöin keskeistä.

Valvontaa koskevat huomiot

18j§ (sivu 172) mainitaan että tarkastukseen voisi sisältyä teknisiä toimenpiteitä kuten erilaisia skannauksia. Näin ei laissa tule suoraan määrittää. On huomattava, että kaikki järjestelmään, tietoverkkoon tai järjestelmäympäristöön kohdistuviin muutoksiin, oli ne kuinka pieniä tahansa, tulee kohdistaa etukäteen niitä samoja järjestelmätestejä ja hyväksymisiä ympäristöstä vastaavalta taholta. Erinäisten skannerien tai tietoa keräävän ohjelmakoodin lisääminen ovat myös muutosta ympäristöön. Mikäli skannaus aiheuttaa tai voi aiheuttaa häiriöitä järjestelmän toimintaan tulee ne olla ennakoitavissa ja etukäteen estettävissä. Skannaus ilman, että toimenpiteen hyväksyntä menee normaalin muutoshallinnan menettelyjen mukaan, rikkoo räikeästi muutoshallinnan periaatteita vastaan ja on omiaan lisäämään järjestelmään kohdistuvia riskejä.

Seuraamusmaksua koskevat huomiot

Ei lausuttavaa

CSIRT-yksikön tehtäviä koskevat huomiot

CSIRT yksikön tehtäviin tulisi tarkemmin määrittää myös tarjotun avun laatu sekä nopeampi reagointi poikkeamatilanteissa. Nyt on selkeä epäsuhta raportoinnin ja CSIRT toiminnan välillä, kun raportointi tulee tehtäväksi 24 h kuluessa ja CSIRTiltä edellytetään vastausta sekä apua ongelman hoitamiseen vain virka-aikana. Esimerkiksi kiirastorstain iltana havaittu tapahtuma on jo yli 100 tuntia ”vanha”, kun virka-aika, ja CSIRT toiminta seuraavan kerran alkaa. Tällöin olisi suotavaa, että apua saisi poikkeaman hallintaan alusta lähtien, tai ainakin sen jälkeen, kun ensimmäinen vaadittu ilmoitus ongelmasta on toimitettu.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Ehdotettu tiedonhallintalain 4 a luku saattaa aiheuttaa haasteita sen soveltajille esitetyn lain vaatimusten samankaltaisuuden vuoksi. Samoin viranomaisten voi olla vaikeaa arvioida, milloin soveltavat tiedonhallintalain tietoturvallisuusvaatimuksia ja milloin kyberturvallisuusvaatimuksia tai milloin heidän tulee soveltaa molempia lakeja samanaikaisesti. Olisiko tarpeen myös pohtia sitä, miltä osin on tarpeen täydentää/tehdä muutoksia tiedonhallintalakiin ja miltä osin pitää nämä kaksi lakia ”erillään”, päällekkäisyyden välttämiseksi ja ymmärrettävyyden helpottamiseksi?

Esitetty menettely tulisi, johtuen kokonaisuuden epäselvyydestä, sekoittamaan asioita sekä lisäämään hallinnollista työtä, kun arvioidaan eri asioiden soveltamista.

On syytä myös huolehtia käsitteiden yhdenmukaisuudesta. Mitä enemmän käsitteitä (esim. tietojärjestelmä) tuodaan uusilla määritelmillä lakiin, sitä haastavampaa on niiden soveltaminen sekä ymmärtäminen kussakin kontekstissa.

Turvallisuusluokittelun laajentaminen tuomioistuimiin

Nyt lausunnon kohteena olevassa muutosehdotuksessa ehdotetaan täsmennettäväksi lakia julkisen hallinnon tiedonhallinnasta (906/2019) (myöh. tiedonhallintalaki) 18 §:ä siten, että myös tuomioistuinten on tehtävä jatkossa turvallisuusluokittelua koskevat merkinnät asiakirjoihinsa. Niin hallinto- kuin erityistuomioistuimissa sekä yleisisä tuomioistuimissa sovelletaan oikeudenkäyntiasiakirjojen julkisuus- ja salassapito määrittelyyn ensisijaisesti tuomioistuinten omia julkisuuslakeja (laki oikeudenkäynnin julkisuudesta hallintotuomioistuimissa (381/2007)ja laki oikeudenkäynnin julkisuudesta yleisissä tuomioistumissa (370/2007)) ja vasta toissijaisesti lakia viranomaisten toiminnan julkisuudesta (521/1999) eli niin kutsuttua yleistä julkisuuslakia. Kun turvallisuusluokittelua koskeva määrittely nojaa nimenomaan yleisen julkisuuslain 24 §:n määrättyihin alakohtiin, johtaa nyt ehdotettu täsmennys yhä osin epäselvään lopputulemaan tuomioistuinten osalta, kun säännöksessä ei huomioida tuomioistuinten oikeudenkäyntiasiakirjojen osalta poikkeavaa ja toimialakohtaista julkisuussääntelyä. Näiltä osin ehdotusta tulee täsmentää.

Verkkotunnusvälittäjiä koskevat huomiot

Ei lausuttavaa

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Ei lausuttavaa

Vaikutustenarviointia koskevat huomiot

Organisaation tulisi esityksen mukaisen lain mukaan reagoida, lähettämällä raportti poikkeamatapauksesta valvovalle viranomaiselle 24 h sisällä siitä, kun on saanut merkittävästä poikkeamasta tiedon. Organisaation tulisi sitten antaa lisätietoa poikkeamasta 72 h sisällä tiedon saannista. Nämä aikarajat eivät riipu siitä, koska tieto poikkeamasta on saatu.

Näin ollen ehdotetun lain mukanaan tuomat raportointivaatimukset tulevat aiheuttamaan uusia vaatimuksia niin toimiville organisaatioillekin kuin sopimusten kautta heidän palveluntarjoajien ja alihankkijoiden sopimuksiin. Tämä tarkoittaa päivystystä tai varallaoloa ja valmiutta tehdä ilmoituksia tietoon tulleista tapauksista. Sopimuksissa tämä tarkoittaa valvonnan ja raportointivelvoitteiden lisäystä sekä palveluntuotannon yksityiskohtaisemman tarkasteluun. Nämä toimenpiteet eivät lisää turvallisuutta mutta tulevat nostamaan palvelujen hintoja.

Tuomioistuinviraston osalta lain soveltaminen tuonee vaatimukset tarvetta muuttaa esimerkiksi Oikeusrekisterikeskuksen ja Valtorin sopimuksia, joihin mainittuja työintensiivisiä aikarajoja ei ole suunniteltu. Raportointivaatimukset tulevat vaatimaan lisääntynyttä kykyä havainnoida poikkeamia, nopeaa reagointi- ja analysointikykyä sekä kykyä raportoida näitä. Kaikkea tätä vaaditaan niin järjestelmän käyttäjiltä ja omistajilta kuin palveluntarjoajiltakin tuotantoketjun kaikilla tasoilla, riippumatta siitä onko toimintaa juuri silloin vai ei. Tällainen vaatii kohotettua valmiustasoa, ja myös vaatimusta järjestää virka-ajan ulkopuolista päivystystä niin virastoissa kuin tietoteknisten palvelujen toimittajissa. Tässä muodossa lailla tulee olla merkittäviä henkilö- ja toimintakustannuksia lisääviä vaikutuksia.

Vaatimukset kaiken kattavasta riskienhallintatoimenpiteistä kaikkiin tietojärjestelmiin ja tiedonkäsittelylaitteisiin lain esityksessä kuvattavalla tavalla tulee lisäämään tarvetta muutoksiin sekä järjestelmissä että niiden käytössä. Näitä kustannusvaikutuksia on mahdotonta ennalta arvioida, mutta tällaisten muutosten toteuttaminen lisää sekä tietotekniikan että toiminnan kustannuksia merkittävästi.

Tuomioistuimille tulee kustannusvaikutuksia myös muutostenhakujen kautta. Esitys laiksi 42 §. Muutoksenhaku toteaa, että hallinnollista seuraamusmaksua koskevaan päätökseen olisi oikeus hakea muutosta oikeudenkäynnistä hallintoasioissa annetussa laissa säädetyssä järjestyksessä. (sivu 151). Näiden muutosten käsittelyn kautta aiheutuvat kustannukset eivät ole käsiteltynä lueteltaessa lain aiheuttamia kustannusvaikutuksia.

Muut huomiot ja avoin palaute esityksestä

Nyt ehdotetun sääntelyn perusteella nousee esille esimerkiksi kysymys siitä, että onko riittävää, että poikkeamahavainnosta tehdään vain ilmoitus nyt ehdotetun lain valvovalle viranomaiselle, kun valvovalle viranomaiselle on puolestaan säädetty velvoite tehdä ilmoitus tietosuojavaltuutetulle, jos ilmoitus koskee henkilötietojen tietoturvaloukkausta (laki kyberturvallisuuden riskienhallinnasta 17 § ja 34 §). Tällä hetkellä esimerkiksi henkilötietojen tietoturvapoikkematilanteessa voi nousta tarve tehdä ilmoitus kyberturvallisuuskeskukselle, tietosuojavaltuutetulle ja poliisille sekä nyt ehdotettu laki tuo vielä tähän yhtälöön vielä ”valvovan viranomaisen” ja mahdollisesti EU:n toimijat. Ilmoituksia tekevien organisaatioiden hallinnollisen taakan keventämiseksi nyt ehdotetun sääntelyn yhteydessä olisi syytä myös selvittää edellytyksiä kansalliselle keskitetylle sähköisen asioinnin ”yhden luukun” -palvelulle, jossa poikkeamatilanteesta ilmoittamiseen organisaatio voisi yhdellä kerralla täyttää lakisääteiset ilmoitusvelvollisuutensa eri viranomaisille. Ilmoitustoiminnallisuuden lisäksi tähän kanavaan voisi keskittää toimintaohjeet ”askelmerkkeineen” organisaatiolle poikkeamatilanteen hallinnan ja hoitamisen osalta huomioiden tietosuojan, tiedonhallinnan, tietoturvan ja riskienhallinnan näkökulman. Myös viranomaisten välisiä toimintaprosesseja olisi syytä kehittää siten, että asiakasrajapinta ilmoittajille olisi mahdollisimman yksinkertainen, mutta samalla tehokkaat viranomaisprosessit käynnistävä.

9§ (sivu 120) Lause ” Viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevilla toimintaperiaatteilla tarkoitetaan toimijan näkemystä tietoturvan päämääristä, periaatteista ja toteutuksesta koko elinkaaren ajan.”. Lauseessa jää epäselväksi mitä tai minkä elinkaarta lauseella tarkoitetaan.

Lause sivu 125: Lisäksi on suojauduttava luonnollisilta ja yhteiskunnallisilta tapahtumilta, kuten tulipaloilta, tulvilta ja levottomuuksilta. – miksi tulipalo olisi esimerkki kummastakaan?

Termin auditointi käyttö (esiintyy useasti esityksessä): Esityksessä puhutaan auditoinnista, kun kohdissa tarkoitetaan tarkastusta. Yleensä puhuttaessa auditoinnista on määritelty ennalta arviointikehikko, jota vastaan se suoritetaan. Jos ei kehikkoa ole, on kyseessä tarkastus tai arviointi.

Jaakkola Riku
Tuomioistuinvirasto

Helaskoski Kimmo
Tuomioistuinvirasto