Suomen Kuntaliitto ry

Lausunto

05.01.2021 1176/03/2020

Asia: VN/24348/2020

Selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; työryhmän väliraportti

Lausunnonantajan lausunto

Ehdotukset poliittisiksi linjauksiksi, kommentit:

Kuntaliitto pitää tarpeellisena sitä, että tietoturvan ja -suojan käytänteitä tarkastellaan yhteiskunnan kriittisten toimialojen/sektoreitten tasolla. EU:n laajuinen yleinen tietoturvasäädöksen (NIS-direktiivi) soveltaminen kansallisesti alkoi 9.5.2018. Tavoitteena luoda yhteiskunnan toiminnan kannalta kes-keisten, digitaalisten palveluiden tarjoajille turvallisuus- ja ilmoitusvaatimukset. Tietosuoja-asetusta alettiin soveltamaan 25.5.2018, ja siihen liittyen ja sen yhteydessä tietoturvan menetelmiä tulee seurata suunnitelmallisesti.

Kuntatoimijoiden näkökulmasta selvityksessä esitetyt toiminnallisuudet ja toimenpiteet koskevat useita kuntien tehtäviä aiheuttaen lisäkustannuksia merkittävien uusien tietoturvavaatimusten kautta. Asetetut tavoitteet on suhteutettava toimintaan, huomioiden kuinka korkeaan laatutasoon voidaan mennä käytettävät resurssit ja osaaminen huomioiden. Toimenpide-ehdotusten rinnalla tulisikin arvioida niiden kustannusvaikutuksia. Kunnille lainsäädännön tai viranomaismääräysten kustannukset tulee kompensoida täysimääräisesti.

Kriittisten toimialojen suunnitelmallinen ja systemaattinen kehittäminen turvallisuuden eri osa-alueilla edellyttää vaikutusarviointeja eri tulokulmista. Ajan- ja tarkoituksenmukainen lainsäädäntö, viranomaisyhteistyö ovat kriittisten toimialojen ytimessä yhtenäistäen julkisen hallinnon turvallisuuskulttuuria. Mahdollistaen toimintojen kehittämisen (tietoturvalliset palvelut, keskeisten tietovarantojen huoltovarmuus, varmuuskopioinnin taso ja kriteerit).

Tulokulmista

- Vesihuollon osalta laitokset ovat automatisoinnin ja etäluettavuuden sekä tietotekniikan suhteen erilaisia. Investointien tarve ja velvoitteet voivat näin ollen vaihdella paljonkin toimialan sisällä.

- Terveydenhuollon tietoturvan kehittäminen ja siihen tehtävien investointien tulee olla osa hyvinvointialueiden muodostamistyötä huomioiden alueuudistuksen myötä muuttuva hallinnoiva organisaatio. Ei yksittäisten kuntien ratkaisuja ilman kokonaiskuvaa.

- Tarkasteltaessa koko kuntaomisteisten energiayhtiöiden kenttää (sähkö, lämpö/jäähdytys), esiintyy käytänteitten osalta kirjavuutta.

- Viranomaisten sekä muiden kriittisten toimijoiden yhteistoiminta häiriötilanteiden hoitamisessa ja valmiussuunnittelun kokonaisuutta suunniteltaessa (tiedonvaihto, resurssikysymykset, osaaminen ja mahdolliset tulevat organisaatiomuutokset; alueuudistus).

- Velvoitteita tulisi harkita tarkennettavaksi vielä tehtävien selvitysten jälkeen. Erityisesti kunnissa tietoturva kytkeytyy usein kaikkien kunnan toimialojen kokonaisuudeksi, eikä jotakin toimintaa tai toimialaa voi irrottaa kokonaan omakseen tietoturvakysymysten näkökulmasta.

Ehdotukset poliittisiksi linjauksiksi, kommentit:

7. Kriittisille toimialoille määritellään selkeät ja oikeasuhtaiset tietoturvavaatimukset lainsäädännössä.

- Vaatimusten pitää olla oikeasuhtaiset on tärkeän perusteellisen arvioinnin paikka.

8. Toimialoille säädetään velvoite pyytää Liikenne. ja viestintäviraston KTK:lta lausunto tietoturvaa koskevista vaatimuksista ennen niiden hyväksymistä ja tarvittaessa myös vaatimusten toimeenpanosta.

- Kunkin julkisen hallinnon organisaation tietoturvahallintakäytänteitten katselmointi sekä mahdollinen auditointi edellyttää hyödynnettävissä olevaa viitekehystä, mikä on suhteutettu organisaation toimintaan.

- Velvoitteen ensisijaisesti koskiessa NIS-sektoriviranomaisia (asianosaisen sektoriviranomaisen ohjatessa ja koordinoidessa esim. kaikkia yksityisiä vesilaitoksia suoraan tai välillisesti kuntien kautta) on toimeenpanon kannalta kiinnitettävä riittävä huomio ohjaukseen.

11. Kriittisille toimialoille säädetään velvoite säännöllisesti auditoida kriittiset tieto- ja tietoliikennetekniset prosessit ja toiminnot. Auditointimalli määräytyy laissa riskiperusteisesti sen mukaan, kuinka kriittistä tietoa sisältävästä järjestelmästä tai prosessista tai toiminta ohjaavasta on kyse. Määrittelyssä huomioidaan taloudelliset vaikutukset.

- Ko. auditointimallin tulisi olla dynaaminen ja skaalautuva eri toimialat ja eri toimijat huomioiden, jotta se ohjaisi toimijoita sekä ylläpitäjiä merkityksellisen tietoturvan ja -suojan edellyttämiin toimenpiteisiin.

- Taloudellisten vaikutusten osalta yhteiskunnan edellyttämien toimenpiteitten tulee olla oikeassa tasapainossa organisaation toiminnan kannalta (riskipohjainen päätöksenteko huomioiden). Ali- ja yli-lyönnit tulee voida välttää, jottei pitkässä juoksussa ajauduta turvallisuuskäytänteitten kiertämiseen.

12. Kriittisten toimialojen merkittävimpien toimijoiden tulee osoittaa käyttävänsä tietoturvallisuuden hallintajärjestelmää ISO 27001 -sertifioinnilla vuoden 2024 loppuun mennessä.

- ISO 27001 –sertifikaatti todistaa, että tietoturvajohtamisjärjestelmä on sertifioitu parhaiden käytäntöjen mukaisesti ja että se täyttää kaikki standardin asettamat vaatimukset.

o Kuntatoimijoille asetettuja lakisääteisiä tehtäviä toteutetaan tyypillisesti eri organisaatioitten/palvelutuotantomallien kautta.

o Palveluiden digitaalisuusasteisuuden kasvaessa, palveluiden toteuttaminen edellyttää tiedon käytettävyyttä ja siirtämistä eri toimintaympäristöjen välillä.

o Riittävää harkintaa tulee käyttää miltä osin on tarpeellista sertifiointi-käytäntöihin, jotta tarpeettomilta kustannuksilta vältytään!

- Valittavaa tietoturvajärjestelmä viitekehystä ja sen osia tulee arvioida soveltuvin osin kustannus-hyöty analyysin kautta, keskittyen niihin asioihin ja toimenpiteisiin missä vaikuttavuus tavoitteitten asettelun kautta on merkityksellisin.

- Kuntakentän kokonaisuus huomioiden, suuret kaupungit ja maaseutukeskukset (22/310) kuuluvat selvityksessä mainittujen merkittävimpien toimijoiden joukkoon.

o Näidenkin kuntatoimijoiden kohdalla toiminnan johtaminen ja ohjaus, vastuitten jakautuminen konsernin (juridisesti erillisten yhtiöitten) ja toteuttavien organisaatioitten välillä sekä turvallisuuskulttuuri ovat eriasteisia (monitoimittajaympäristö-rakenne).

o Tarvittavat käytänteet tulee olla koko organisaation kannalta yhteneviä toteutukseltaan huomioiden sisäinen/ulkoinen turvallisuus (kuntakentässä suuret kaupungit ja maaseutukeskukset ovat panostaneet näille osa-alueille - heidän joukostaan löytyy ko. osa-alueitten edelläkävijöitä).

16. Varmistetaan, että tietoturvallisuus on otettu huomioon vesihuoltolaitosten suunnitelmissa häiriötilanteisiin varautumiseksi.

- Valvonta ja lainsäädännön noudattaminen (tarvittava mekanismi).

o Varautumiseen ja infraan liittyvät salassa pidettävät asiat tulisi kyetä arvioida toimiala kohtaisesti (pienille toimijoille helposti kohtuuton rasite).

- Tarkoituksen mukaisesti määritelty joukko laitoksia.

- Kunnalliset toimijat eivät voi luopua tarjoamasta palve-luja tuotantokustannuksiin vedoten (kustannukset siir-tyvät asiakasmaksuihin ja alueellisten pienten toimijoiden asiakkaiden asema epätasa-arvoistuu).

- Julkisen sektorin merkitys kriittisenä toimialana tunnistetaan ja huomioidaan (vakioidaan).

o Tietoja tulee hallinnoida käyttöoikeuksin. Esim. vesijohtoverkostotietoja jaetaan/julkaistaan tarkoituksenmukaisesti. Toiminnan edellytyksenä on, että tiedot ovat saatavilla niille jotka niitä tarvitsevat.

27. Selvitetään Suomen 15 suurimman kunnan tietoturvan ja tietosuojan taso terveydenhuollossa, energiahuollossa ja vesihuollossa.

- Selvitysten kustannusten kohdentaminen.

- Yhtenevä agenda siitä mitä ja miksi selvitetään/tutkitaan (sisällöllisesti ja tavoitteellisesti oltava hyödyllinen organisaation toiminnan kehittämisen kannalta, jotta organisaatiot sitoutuvat toteutukseen).

- Eri organisaatioitten ja palveluiden toteuttajien rakenteitten ja vastuitten huomioiminen.

o PK-seudulla (Helsinki, Espoo, Vantaa) yhteinen vesihuoltotoimija (HSY kuntayhtymä), Turussa kaupungin vesihuolto Oy + seudullinen jätevesiyhtiö + seudullinen tukkuvesiyhtiö, Tampereella ja Oulussa vesiliikelaitos, Tampereelle tulossa seudullinen jätevesiyhtiö, Hämeenlinnassa seudullinen vesihuolto oy jne.

Väliraportin muut osat, kommentit:

Johdanto

- Eri viranmaisten roolia ja suorituskykyä tulee voida arvioida kriittisesti esitettävien tehtävien ja resurssien kautta.

- Jo käynnissä oleva työ huomioiden (julkisen hallinnon digitaalinen turvallisuus) olisi harkittava kuinka ohjauksen ja eri hallinnon alojen yhteistoiminnan kautta voitaisiin selvityksessä esitettyjen täydentävien asioitten/toimenpiteitten avulla edesauttaa positiivista kehitystä tietoturvan ja tietosuojan parantamiseksi, systematisoituna.

- Toimivaltakysymykset on syytä huolella harkita lainsäädännöllisiin toimiin ryhdyttäessä. Lainsäädännöllisten toimenpiteiden luonnetta ja muotoa tulisi kyetä arvioimaan toimialakohtaisesti vaikutustenarvioinnin kautta. Ennalta ehkäisten mahdolliset tarpeettomat muodolliset ja kalliit toimenpiteet esillä oleville toimialoille ja kaikille toimijoille.

Nykytilan arviointi

- Selvityksessä kiinnitetään huomio julkisen sektorin tietoturvan tasoa selvittävään valtiovarainministeriön Haukka-ohjelmaan. Ensimmäisiä kuntatoimijoilta kerättyjä tietoja analysoidaan par'aikaa, ja tulosten valossa kuntakenttä on toiminnallisesti eritasoinen tietoturva ja -suoja osa-alueilla. Jotkut kuntatoimijat ovat edelläkävijöitä (kokoluokasta riippumatta), mutta kokonaisuutena kuntakenttää tarkasteltaessa yhtenevät, yhteismitalliset käytänteet puuttuvat.

Auditoinnit ja sertifioinnit

- Tarvitaan yhtenäinen julkisen hallinnon auditointimalli. Huomioiden katselmointi vs. auditointi. Riippuen toimialan ja organisaation käytännöistä itsearviointi ymmärretään auditoinniksi siinä missä ONSITE-auditointi.

- Tiedonhallintalain jalkauttamisen/soveltamisen kautta julkisen hallinnon organisaatiot ovat aloittaneet tarvittavan työn kriittisten tietojärjestelmien, toimintaprosessien kuvaamisen ja niihin liittyvien riskien tunnistamisen osalta.

- Kuntatoimijoiden osallistaminen edellyttää oikean tasapainon löytämistä, ajankäyttö, resurssien hallinta ja investoinnit huomioiden. Pääpainon ollessa toteuttamiskelpoisuudessa, ratkaisuhakuisuudessa.

Sertifioinnin taloudelliset vaikutukset

ISO 27001 –tietoturvasertifikaatin hankkimisen kokonaiskustannuksiksi on arvioitu 76 480 euroa.

- Esimerkkinä toimialasta (havainnollistamaan asioita): Vesihuoltolaitoksista suurin osa työllistää vain 0-4 henkeä (n. 1200), yli 50 henkeä työllistäviä laitoksia on vain 29 kpl. 88 %:ssa on alle 10 henkeä työssä.

o Haaste on usein juuri valvonnan resursointi.

o Toimialan muutos valvontaa/velvoittavuutta mitoitettaessa, esim. 1500 yksityisen vesilaitoksen sertifioinnin kautta.

- Lisäisi painetta lakkauttaa vesiosuuskuntia.

- Kasvattaen kuntien roolia vesihuollon osalta.

o Kunnallisia laitoksia on noin 400.

- Näitten osalta tulisi käyttää harkintaa sertifiointien osalta

Mikäli sertifioinnin valvonta on kattavaa ja mahdolliset sanktiot suuria, on mahdollista, että yritykset lopettavat liiketoimintaansa tämän takia.

- Olisi kyettävä arvioimaan, selvityksen linjausten ja säätelyn vaikutukset alueelliseen/paikalliseen/seudulliseen palveluntarjontaan.

- Selkeät julkisen hallinnon johdonmukaiset pelisäännöt ovat madaltamassa mahdollisia ylireakointeja palveluntarjoajien puolelta.

- PK-sektorin riskinotto julkisen hallinnon ratkaisujen osalta!

Ylikoski Jari
Suomen Kuntaliitto ry - Strategia- ja kehitysyksikkö