Insta Group Oy

Lausunto

05.01.2021

Asia: VN/24348/2020

Selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; työryhmän väliraportti

Lausunnonantajan lausunto

Ehdotukset poliittisiksi linjauksiksi, kommentit:

Kiitämme mahdollisuudesta lausua työryhmän väliraportista. Insta Group on suomalainen riippumaton yritys, jonka tavoitteena on edistää turvallista digitalisaatiota. Tietoturva- ja tietosuojapalveluidemme asiakkaina on kattavasti kriittisillä toimialoilla toimivia organisaatioita sekä julkiselta että yksityiseltä sektorilta.

Ehdotettu linjaus (1) viranomaisten yhteistoiminnan varmistamisesta on kannatettava ja on tärkeää, että yhteistoiminnalle luodaan toimiva säädöspohja. Pidämme tältä osin tärkeänä, että säädöspohjaa suunniteltaessa otetaan huomioon viranomaisten lisäksi myös yritysten merkittävä rooli sekä kriittisten alojen toimijoina että näille palveluita tuottavina organisaatioina.

Kriittisiä toimialoja koskevien lakisääteisten tietoturvavaatimusten osalta (7) pidämme tärkeänä, että lainsäädännössä otetaan riittävällä tavalla huomioon tietoturvan jatkuva kehittyminen ja varmistetaan, että säädöspohja mahdollistaa vaatimusten päivittämisen ja ajan tasalla pitämisen käytännössä. Vaatimusten on toisaalta myös oltava riittävän selkeitä sekä lainsäädännön että viranomaismääräysten tasolla, ja pidämme tärkeänä, että vaatimuksia täsmennetään tarvittaessa ohjeistuksella. Riskiperusteisen lähestymistavan osalta on syytä varmistaa, että riskien arvioinnille on yhtenäiset kriteerit.

Kansalliseen lainsäädäntöön mahdollisesti tulevia vaatimuksia valmisteltaessa tulee ottaa huomioon myös muu sääntely ja vaatimukset sekä näiden tulkinnat (mukaan lukien EU:n yleinen tietosuoja-asetus ja erityisesti sen 32 artikla sekä finanssialaa koskeva EU:n tuleva DORA-asetus). On välttämätöntä, että eri vaatimusten suhde toisiinsa on selvä. Väliraportissa viitattujen lakisääteisten tietoturvavaatimusten suhde erityisesti ehdotettuun NIS2-direktiiviin ja sen vaatimuksiin jää epäselväksi.

Kyberturvallisuuskeskukselta tietoturvavaatimuksista ennen hyväksyntää pyydettävää lausuntoa koskeva ehdotettu linjaus (8) on väliraportissa epäselvä ja sen sisältöä ja kattavuutta tulee selventää.

Työryhmän ehdottaman linjauksen (12) mukaan kriittisten toimialojen merkittävimpien toimijoiden tulee osoittaa käyttävänsä tietoturvallisuuden hallintajärjestelmää ISO 27001 -sertifioinnilla vuoden 2024 loppuun mennessä. Tältä osin tulee kiinnittää huomiota myös hallintajärjestelmän soveltamisalaan ja siihen, että sertifiointi tosiasiassa kattaa toiminnan riittävän laajasti. Ehdotuksen kattavuuden osalta muotoilu kriittisten toimialojen merkittävimmistä toimijoista on epäselvä.

Ehdotettujen linjausten mukaan sekä Valtorin (22) että kriittisten toimialojen rekisterinpitäjien (29) tulee varmistaa vuoden 2021 loppuun mennessä, että tietosuojaa koskevat vaikutustenarvioinnit on toteutettu siltä osin, kun käsittely todennäköisesti aiheuttaa korkean riskin ihmisten oikeuksille ja vapauksille. Tältä osin kiinnitämme huomiota siihen, että vaikutustenarviointien toteuttaminen näissä tilanteissa on poliittisen linjauksen sijaan rekisterinpitäjille jo nykyisessä lainsäädännössä asetettu velvollisuus.

Ehdotetut linjaukset sisältävät ehdotuksen, jonka mukaan arvioidaan mahdollisuuksia hyväksyä olemassa olevia tietoturvan arviointikriteerejä yleisen tietosuoja-asetuksen mukaisiksi sertifiointikriteereiksi (31). Olemassa olevien määräysten ja kriteerien hyödyntäminen on tietoturvan osalta kannatettavaa, mutta tietosuoja-asetuksen mukaisen sertifioinnin tulee kattaa tietoturvaa koskevien kriteerien lisäksi laajemmin tietosuojan eri osa-alueet, mukaan lukien esimerkiksi tietosuoja-asetuksen 5 artiklan mukaisten periaatteiden toteutuminen.

Ehdotetun mobiilisovelluksen (35) taustalla oleva ajatus ajankohtaisen tiedon jakamisesta ja ilmoitusten tekemisen helpottamisesta on kannatettava. Keskitettyä ilmoituskanavaa eri viranomaisille tulisi harkita etenkin NIS2-direktiiviehdotuksen laajempien ilmoitusvelvollisuuksien myötä. Pidämme kuitenkin epätodennäköisenä, että mobiilisovellus olisi tarkoituksenmukaisin keino esimerkiksi tietoturvaloukkauksista ilmoittamiseen.

Väliraportin muut osat, kommentit:

Pidämme olennaisen tärkeänä, että väliraportissa on tunnistettu, että lakisääteiset velvoitteet ja määräykset eivät yksin takaa riittävää tietoturvan ja tietosuojan tasoa. Käytännössä merkittävää on myös se, millaisina tekijöinä tietoturva ja tietosuoja koetaan ja millainen tietoturva- ja tietosuojakulttuuri organisaatioissa on. Onkin valitettavaa, että väliraportissa on muutoin omaksuttu lähtökohta vastakkainasettelusta tietoturvan ja tietosuojan sekä tehokkaan toiminnan ja esimerkiksi järjestelmien käytettävyyden välillä. Asianmukaisesti toteutettu ja toimintaan sisäänrakennettu tietoturva ja tietosuoja eivät ole toimintaa väliraportissa kuvatulla tavalla hankaloittavia tekijöitä. Hyvää tietoturva- ja tietosuojakulttuuria ei edistä, jos tietoturva ja tietosuoja nähdään ensisijaisesti toimintaa hankaloittavina rajoitteina. Kulttuurin edistämisen kannalta on myös tärkeää, että tietoturvaa ja tietosuojaa ei tarkastella vain tietojärjestelmien näkökulmasta.

On tärkeää, että väliraportissa on tunnistettu, että henkilötietojen suojan osalta tietoturva on vain yksi keino tietojen suojaamiseen ja merkitystä on myös esimerkiksi tietojen minimoinnin periaatteella. Tämä korostaa sitä, että tietoturvan ja tietosuojan parantamisen osalta ei tule keskittyä yksinomaan tekniseen tietoturvaan.

Väliraportissa on tarkasteltu tietoturvaa ja tietosuojaa runsaasti taloustieteellisestä näkökulmasta. Taloustieteellinen lähestymistapa perustuu myös väliraportissa ajatukselle taloudellisesti rationaalisesta toimijasta, joka toimii erilaisten kannustimien ohjaamana. Tietoturvaan ja tietosuojaan liittyvät kannustimet ja seuraukset ovat kuitenkin siinä määrin kompleksisia, että tarkastelutapa jää etäälle käytännöstä. Myös väliraportissa on myöhemmin nostettu esiin esimerkiksi kriittisten toimialojen keskinäisriippuvuuksien merkittävät vaikutukset, ja erityisesti näiden osalta mahdollisten epäsuorien kustannusten arviointi ja huomioon ottaminen on vaikeaa. Negatiivisten kannustinten osalta sanktioiden rooli korostuu, mikä ei kaikissa tilanteissa ole toivottavaa.

Jaamme työryhmän päätelmät siitä, että kriittisten toimialojen tietoturvan ja tietosuojan tasoa voidaan parantaa prosessien ja toimintojen auditoinnilla ja sertifioinnilla. Esimerkiksi ISO 27001 -standardin mukainen asianmukaisesti toteutettu tietoturvan hallintajärjestelmä muodostaa erinomaisen pohjan organisaation tietoturvalle, joskin on tärkeää ottaa huomioon myös standardin rajoitteet ja esimerkiksi vaatimusten yleisluonteisuus, mihin väliraportissa on viitattukin.

ISO 27001 -sertifioinnin kustannusten osalta väliraportissa viitataan opinnäytetyöhön, jossa on pyritty arvioimaan yksittäisen ohjelmistoyrityksen sertifioinnin kokonaiskustannuksia. Kiinnitämme tältä osin huomiota siihen, että väliraportissa mainitut kustannukset ovat tietyllä toimialalla toimivaa yksittäistä yritystä koskevia arvioita, eikä kyse ole sen kaltaisesta tutkimuksesta, josta voitaisiin vetää laajempia johtopäätöksiä kustannuksista yli toimialojen tai yritysten. Kustannuksiin vaikuttaa merkittävästi muun muassa hallintajärjestelmää käyttöönottavan toimijan aiempi tietoturvan kypsyystaso. Kustannusten osalta on myös tärkeää erottaa kustannukset, jotka aiheutuvat itse sertifioinnista niistä tietoturvaan liittyvistä kustannuksista, jotka aiheutuvat riippumatta siitä, onko toimijalla ISO 27001 -standardin mukaista tietoturvallisuuden hallintajärjestelmää. Esimerkiksi henkilötietojen käsittelyn osalta nykyisin voimassa oleva sääntely edellyttää paitsi riskiperusteisesti toteutettua riittävää tietosuojan ja tietoturvan tasoa, myös sen dokumentointia. Huomionarvoista on myös, että ISO 27001 -standardi ei edellytä eri organisaatioilta samanlaista toteutusta, vaan vaatimuksiin kuuluu, että kukin organisaatio arvioi eri hallintakeinojen tarpeellisuutta oman toimintansa ja siihen liittyvien riskien kannalta.

Selvää joka tapauksessa on, että sertifioinnit ja tietoturvan sekä tietosuojan taso parantaminen aiheuttavat kustannuksia. Toisaalta kustannuksia ei tule verrata yksinomaan nykyiseen tasoon, ja huomioon on otettava myös mahdollisten tietoturvaloukkausten aiheuttamat kustannukset ja muut haitat. Huomionarvoista yksityisen sektorin toimijoiden osalta on, että etenkin kansainvälisesti

toimivien kriittisten alojen yritysten ja palveluntarjoajien osalta asiakkaat usein asettavat jo nykyisellään vaatimuksia tai odotuksia sertifioinneista, ja kyse on tältä osin myös kilpailutekijästä.

Pidämme tärkeänä, että väliraportissa oli nostettu esiin yleisen tietosuoja-asetuksen 42 artiklan mukaiset tietosuojasertifioinnit, joiden merkitys toistaiseksi on jäänyt valitettavan vähäiseksi sekä Suomessa että EU:ssa laajemmin. Näemme, että Suomella on tältä osin tilaisuus vaikuttaa tietosuojasertifiointien osalta myös EU:n laajuisesti.

Väliraportissa ei erikseen ollut käsitelty tietoturvaan ja tietosuojaan liittyvien häiriötilanteiden harjoittelua. Pidämme tärkeänä, että työryhmän jatkotyössä tunnistetaan harjoitustoiminnan merkitys sekä tietoturvan ja tietosuojan tason parantamisessa että häiriötilanteisiin ja niiden hallintaan varautumisessa. Harjoitustoiminnan avulla voidaan testata ja kehittää olemassa olevia varautumissuunnitelmia ja henkilöstön osaamista sekä hakea kehityskohteita tietoturva- ja tietosuojajärjestelyiden parantamiseksi. Linjauksissa tulisi ohjata kriittisillä toimialoilla toimivia organisaatioita harjoittelemaan toimintaa häiriötilanteiden varalle suunnitelmallisesti ja pitkäjänteisesti sekä ohjata koordinoivia viranomaisia tukemaan harjoitustoimintaa. Myös harjoitustoiminnassa julkisen ja yksityisen sektorin yhteistyö on merkittävässä roolissa.

Valo Janne
Insta Group Oy