Nixu Certification Oy
Keilaranta 15B
FI-02150 Espoo

Sosiaali- ja terveysministeriö
Meritullinkatu 8
Helsinki
PL 33
00023 VALTIONEUVOSTO

kirjaamo@stm.fi.
Viite: VN/8786/2021

Espoo 12.4.2021

Lausunto toisiolain siirtymäsäännösten muutosesityksestä

Tietoturvallisuus on tietoyhteiskunnan turvallisuutta. Pidämme erittäin hyvänä, että terveydenhuollossa on ryhdytty toimenpiteisiin, joilla arkaluontoista terveyteen liittyvää tietoa suojataan aiempaa paremmin. Eräs näistä on toisiolain perusteella annettu THL:n määräys 1/2020 muiden kuin Findatan turvallisille käyttöympäristöille asetettavista tietoturvallisuusvaatimuksista. Lain ja määräyksen tavoitteet ovat erittäin hyvät, ja haluamme korostaa, että tietoturvallisuuden hyvän tason asettaminen säädökseksi lakiin kertoo, kuinka tärkeästä asiasta on kyse. Tieturvallisuus ei ole enää vain hyvää käytäntöä, vastuullisten toimijoiden oma-aloitteisuutta tai jonkin alan etujärjestöjen aikaansaannosta, vaan ehdoton edellytys turvalliselle toiminnalle.

Lain perusteella annettua määräystä valmisteltiin noin vuosi sitten, ja tuolloin annetuissa lausunnoissa ilmeni huoli, vaaditaanko liian paljon liian nopeasti. Ensimmäinen luonnos oli vaatimuksiltaan niin tiukka, että oli epävarmaa, olisiko vaatimusten täyttäminen ollut mahdollista ensinkään.

Määräyksen lopullinen versio oli edelleen tiukka, mutta sen mukaisten käyttöympäristöjen rakentaminen ja käyttö on mahdollista – joskin vaativaa. Kun otetaan huomioon, ettei toissijaisen terveystiedon käsittelylle ole aiemmin asetettu erityisiä tietoturvallisuusvaatimuksia, on muutos raju: säätelemättömästä alasta tietoturvallisuuden eturiviin.

Kannatamme vahvasti tietoturvallisuuden tason nostamista velvoittavilla säädöksillä, mutta toisiolain aikataulu oli erittäin tiukka. Määräyksen julkistamisen jälkeen oli alle seitsemän kuukautta aikaa saattaa käyttöympäristöt määräyksen mukaisiksi, auditoida ne ja saada tästä todistus.

Määräyksen mukaisten käyttöympäristöjen auditoinnissa olemme havainneet seuraavia, parannusta kaipaavia asioita. Olemme kertoneet näistä auditointeja koskevissa THL:n järjestämissä työpajoissa sekä muissa sopivissa yhteyksissä.

1) Määräys viittaa monissa yksittäisissä vaatimuksissa kansalliseen turvallisuusauditointikriteeristö Katakriin (versio 2015). Tämä on sinällään hyvä asia, mutta yksiselitteisen viittauksen myötä tulee mukanaan myös Katakrin mukainen tulkinta siitä, mikä on hyväksyttävää ja mikä ei. Arviointilaitokset ovat auditoineet vuosia Katakria, ja heille viittaus katakrinmukaisuudesta on yksiselitteinen, mutta vaikuttaa ilmeiseltä, että määräyksen antaja on ajatellut vähemmän tiukkaa tulkintaa. Vähemmän tiukka tulkinta ei ole arviointilaitoksille sinällään ongelma, mutta sen tekeminen, kun määräyksen vaatimus on kirjoitettu kuten on, on. Olemme tiukkojen tulkintojen kannalla, mutta ymmärrämme, jos kokonaisuuden kannalta arvioiden päädytään sallivampiin tulkintoihin.

2) Auditointiin sisältyy aina tulkintatraditio ja kannanotto rajatapauksiin tai muuten hankaliin kohtiin. Näiden käsittelyn ja julkistamisen sopivalla foorumilla näemme olevan kaikkien asianosasten etu. Tulkintojen tekeminen on aloitettu Findatan kanssa, mutta tämä on epävirallista, ja kaipaa kanavan tulosten julkistamiselle. Vaikuttaa, että asiaa ei ole ajateltu määräystä valmisteltaessa.

3) Kun auditointi valmistuu, selviää auditointiraportista, miten kukin määräyksen vaatimus täyttyy auditoitavassa käyttöympäristössä. Mikäli kaikki vaatimukset täyttyvät, täyttää käyttöympäristö määräyksen vaatimukset. Mikäli yksi vaatimus ei täyty, mutta poikkeama on kokonaisuuden kannalta vähäinen (ns. pieni poikkeama), ei ole enää yksiselitteistä, täyttyykö määräyksen vaatimus vai ei. Katakri-, VAHTI- ja PCI DSS-auditoinneissa todistusta (sertifikaattia) ei voida myöntää, kun taas ISO 27001 -auditoinneissa voidaan. ISO-auditoinneissa vain vakava poikkeama estää todistuksen myöntämisen. Määräystä annettaessa ei tätä kysymystä ollut ratkaistu, jolloin sen pohdintaa jouduttiin tekemään auditointien jo alettua, ja vastakkain oli kaksi poikkeavaa näkemystä: Katakri- ja ISO-traditio.

   Arviointilaitoksena katsomme, että tärkeintä on saada selkeä päätös noudatettavasta menettelystä.

   Pidämme parhaana ratkaisua, jossa valvontaviranomainen tekee päätöksen arviointilaitoksen raportin pohjalta. Mikäli tämä on lain 26§2 mukaan mahdotonta, voidaan asia ratkaista niin, että valvontaviranomainen antaa arviointilaitoksille ohjeen, millä perusteella todistus voidaan antaa, ja arviointilaitosten toimintaa valvova Traficom hyväksyy menettelyn ja päivittää Arviointilaitosohjetta asianmukaisesti.

4) Nixu Certification Oy haluaa olla aktiivisesti mukana tietoturvan edistämisessä, kuten tiedotustoiminnassa. Vaikuttaa ilmeiseltä, että lain määräajoista tiedottaminen ei ole sujunut kovin hyvin, kun merkittävät, tietoturvallisuuteen panostavat toimijat eivät ole tilanneet auditointia käyttöympäristöihin ajoissa. Olemme pyytäneet yhteystietoja, mutta emme ole saaneet. Olemme ehdottaneet molempien toisiolain mukaisiin auditointeihin pätevöityneiden arviointilaitosten

ja valvontaviranomaisten yhteistä kohdennettua viestintää, mutta asia ei ole edennyt.

5) Pyynnöistä huolimatta emme ole saaneet edes summittaista arvioita auditoinnin kohteiden lukumäärästä. Tieto on tarpeen paitsi edellisen kohdan viestinnän takia myös resurssien varaamiseksi. Vaikka Nixu Certification Oy on vain noin 10 henkilöä, on meillä mahdollisuus käyttää emoyhtiömme Nixu Oyj:n noin 400 osaajaa. Tämä edellyttää heidän varaamistaan, emmekä halua tätä tehdä ilman käsitystä tulevien auditointien määrästä. Emme tarvitse tarkkaan tietoa, hyvä arvaus on riittävä.

6) Ulkomaisten auditointien tekeminen on vaikeaa. Korona estää ne tyystin, mutta normaalitilanteessakin ne vaativat huomattavasti pidemmän ajan kuin kotimaiset kohteet. Suurten pilvipalvelutoimittajien arviointi (esimerkiksi Pilvipalveluiden turvallisuusauditointikriteeristö Pitukria hyödyntäen) on välttämätöntä, ja tämä lienee parasta tehdä keskitetysti. Pienempien käyttöympäristöjen ylläpitäjien turvallisuuden arvioinnissa on tasapuolisuuden vuoksi oltava samat vaatimukset kuin kotimaisten, mutta määräystä ei ole englanniksi. Katakri on käännetty englanniksi, mutta se ei ole tunnettu ulkomailla.

   Nixu Certification on tehnyt ja pystyy tekemään auditointeja ulkomailla (Eurooppa, USA, Aasia).

   Voidaan harkita muiden maiden kansallisten auditointikriteeristöjen mukaan tehtyjen auditointien hyväksymistä, jos Suomen ja kohdemaan välillä on General Security Agreement -sopimus.

   Ulkomaisten toimijoiden esittämien hyväksyttyjen hyväksilukua osoituksen määräyksenmukaisuudesta voidaan harkita, mutta on syytä varoa tilannetta, jossa ulkomaiselta toimijalta edellytetään tosiasiassa vähemmän kuin kotimaiselta.

7) Nykyisen lain mukaan (Toisiolaki 26§3) todistus myönnetään 5 vuoden ajaksi. Laki tai määräys ei edellytä vuosittaisia seuranta-auditointeja. Pidämme tätä selkeänä puutteena. Määräystä tulisi tarkentaa siten, että arviointilaitos tekee seurantakäynnin vuosittain, jossa käydään läpi mahdolliset muutokset sekä tehdään pistokoemainen tarkastus. Tämä olisi edellytys todistuksen voimassa ololle. Seuranta-auditointi olisi siis selkeästi kevyempi kuin ensiauditointi, mutta lisäisi varmuutta siitä, että ympäristön tietoturvallisuus pysyy riittävällä tasolla.

Ehdotettua siirtymäajan muutosta pidämme käytännön sanelemana pakkona. On vain huonoja valintoja: merkittävä haitta tutkimus- ja opetustoiminnalle, tietoturvallisuuteen panostavien toimijoiden muuttuminen lain rikkojiksi tai lain siirtymäajan muuttaminen viime tipassa, kun valveutuneimmat toimijat ovat jo auditointinsa käynnistäneet. Siirtymäsäännöksen 60§1 muuttaminen tässä vaiheessa on huono asia, mutta valittavissa olevista vaihtoehdoista selvästi vähiten huono.

Nixu Certification Oy on Traficomin hyväksymä arviointilaitos, jonka pätevyysalueeseen kuuluu toisiolain mukaisten käyttöympäristöjen auditointi sekä Katakri- ja VAHTI- ja THL:n määräyksen 1/2015 (ns. KanTa-auditoinnit) tarkastukset. Yritys on ISO 27001 sertifiointielin.

Nixu Certification Oy:n puolesta

Niki Klaus
Toimitusjohtaja

Olli-Pekka Soini
Lead Auditor
CISSP, CISA, CISM, CRISC, CSA STAR Lead Auditor
ISO 27001 Lead Auditor