Suomen Vesilaitosyhdistys ry

Lausunto

05.01.2021

Asia: VN/24348/2020

Selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; työryhmän väliraportti

Lausunnonantajan lausunto

Ehdotukset poliittisiksi linjauksiksi, kommentit:

Vesilaitosyhdistys (VVY) on vesihuoltolaitosten toimialajärjestö. Jäseninämme on noin 300 vesihuoltolai-tosta kattaen noin 90 % maamme keskitetysti järjestetystä talousveden toimituksesta. Vesilaitosyhdistys kiittää mahdollisuudesta antaa lausunto väliraportista tietoturvan ja tietosuojan parantamiseksi yhteis-kunnan kriittisillä toimialoilla.

Väliraportissa kartoitetaan lainsäädännön muutoksia ja muita toimenpiteitä tietoturvan ja tietosuojan kehittämiseksi yhteiskunnan kriittisillä toimialoilla. Muun muassa vesihuolto mainitaan raportissa yhtenä kriittisistä toimialoista. Väliraportissa on listattuna poliittisia linjauksia, joissa ehdotetaan toimenpiteitä. Pidämme tärkeänä, että ehdotusten taloudelliset vaikutukset arvioidaan ja suhteutetaan mahdollisiin riskeihin. Riskiperusteisuus tulee ottaa vaatimuksissa huomioon.

Linjaus 1: Vesilaitosyhdistys toteaa, että viranomaisten välinen yhteistyö ja sille yhteinen säädöspohja on tarpeen tietoturvaloukkaustilanteiden selvittämiseksi. Väliraportissa muistutetaan myös siitä, että viran-omaisten yhteistoimintaan tarvitaan riittävät resurssit.

Linjaukset 2 ja 3: Ehdotukset Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen kriittisten toimialo-jen sektoriviranomaisille antamasta asiantuntijapalvelusta (linjaus 2) ja koulutuksesta (linjaus 3) ovat kannatettavia, sillä tietoturvaan ja tietosuojaan liittyvät kysymykset eivät tyypillisesti kuulu sektorin toimi-joiden osaamiseen. Vesihuoltoa valvovat ja ohjaavat sektoriviranomaiset toimivat jo nyt varsin niukoilla resursseilla, joten ehdotetun tuen vastaanottaminen ja hyödyntäminen viranomaisessa ja edelleen toimi-joiden taholta edellyttää resurssien vahvistamista myös näiden toimijoiden osalta.

Linjaukset 4 ja 6: Kannatamme myös Kyberturvallisuuskeskuksen tietoturvallisuuden kartoituspalvelun (linjaus 4) sekä tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä Havaron (linjaus 6) mahdollis-tamisen kaikille kriittisille toimialoille.

Linjaus 7: Selkeät, oikeasuhtaiset ja toimialan tarpeista asetetut yleiset tietoturvavaatimukset edistäisivät yhdenmukaisesti ja laajasti toimialan tietoturvaa ja pienentäisivät tietoturvaloukkausten riskiä. Yhdenmu-kaiset vaatimukset lainsäädännössä varmistaisivat myös palveluntarjoajien tarjoamien ratkaisujen sovel-tuvuutta toimialalle ja helpottaisivat sitä kautta hankintaprosesseja ja palveluntarjoajan valintaa.

Vesihuoltoalan tietoturvassa korostuu erityisesti automaatiojärjestelmien ja tietoliikenneyhteyksien toi-mintavarmuuden turvaaminen. Suurimmilla vesihuoltolaitoksilla tämä on varmistettu omilla henkilöre-sursseilla, mutta toimialalla hyödynnetään myös laajasti ostopalveluita ja digitalisaation lisääntyessä alal-le tulee myös uusia palveluntarjoajia. Vesihuoltotoimialalla on kokonaisuudessaan hyvin niukasti toi-mialan tarpeet ja vaatimukset hallitsevia tietoturvaosaajia. Vesihuoltolaitosten tietoturvaosaamista on lähdetty lisäämään perustamalla toimialalle oma Kyberturvallisuuskeskuksen alainen ISAC-tiedonvaihtoryhmä. Suurin osa vesihuoltolaitoksista on riippuvaisia kuntien tietohallintopalveluista, mikä on syytä huomioida toimialan tietoturvallisuuden kokonaisvaltaisessa kehittämisessä.

Linjauksessa 8 todetaan, että toimialoille säädetään velvoite pyytää Liikenne- ja viestintäviraston Kyber-turvallisuuskeskukselta lausunto tietoturvaa koskevista vaatimuksista ennen niiden hyväksymistä ja tarvit-taessa myös vaatimusten toimeenpanosta. Olisi syytä selkeyttää koskeeko tämä linjauksessa 7 esitettyjä lainsäädännön vaatimuksia, vai joitain muita vaatimuksia.

Linjaukset 10, 11 ja 12: Väliraportissa ehdotetaan kriittisille toimialoille velvoitetta määritellä kriittiset tieto- ja tietoliikennetekniset prosessit ja toiminnot ja auditoida toiminnot säännöllisesti. Lisäksi ehdote-taan, että kriittisten toimialojen merkittävimpien toimijoiden tulee osoittaa käyttävänsä tietoturvallisuu-den hallintajärjestelmää ISO 27001 -sertifioinnilla vuoden 2024 loppuun mennessä. Vesihuoltolain 15 b §:n mukaan vesihuollon merkittävimpiä toimijoita ovat yli 30 000 asukkaan (volyymissä yli 5 000 m3/vrk) vesihuollosta vastaavat toimijat. Väliraportissa tarkastellaan toimijoiden mahdollisuutta hankkia sertifi-kaatteja. Siinä todetaan mm., että ISO 27001 – tietoturvasertifikaatin hankkimisen kokonaiskustannuksiksi on arvioitu 76 480 euroa (s. 31), mikä on merkittävä kustannus lähes kaikille vesihuoltolaitoksille. Vaati-mukset auditoinneille ja tietoturvan sertifioinnille tulee asettaa suhteessa toimijan toimintaan ja siinä oleviin tietoturvavaaroihin. Vesihuollon osalta on otettava huomioon, että auditointien ja sertifiointien pitää kattaa myös automaatioon kohdistuvat tietoturvauhkat. Vaatimuksissa on syytä ottaa huomioon toimijan ja toiminnan valvonnan resurssit ja niiden kohdentaminen kriittisen toiminnan tai palvelun tuot-tamisen kannalta oleellisimpiin seikkoihin, ei pelkästään tietoturvaan. Katsomme, että sertifiointivelvoite johtaisi kohtuuttomaan ja epäsuhtaiseen resurssien kohdentamiseen ja se on syytä poistaa poliittisia linjauksia koskevista ehdotuksista.

Linjaus 16: Väliraportissa ehdotetaan varmistettavaksi, että tietoturvallisuus on otettu huomioon vesi-huoltolaitosten suunnitelmissa häiriötilanteisiin varautumiseksi. Tietoturvallisuus on osa toimintavar-muutta ja toiminnan häiriöttömyyttä parantavaa riskienhallintaa sekä häiriötilanteisiin varautumista ja siten sen on sisällyttävä vesihuoltolain 15 a §:n velvoittamiin varautumissuunnitelmiin. Nykyinen lainsää-däntö ei edellytä täsmällisesti tietoturvan huomioon ottamista osana häiriötilanteisiin varautumista. Ve-sihuoltolaitoksille vesihuoltolain varautumisvelvoitteen täyttämiseksi laadittu ohjeistuskaan ei tue tieto-turvahäiriöihin varautumista, mutta asian tueksi on laadittu ja olemassa muuta ohjeistusta. Vesihuollossa tietoturva pitää ottaa varsinaisten tietoturvaloukkausten lisäksi huomioon lähes kaikissa muissakin häiriö-tilanteissa. Lainsäädännön täsmentämisen lisäksi tarvitaan resursseja ohjeistuksen parantamiseen ja sen jalkauttamiseen toimijoiden toimintaan.

Linjaus 27: Raportissa ehdotetaan, että Suomen 15 suurimman kunnan tietoturvan ja tietosuojan taso terveydenhuollossa, energiahuollossa ja vesihuollossa selvitetään. Selvityksessä hyödynnettäisiin toimen-piteessä 4 mainittua Kyberturvallisuuskeskuksen tarjoamaan tietoturvallisuuden kartoituspalvelua. Vesi-laitosyhdistys katsoo, että selvityksessä tulee ottaa huomioon, että esim. vesihuollon tietoturvalle ei ole asetettu velvoittavia vaatimuksia. Tietosuojan osalta vesihuoltolaitokset ovat toteuttaneet säädösten mukaiset toimenpiteet asiakkaiden henkilötietojen suojaamiseksi. Selvityksen tekemisessä on syytä ottaa huomioon, että mainituista palveluista vastaavat eri kunnissa eritavoin organisoidut (paikalliset, alueelli-set, kunnan virastot, liikelaitokset, osakeyhtiöt, kuntayhtymät) organisaatiot.

Linjaus 35: Väliraportissa ehdotetaan uusia toimintatapoja tietoturvauhkista ja –loukkauksista viesti-miseksi ja ilmoittamiseksi. Siinä ehdotetaan yksityishenkilöille ja organisaatioiden edustajille mobiilipääte-laitteeseen asennettavaa sovellusta, jonka kautta olisi mahdollista mm. ilmoittaa tietoturvauhkista ja -loukkauksista Kyberturvallisuuskeskukselle, kriittisen toimialan valvovalle viranomaiselle ja/tai poliisille. Lisäksi sovelluksesta voisi ilmoittaa henkilötietojen tietoturvaloukkauksesta Tietosuojavaltuutetun toimis-tolle. Kannatamme helppokäyttöisen ilmoitussovelluksen käyttöönottoa vesihuoltolaitoksille. Vesihuolto-lain 15 b § velvoittaa merkittävimpiä vesihuoltolaitoksia ilmoittamaan merkittävistä häiriöistä viranomai-sille. Jos häiriötilanne aiheutuu verkko- tai tietoturvahäiriöstä, ilmoitus tehdään Kyberturvallisuuskeskuk-sen www-sivuilla olevalla sähköisellä lomakkeella (NIS-Direktiivin mukainen tietoturvailmoitus). Vesihuol-lon kannalta olisi lisäksi toivottavaa, että samalla sovelluksella olisi mahdollista tehdä ilmoitus myös muusta vesihuollon merkittävästä häiriöstä. Sovelluksen on mahdollistettava vakavimpien tietoturvauh-kien ja -loukkausten nopea tunnistaminen ja niihin reagointi. Sovelluksesta ja sen oikeasta käytöstä vies-timiseen pitää panostaa.

Linjaukset 28-32: Katsomme, että eri sektoreita koskevat tietosuojavaatimukset tulisi mitoittaa sen mu-kaan, kuinka arkaluontoisia tietoja toimialalla käsitellään. Samanlaiset vaatimukset eivät ole tarpeen ei-vätkä sovi kaikille toimialoille, koska riskit ovat erilaisia. Vesihuollossa asiakassuhteet perustuvat yleensä sopimuksiin. Vesihuoltolaitosten hallussa on yleensä tavanomaisia asiakastietoja, joita tarvitaan vesi-huoltopalvelujen toimittamisessa ja laskuttamisessa. Jo sopijapuolten välisen luottamuksen säilyttäminen edellyttää, että asiakkaiden henkilötiedot ja liikesalaisuudet suojataan ulkopuolisilta lainsäädännön mu-kaisesti.

Vesihuoltolaitoksilla on kriittisiä kohteita muuallakin kuin tietoverkoissa. Raportissa tarkoitetun tietotur-van lisäksi merkitystä on sillä, millaisia tietoja vesihuoltolaitokset joutuvat antamaan julkisuuteen esimer-kiksi vedenhankinnan kannalta tärkeistä kohteista. Se, että suojataan tietotekniset prosessit, ei riitä, jos lainsäädäntö on epäselvä esim. siinä, voidaanko vesihuollon turvallisuuden kannalta tärkeitä tietoja suo-jata. Tietojen julkisuutta ja avoimuutta korostava lainsäädäntö on tarpeen, mutta sitä koskevista tulkin-noista aiheutuu, että etenkin kunnallisissa vesihuoltolaitoksissa on entistä vaikeampaa suojata vesihuol-lon turvallisuuden kannalta tärkeitä tietoja.

Tietojen julkisuutta ja käsittelyä koskevia säännöksiä tulee eri laeista. Ne ovat yleispäteviä ja niitä on toisi-naan vaikea soveltaa kriittisiin toimialoihin. Kriittisille toimialoille tulisikin löytää niille sopivat säännökset. Mahdollista uutta sääntelyä tulisi valmistella myös toimialakohtaisesti, läheisessä yhteistyössä toimijoi-den ja toimialajärjestöjen kanssa. Sääntelyn ennustettavuudesta, tarkkarajaisuudesta ja oikeasuhtaisuu-desta on pidettävä erityistä huolta.

Väliraportin muut osat, kommentit:

-

Liikanen Riina
Suomen Vesilaitosyhdistys ry