Elinkeino-, liikenne- ja ympäristökeskus

RAPORTTEJA 62 | 2023

Kyberturvallisuus vesihuollossa

Suomen vesihuoltolaitosten kyberturvallisuustilanne ja sen kartoittamisen keinot

Kyberturvallisuus vesihuollossa

Suomen vesihuoltolaitosten kyberturvallisuustilanne ja sen kartoittamisen keinot

RAPORTTEJA 62 | 2023

KYBERTURVALLISUUS VESIHUOLLOSSA
SUOMEN VESIHUOLTOLAITOSTEN KYBERTURVALLISUUSTILANNE JA SEN KARTOITTAMISEN KEINOT

Etelä-Savon elinkeino-, liikenne- ja ympäristökeskus

Taitto: Ramboll Finland Oy
Kansikuva: Ramboll Finland Oy

ISBN 978-952-398-181-2 (PDF)
ISSN 2242-2854 (verkkojulkaisu)

URN:ISBN:978-952-398-181-2

www.doria.fi/ely-keskus

Sisältö

Kyberturvallisuuden merkitys Suomen vesihuollolle

Viime vuosien aikana vesihuoltolaitosten kybertoimintaympäristö on muuttunut entistä monimutkaisemmaksi ja haastavammaksi. Tämä johtuu osaltaan teknologian kehittymisestä sekä järjestelmien ja toimintojen verkottumisesta, mutta myös Venäjän hyökkäyssodasta Euroopassa. Digitaaliset verkot ovat haavoittuvia ja niiden myötä on syntynyt uudenlaisia uhkia kuten kyberrikollisuutta, kybervakoilua ja kyberhyökkäyksiä. Lisäksi Suomen kriittiseen infrastruktuuriin kohdistuu aiempaa suurempi kiinnostus. Kyberturvallisuuden laiminlyönti voi johtaa tietomurtoihin, taloudelliseen vahinkoon, organisaation maineen menetykseen ja jopa ihmisten fyysisen turvallisuuden vaarantumiseen. Tästä johtuen kyberturvallisuus on olennaisessa asemassa myös vesihuoltolaitosten toiminnassa.

Kyberturvallisuuden varmistaminen on erityisen tärkeää yhteiskunnalle välttämättömien toimintojen kuten vesihuollon kannalta, sillä nämä ovat keskeisessä roolissa ihmisten perustarpeiden täyttämisessä ja turvallisuuden varmistamisessa. Jos kyberturvallisuutta ei huomioida, kyberhäiriöt voivat haitata tai jopa pysäyttää vesihuollon kriittisten järjestelmien toiminnan ja aiheuttaa vakavia seurauksia yhteiskunnalle. Kyberhäiriöt voivat johtua haittaohjelmista, palvelunestohyökkäyksistä, tietomurroista tai niitä voi ilmetä tavanomaisen toiminnan kuten päivitysten yhteydessä. Mahdollisia häiriöitä ovat esimerkiksi veden laatuhäiriöt tai vedenjakelun tai jätevedenpuhdistuksen keskeytyminen. Jos vesihuollon tietojärjestelmiin tunkeudutaan, tietomurron tekijät voivat myös päästä käsiksi herkkiin tietoihin kuten asiakastietoihin tai verkkotietoihin ja näiden tietojen käyttö voi estyä tai ne voivat jopa tuhoutua.

Parhaillaan kyberturvallisuuden tilaa pyritään parantamaan sekä kansallisesti että EU-lainsäädännön kautta. EU-lainsäädännöstä on tulossa kyberturvallisuutta koskevia vaatimuksia myös vesihuollolle. CER-direktiiviehdotuksella (CER = Critical Entities Resilience) halutaan vahvistaa kriittisen infrastruktuurin kriisinkestävyyttä, parantaa toimijoiden häiriönsietokykyä sekä jatkuvuudenhallintaa ja siten vahvistaa yhteiskunnan kriisinkestävyyttä ja kansallista turvallisuutta. Kyberturvallisuusdirektiivi (NIS2-direktiivi, 2022/2555; NIS = Network and Information Security) puolestaan yhdenmukaistaa velvoitteita, jotka koskevat yhteiskunnan tiettyjen kriittisten sektoreiden kyberturvallisuusriskienhallinnan ja raportoinnin vähimmäistasoa. Direktiivit on saatettava osaksi kansallista lainsäädäntöä lokakuuhun 2024 mennessä. Tätä raporttia kirjoitettaessa ei ole vielä selvää, mitä vesihuoltolaitoksia direktiivien vaatimukset tulevat koskemaan. Selvityksen tekohetkellä vielä voimassa ollut verkko- ja tietoturvadirektiivi (NIS-direktiivi) edellytti muita kattavampia toimia vesihuolto- tai tukkuvesilaitoksilta, jotka toimittavat vähintään 5 000 m^3/vrk vettä tai vastaanottavat vähintään 5 000 m^3/vrk jätevettä. Näitä laitoksia kutsutaan tässä raportissa NIS-laitoksiksi ja muita ei-NIS-laitoksiksi.

Suomen kansallisen kyberturvallisuusstrategian *(Turvallisuuskomitea 2019)* tavoitteena on vastata kyberuhkiin, vahvistaa yhteiskunnan kokonaisturvallisuutta ja varmistaa kybertoimintaympäristön toimivuus kaikissa oloissa. Tämä koskee myös vesihuoltoalaa, jonka kyberturvallisuuden nykytilaa selvitettiin tässä raportissa kuvatussa hankkeessa.

Selvityksen tausta ja toteutustapa

Etelä-Savon ELY-keskuksen vesihuoltopalvelut-yksikkö on vuodesta 2022 hoitanut maa- ja metsätalousministeriön ohjauksessa olevia vesihuoltotehtäviä kuten vesihuoltolain mukaista valvontaa, asiantuntijapalveluita ja vesihuollon viranomaistehtäviä. Vesihuollon kyberturvallisuuden edistäminen on yksi vesihuoltopalvelut-yksikön tehtävistä vesihuollon muun varautumisen edistämisen ohessa.

Tässä raportissa esitetään suomalaisten vesihuoltolaitosten kyberturvallisuutta kartoittaneen projektin tuloksia. Tavoitteena oli sekä hahmottaa kyberturvallisuuden tilaa suomalaisilla vesihuoltolaitoksilla että sitä, millä tavoin viranomaisen kannattaa selvittää vesihuoltolaitosten kyberturvallisuusasioita ja miten kyberturvallisuus kytketään osaksi vesihuoltoalan päivittäistä toimintaa. Projekti sai rahoitusta Huoltovarmuuskeskuksen Digitaalinen turvallisuus 2030-ohjelmasta ja sen toteutti Ramboll Finland Oy yhdessä tilaajan ja alan asiantuntijoista koostuneen ohjausryhmän kanssa. Ohjausryhmään kuului edustajia ELY-keskuksista, Huoltovarmuuskeskuksesta, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksesta, vesihuoltolaitoksilta sekä Huoltovarmuusorganisaation Vesihuoltopoolista. Digipooli toimi projektin neuvonantajaryhmässä.

Projektissa kyberturvallisuuden tilan kartoittamiseen käytettiin Kyberturvallisuuskeskuksen laatimaa Kybermittari-työkalua, joka on vapaasti saatavilla Kyberturvallisuuskeskuksen verkkosivuilta. Excel-taulukkomuotoinen Kybermittari-työkalu koostuu kaikkiaan 150 erilaisen käytännön kuvauksesta eli kysymyksestä. Kyberturvallisuuskeskus valikoi projektia varten Kybermittarista vesihuoltolaitosten kannalta tärkeimmät kysymykset ja muokkasi hieman kysymysten muotoilua. Ei-NIS-laitoksia koskemaan valittiin 49 Kybermittarin kysymystä ja NIS-laitoksia koskemaan 88 kysymystä. Ramboll laati Kybermittarin käytön tueksi sanaston ja Kybermittarin sisällön ymmärrystä tukevia esimerkkikuvauksia ja lisätietoja.

Kybermittari on jaoteltu 11 eri osa-alueeseen ja jokaisen osa-alueen sisällä on kysymyksiä kolmea eri kypsyystasoa koskien. Kypsyystasojen kuvaukset ovat seuraavat:

- Taso 0 – Organisaatio ei toteuta kyberturvallisuuden hallintaan liittyviä käytäntöjä.
- Taso 1 – Organisaatio toteuttaa käytäntöjä tapauskohtaisesti ja tekeminen ei ole säännöllistä
- Taso 2 – Organisaatiolla on määritetty dokumentoidut säännöllisesti toistettavat ja ylläpidettävät kyberturvallisuuden hallinnan mallit, vastuut ja valtuudet kyberturvallisuuden toteuttamiseksi.
- Taso 3 – Organisaatio toteuttaa kyberturvallisuutta riskilähtöisesti, koko organisaation kattavia toimintamalleja ylläpidetään jatkuvasti ja kyberturvallisuudelle on määritetty tavoitteet, joita mitataan säännöllisesti.

Ei-NIS-laitoksia koskee kysymyksiä vain kypsyystasolta 1. NIS-laitoksia koskevia kysymyksiä on myös tasoilla 2 ja 3. Vastatessa voi valita vaihtoehdoista ”0 - Vastaus puuttuu”, ”1 – Ei toteutettu tai ei tietoa”, ”2 – Osittain toteutettu”, ”3 – Enimmäkseen toteutettu”, ”4 – Täysin toteutettu”. Jokaisen suomalaisen vesihuoltolaitoksen ja tukkuvesilaitoksen tulisi saavuttaa kyberturvallisuudessa kypsyystaso 1. Tämän tason saavuttaminen edellyttää, että kaikkiin Kybermittarin vesihuoltoa koskeviin kysymyksiin on vastattu joko vaihtoehto 3 tai 4.

Selvityksessä lähestyttiin Varsinais-Suomen ja Satakunnan yhteensä 68 vesihuoltolaitosta ja tukkuvesiyhtiötä ja pyydettiin täyttämään Kybermittari, jonka avulla laitos arvioisi kyberturvallisuuden tilaa itsenäisesti. Tämän jälkeen tarkoitus oli, että vastaukset käydään yhdessä konsultin kanssa läpi vastausten yhdenmukaisuuden ja vertailukelpoisuuden varmistamiseksi. Vastauksia saatiin 15 vesihuoltolaitokselta ja tukkuvesiyhtiöltä. Osallistuneista laitoksista 10 oli ei-NIS-laitoksia ja 5 NIS-laitoksia. Osa vesihuoltolaitoksista haastateltiin alkuperäisen suunnitelman mukaan, osa täytti Kybermittarin yhdessä konsultin asiantuntijoiden tukemana. Kahdelta laitokselta ei saatu haastattelua, ainoastaan valmiiksi täytetty Kybermittari.

Vuonna 2024 toteutetaan vielä projektin seurantaosio, jossa kartoitetaan, miten projektiin osallistuminen on vaikuttanut vesihuoltolaitosten käytäntöihin.

Kyberturvallisuuden kartoittaminen Kybermittarin avulla

Kartoituksen toteutus

Selvitykseen osallistuneiden vesihuoltolaitosten ja tukkuvesiyhtiöiden Kybermittareiden pohjalta kartoitettiin kyberturvallisuuden eri osa-alueiden tilaa sekä alan vahvuuksia ja kehittämistarpeita. Lisäksi haastatteluiden avulla kerättiin tarkemmin tietoa Kybermittarin käyttökokemuksista, kyberturvallisuusasioiden ymmärryksestä ja laitosten toimintaympäristöstä kyberturvallisuuden näkökulmasta. Seuraavassa on esitetty kyberturvallisuuden tilanne projektiin osallistuneiden 15 vesihuolto- ja tukkuvesilaitoksen vastausten pohjalta.

Haastatteluiden anti ja kokemukset Kybermittarin käytöstä

Projektin yhtenä tavoitteena oli koota kokemuksia vesihuoltolaitosten kyberturvallisuuden arvioinnista ja Kybermittarin käytöstä arviointityökaluna. Tavoitteeseen pääsemistä vaikeuttivat monet käytännön asiat. Kybermittari ohjeineen lähetettiin vesihuoltolaitoksille vuoden 2022 marraskuun lopussa ja alun perin laitoksilla oli tammikuun 5. päivään aikaa vastata kyselyyn. Vaikka vastausaikaa jatkettiin, oli ajankohta selvästi huono vastaamiselle vuodenaikaan liittyvien kiireiden ja lomien takia. Yleisesti ottaen suurin este vastausten saamiselle vaikutti kuitenkin olevan resurssipula.

Osa vesihuoltolaitoksista täytti Kybermittarin itsenäisesti ja se käytiin läpi konsultin kanssa, osan kanssa konsultti toimi apuna täyttämisessä. Jälkimmäinen vaihtoehto nähtiin toimivampana tapana. Etenkin itsenäisesti täytettäessä Kybermittari koettiin raskaaksi ja vaikeaselkoiseksi ja täyttäminen aikaa vieväksi. Kybermittarin kysymyksiä pidettiin usein pitkinä ja vaikeasti ymmärrettävinä. Toivottiin, että kysymykset itsessään olisivat lyhyitä ja niihin annettaisiin enemmän tietoa ja projektissa laadittuakin runsaammin esimerkkejä Kybermittarin lisätietokentässä.

Mitä pienempi vesihuoltolaitos oli kyseessä, sen vaikeaselkoisemmaksi Kybermittari koettiin. Kaivattiin vielä yksinkertaisempaa mallia, josta kävisi selvästi ilmi, minkä asioiden minimissään pitäisi olla kunnossa pienillä laitoksilla. Kysymyksistä toivottiin lyhyempiä ja yksinkertaisempia ja laajempaa selitystä sille, mistä on kyse. Sekä käsitteistöstä että kysymyspatteristosta toivottiin yksinkertaisempia ja kysymysten määrää vähäisemmäksi. Riittäisikö esimerkiksi, että laitoksella olisi vain yksi riskienhallintasuunnitelma, joka sisältäisi kyberriskien hallintasuunnitelman? Haastatteluissa esiin tulleet toiveet heijastelevat toisaalta sitä, että perusasiat haluttaisiin kuntoon, mutta toisaalta sitä, että kyberturvallisuus koetaan omasta ydintoiminnasta irralliseksi asiaksi, joka haluttaisiin saada haltuun hyvin rajatuilla toimenpiteillä. Pienillä laitoksilla koettiin usein, ettei asia koske heitä Kybermittarin edellyttämässä laajuudessa.

Haastattelut ja etenkin Kybermittarin tuettu täyttäminen yhdessä konsultin kanssa koettiin hyödyllisiksi ja näiden jälkeen oltiin positiivisella mielellä. Parhaimmillaan tilanteet olivat silloin, kun paikalla oli sekä vesihuoltolaitoksen että kunnan IT:n edustajat. Kun saatiin oikeat ihmiset keskustelemaan kyberturvallisuudesta, työpajassa oli ainutkertainen tilaisuus tutustua ja keskustella aiheesta. Mikäli haastatteluun saatiin vain vesilaitoksen johtaja, haastatteluiden anti oli vähäistä, sillä johtajalla ei välttämättä ole tietoa kunnan IT-asioista. Kunnan IT:n rooli oli kahtalainen: Vaikka kunnan IT:llä on kokonaisvastuu kyberturvallisuudesta, vesihuolto ei näyttänyt olevan heillä erityisesti fokuksessa. Toisaalta vesihuoltolaitos sai tarvittaessa pyytämällä tukea IT:stä.

Haastatteluissa vaikutti siltä, että kyberturvallisuus nähdään omasta ydintoiminnasta niin erillisenä asiana, ettei oikein tiedosteta, mitä se vesihuoltolaitoksen tapauksessa on ja millaisia uhkia siihen liittyy. Haastattelutilanteissa ilmeni esimerkiksi, ettei nähty, että vedenjakelu voi loppua kyberhäiriön

seurauksena. Sähkökatkoa oli mietitty, mutta ei mielletty, että vastaava tilanne voisi syntyä kyberhäiriön tuloksena. Haastattelija pystyi avaamaan asiaa esimerkkien avulla. Projektin kokemusten pohjalta vaikuttaa, että Kybermittarin täyttö vaatii tahon, joka ohjaa keskustelua ja avaa Kybermittarissa kuvattujen käytäntöjen kuvauksia. Haastattelija voi esimerkiksi kertoa mitä on ”segmentointi” ja antaa tästä esimerkkejä, jotka liittyvät vesihuoltolaitoksen toimintaan. Haastatellut laitokset kaipasivat lisää esimerkiksi seminaareja, koulutuksia ja kyberharjoituksia eli osaamisen kasvattamisen tarve tiedostettiin.

Useilla projektin alussa kontaktoiduista laitoksista oli selvästi huutava resurssipula ja tämä ilmeni myös haastatteluissa. Kun kyberturvallisuus koetaan vaikeaksi aiheeksi ja se tulee kaikkien muiden töiden päälle, se jää toiminnassa helposti syrjään.

Kyberturvallisuustilanne lyhyesti

Selvityksen perusteella vesihuoltolaitosten kyberturvallisuuden taso on vaihtelevaa ja osin puutteellista. Vesihuollossa on toteutettu kyberturvallisuutta koskevia toimenpiteitä, mutta kyberturvallisuuden kehittämiseksi tarvitaan toiminnan systemaattisuuden ja dokumentoinnin parantamista sekä kumppanuusverkon parempaa hallintaa.

Kybermittarin ja haastatteluiden pohjalta nousivat kehittämiskohteina esiin seuraavat asiat:

- Kunnan IT:n ja vesihuoltolaitoksen yhteistyön kehittäminen ja lisääminen: Moni asia on täysin kunnan vastuulla ja tarvitaan yhteistyötä riittävän kyberturvallisuuden tason takaamiseksi.
- Sopimusten päivittäminen: Sopimuksiin olisi tarpeen jatkossa kirjata, mitkä asiat ovat järjestelmätoimittajan, mitkä vesihuoltolaitoksen vastuulla. Sopimuksiin tulisi lisätä kyberturvallisuuteen liittyviä ehtoja sekä vesihuoltolaitoksen omat tietoturvaperiaatteet ja -vaatimukset.
- Koulutuksen ja tietoisuuden lisääminen: Etenkin pienet laitokset tarvitsevat ulkopuolista asiantuntija-apua ja matalan kynnyksen koulutuksia ja tietoiskuja.
- Konkreettisen harjoittelun ja esimerkiksi Taisto- ja Tieto-harjoituksiin osallistumisen lisääminen.

Kyberturvallisuuden mahdollistaminen

Riskienhallinnan rooli vesihuoltoa koskevassa lainsäädännössä

Kyberturvallisuus voidaan lukea osaksi vesihuoltolaitoksen riskienhallintaa ja omaisuudenhallintaa. Vesihuoltoa koskevassa lainsäädännössä riskienhallintaa käsitellään useissa eri yhteyksissä.

Vesihuoltolaki (119/2001) edellyttää vesihuoltolaitoksilta suunnitelmaa häiriötilanteisiin varautumisesta ja sen pitämistä ajan tasalla. Tämä ns. varautumissuunnitelma sisältää ohjeet normaaliolojen häiriö- ja erityistilanteissa ja valmiuslain tarkoittamissa poikkeusoloissa toimimiseen. Varautumistoimenpiteillä on turvattava yhteiskunnan toimivuuden kannalta kriittinen infrastruktuuri ja kriittisen tuotannon jatkuminen kaikissa olosuhteissa. Vesihuoltolaki kattaa periaatteessa myös kyberturvallisuuden. Varautumissuunnitelmassa tulisi tunnistaa ja dokumentoida vesihuoltolaitoksen yhteiskunnalle tuottamat kriittiset palvelut sekä niiden tuottamiseen tarvittavat tiedot, prosessit ja järjestelmät. Suunnitelmassa tulisi esittää esimerkiksi toimintakorttien avulla, miten erilaisissa häiriötilanteissa toimitaan ja miten erilaisiin uhkiin, myös kyberuhkiin, varaudutaan. Vesihuoltolaissa on esitetty myös vesihuoltolaitoksen selvilläolo- ja tarkkailuvelvollisuus, jonka perusteella vesihuoltolaitoksen on oltava selvillä käyttämänsä raakaveden määrään tai laatuun kohdistuvista riskeistä, joihin voidaan lukea myös kyberriskit. Lisäksi NIS-laitoksilla on velvollisuus ilmoittaa merkittävästä häiriöstä vesihuollossa.

Ympäristönsuojelulaki (527/2014) sisältää ennaltavarautumisvelvollisuuden, jonka mukaan luvanvaraisen toiminnan harjoittajan (kuten jätevedenpuhdistamon) on ennakolta varauduttava onnettomuuksien ja muiden poikkeuksellisten tilanteiden estämiseksi ja niiden terveydelle ja ympäristölle haitallisten seurausten rajoittamiseksi. Toiminnanharjoittajan on laadittava riskinarviointiin perustuva varautumissuunnitelma ja mm. laadittava toimintaohje ja harjoiteltava toimia onnettomuuksia ja muita poikkeuksellisia tilanteita varten.

Myös terveydensuojelulaissa (763/1994) on säädetty riskienhallinnasta. Terveydensuojelulain mukaan kaikkien vähäistä suurempien talousvettä toimittavien laitosten (myös muiden kuin vesihuoltolaitosten) tulee laatia ja pitää ajan tasalla riskienhallintasuunnitelma sellaisten riskien ennalta ehkäisemiseksi ja hallitsemiseksi, joista voi aiheutua terveyshaittaa talousveden välityksellä. Riskienhallintasuunnitelmassa pitää tunnistaa vaaratekijät ja periaatteessa tämä kattaa myös kyberuhkat. Vuonna 2023 on annettu myös valtioneuvoston asetus talousveden tuotantoketjun riskienhallinnasta ja omavalvonnasta (7/2023). Siinä esitetään riskienhallintasuunnitelman sisältövaatimukset ja kerrotaan riskinarvioinnista ja riskienhallinnasta.

Myös kuntiin kohdistuu vesihuoltoon liittyviä velvoitteita. Valmiuslaki (1552/2011) edellyttää kunnilta, kuntayhtymiltä ja muilta kuntien yhteenliittymiltä valmiussuunnitelman laatimista. Valmiussuunnitelmassa kuvataan toimintatapa häiriötilanteissa ja poikkeusoloissa. Vesihuoltolain (119/2001) mukaan kuntien vastuulla on vesihuollon kehittäminen yhdyskuntakehitystä vastaavasti sekä usein myös vesihuollon järjestäminen. Sosiaali- ja terveysministeriön asetuksessa talousveden laadusta ja valvonnasta sekä rakennusten vesilaitteistojen riskienhallinnasta (1352/2015) annetaan kunnan terveydensuojeluviranomaiselle velvoite laatia häiriötilannesuunnitelma ja pitää sitä ajan tasalla sekä säädetään häiriötilannesuunnitelman sisällöstä.

Lisäksi kuntia koskevat kuntalakiin (410/2015) sisältyvät säännökset kunnan ja kuntakonsernin sisäisestä valvonnasta ja riskienhallinnasta, joiden järjestäminen on osa kunnan ja kuntakonsernin johtamista. Sisäisellä valvonnalla tarkoitetaan niitä toiminta- ja menettelytapoja, joilla tilivelvolliset ja muut esimiehet pyrkivät varmistamaan mm., että kunnan omaisuus ja voimavarat turvataan. Riskienhallinnassa tunnistetaan, arvioidaan ja hallitaan asetettujen tavoitteiden saavuttamista uhkaavia tekijöitä. Riskienhallinnan tavoitteena on saada kohtuullinen varmuus organisaation tavoitteiden saavuttamisesta sekä toiminnan jatkuvuudesta ja häiriöttömyydestä. Riskienhallintaprosessissa tunnistetaan ja kuvataan sekä sisäiset että ulkoiset riskit, arvioidaan häiriöiden todennäköisyys ja vaikutukset, hallitaan riskejä ja raportoidaan ja seurataan riskejä. Riskit kattavat sekä sisäiset että ulkoiset riskit. Sisäisen valvonnan ja riskienhallinnan järjestämisestä vastaa kunnanhallitus. Lisäksi kaikki ne toimielimet ja viranhaltijat, joille on annet-

tu toimivaltaa kunnan varojen käytössä ja toimivat viranomaisina, vastaavat sisäisen valvonnan ja riskienhallinnan toteuttamisesta. *(Kuntaliitto 2013)*

Kyberturvallisuuden rooli vesihuoltoa koskevassa lainsäädännössä

Edellä kuvatuissa lainkohdissa kyberturvallisuus ei tule vahvasti esiin, vaikka se periaatteessa sisältyykin organisaation riskienhallintaan. Kyberturvallisuutta käsitteenä ei mainita nykyisessä lainsäädännössä. Vesihuoltoa koskevassa lainsäädännössä vaatimusten pääpaino näyttäisi olevan sillä, että on varauduttu erityistilanteisiin ja poikkeusoloihin ja pystytään toimimaan niissä. Häiriötilanteiden systemaattinen ennaltaehkäisy jää vähemmälle huomiolle. Kuntiin kohdistuvat velvoitteet kattavat myös riskienhallinnan ja omaisuuden ja voimavarojen turvaamisen ja niissä näyttäisi siten olevan aineksia myös kyberturvallisuuden kehittämiseen. Kuntien riskienhallinnan voidaan katsoa kattavan myös kyberturvallisuuden, jolloin tämä velvoite koskee kuntien omistamia vesihuoltolaitoksia. Toisaalta voidaan katsoa, että ainakin vesihuoltolain edellyttämä varautumissuunnitelman ja talousvettä toimittavien laitosten riskienhallintasuunnitelman tulisi kattaa myös kyberturvallisuus. Lokakuusta 2024 lähtien NIS2-lainsäädäntö edellyttää suurilta vesihuoltolaitoksilta kyberturvallisuuden suhteen tiettyjä toimia ja näille tulee kyberriskien hallinnan velvollisuus. Pienempien vesihuoltolaitosten osalta ei tällä hetkellä mikään laki yksiselitteisesti vaadi kyberturvallisuuden saattamista kuntoon.

Kyberturvallisuuden käytännön toteutus ja valvonnan mahdollisuudet

Vesihuoltolaitoksen riskienhallinnan välineinä toimivat WSP (water safety plan) ja SSP (sanitation safety plan) ja niitä tukevat Vesilaitosyhdistyksen laatimat varautumisen ohjeet. Moni laitos laatii riskienhallintasuunnitelman WSP:n ja SSP:n avulla. Työkalut ohjaavat vesihuoltolaitosta tunnistamaan vaarat ja arvioimaan niihin liittyvät riskit sekä valitsemaan toimenpiteet riskien vähentämiseksi. WSP:ssä ja SSP:ssä tulisi tunnistaa vesihuoltopalveluiden tuottamiseen tarvittavat prosessit, tilat, laitteet, tuotantoketjut ja tuotannon keskeytymisen seurannaisvaikutukset. Kyberturvallisuuden osuus niissä on kuitenkin pieni.

Kyberturvallisuus huomioidaan esimerkiksi varautumissuunnitelmissa käytännössä vaihtelevasti. Vesihuoltolaitoksille laaditussa oppaassa *(Huoltovarmuusorganisaatio 2016)* häiriötilanteisiin varautuminen kattaa myös prosessien ja toimintatapojen kehittämisen, mutta kyberturvallisuutta ei käsitteenä mainita oppaassa. Yleisesti ottaen oppaita ja vaatimuksia olisi tarve täydentää kyberturvallisuutta koskevilla osioilla.

Viranomaisen tapa valvoa kyberturvallisuutta voisi tulevaisuudessa perustua vesihuoltolaitoksen kyberturvallisuustilanteesta selvilläolon valvontaan. Tällöin valvonnan painopisteenä olisi neuvonta ja ohjaus, joiden avulla tuettaisiin ja edistettäisiin kyberturvallisuutta. Selvilläolon lisäksi voitaisiin edellyttää, että vesihuoltolaitos on tietoinen oman toimintansa keskinäisistä riippuvuuksista kuten omien tietojen, tietojärjestelmien ja kumppaniorganisaatioiden toiminnan vaikutuksesta vesihuoltopalveluiden tuottamiseen.

Vesihuollon organisointi ja alueellinen yhteistyö

Suomessa toimii tällä hetkellä 1100 vesihuoltolaitosta, joista kunnallisia vesihuoltolaitoksia on 400. Henkilöstömäärän mediaani Vesilaitosyhdistyksen (VVY) jäsenlaitoksissa on henkilöstökyselyn mukaan 6,5 henkilöä. Vesihuollon toimijat ovat siis pieniä, ja laitosten resurssit ovat rajalliset.

Vuonna 2023 toteutetun selvityksen *(Kuivamäki ym. 2023)* mukaan vesihuoltolaitokset ovat suurelta osin aliresursoituja, joten vesihuollon resurssien kasvattamiselle on Suomessa välttämätön tarve. Selvityksessä tarkasteltiin vesihuoltolaitosten koon merkitystä suhteessa asukaspohjaan ja todettiin, että selviytyäkseen arkipäivän haasteista ja pystyäkseen kehittämään toimintaansa vesihuoltolaitoksen asukaspohjan on oltava vähintään noin 50 000 asukasta. Yli 100 000 asukkaan asukaspohjalla laitoksella on edellytykset vesihuoltotoimintojen prosessien parantamiseen, kun laitos pystyy houkuttelemaan monipuolista osaamista henkilöstöön. Vesihuoltolaitosten mittakaavaa kasvattamalla voidaan siis parantaa osaamista ja turvata resursseja. Keskeistä on myös, että tunnistetaan vesihuollon rooli yhteiskunnan kannalta kriittisenä palveluna ja

eriytetään toiminta muusta kuntaorganisaatiosta siinä määrin, että riittävät resurssit myös esimerkiksi kyberturvallisuuden järjestämiseksi pystytään varmistamaan.

Kyberturvallisuuden hoitamisessa voidaan harjoittaa alueellista yhteistyötä esimerkiksi häiriötilanteisiin varautumisessa ja reagoinnissa tai yhteisen valvontaringin muodossa. Yhteistyömahdollisuuksia on myös esimerkiksi tietojärjestelmien kyberturvallisuusvaatimusten määrittämisessä etenkin laitoksilla, joilla on samoja järjestelmiä käytössä. Lisäksi kooltaan tai toimintaympäristöltään samantyyppiset vesihuoltolaitokset voivat hyötyä kyberturvallisuuteen liittyvästä yhteistyöstä ja kyberturvallisuuteen liittyvää vierihoitoa voidaan jossain määrin antaa tietyn alueen vesihuoltolaitoksille yhteisesti. Vesihuoltolaitosten kyberturvallisuudesta huolehtiminen täytyy viime kädessä kuitenkin tehdä kunkin laitoksen kohdalla erikseen, sillä esimerkiksi organisaatiorakenne, vastuutahot, kuntayhteistyö ja tietojärjestelmät ovat jokaisella omanlaisensa.

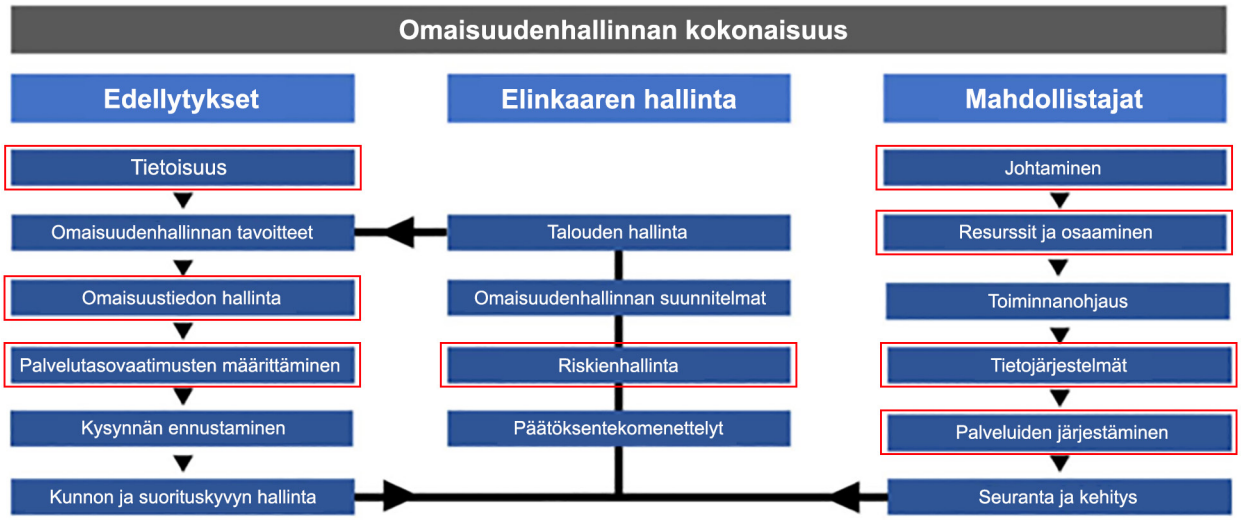
Omaisuudenhallinnan vahvistaminen

Selvityksessä kyberturvallisuuden arviointiin käytettiin Kybermittari-työkalua, jossa kuvataan hyviä käytäntöjä, joiden avulla organisaatio pystyy huomioimaan kyberturvallisuuden toiminnassaan. Hyvien käytäntöjen toteutuessa organisaation toiminta on systemaattista ja dokumentoitua. Kybermittarin kypsyystasojen saavuttaminen edellyttää palveluiden tuottamiseen tarvittavien prosessien, järjestelmien, tilojen ja laitteiden sekä toimitusketjujen tunnistamista ja dokumentointia. Kyberturvallisuutta edistetään mm. erilaisten rekisterien, suunnitelmien ja strategioiden kautta. Lisäksi edellytetään palvelun heikentymisen aiheuttamien seurannaisvaikutusten tunnistamista ja dokumentointia. Kybermittari edellyttää myös turvallisuuden- ja riskienhallinnan ohjeistuksen ja prosessien olemassaoloa, sekä kybertapahtumien ja -häiriöiden hallintasuunnitelmaa. Organisaatiolla tulee myös olla rekisteri toiminnon kannalta tärkeistä laitteista ja ohjelmistoista sekä tietovarannoista, ja organisaation tulee kerätä näiden käytöstä sekä näihin tehdyistä muutoksista lokia. Lisäksi organisaatiolla tulee olla jatkuvuussuunnitelma sekä suunnitelma kyberhäiriöihin reagointiin ja kyberarkkitehtuurin kehittämiseen.

Edellä kuvatun kaltaista systemaattista lähestymistapaa tarvitaan yleisesti silloin, kun tavoitellaan korkeatasoista omaisuudenhallintaa. Omaisuudenhallinnalla tarkoitetaan tässä laajaa käsitettä, jossa omaisuus kattaa kaiken vesihuolto-omaisuuden sisältäen verkostot, käsittelylaitokset ja digitaalisen omaisuuden, erotuksena Kybermittarin Asset-välilehteen, jossa käsitellään vesihuoltolaitoksen laite-, ohjelmisto- ja tieto-omaisuutta. Omaisuudenhallinnan standardi ISO55000 mukaisia omaisuudenhallinnan keskeisiä periaatteita ovat mm. yhdenmukaisuus, dokumentointi, läpinäkyvyys ja toistettavuus sekä riskiperustaisuus.

Omaisuudenhallinnan tason parantaminen on nostettu yhdeksi keskeisistä alan muutostarpeista Kansallisen vesihuoltouudistuksen ohjelmassa *(Maa- ja metsätalousministeriö 2021)*. Täyttääkseen Kybermittarissa esitetyt vaatimukset vesihuoltolaitoksen täytyy harjoittaa korkeatasoista omaisuudenhallintaa. Vesihuoltoalalla omaisuudenhallinta käsitetään usein saneeraustoiminnaksi, mutta oikeastaan omaisuudenhallinnalla tarkoitetaan johtamisjärjestelmää, jonka tavoitteena on maksimoida omaisuuden mahdollistama palvelu ja tuotettu arvo, sekä hallita siihen liittyviä riskejä *(Paavilainen 2019)*. Kuvassa 1 esitetään omaisuudenhallinnan kokonaisuus, johon on oranssilla merkitty osa-alueet, joista on löydettävissä suurimmat yhtymäkohdat Kybermittarin käytäntöihin.

Kuvassa 1 esitetyistä osa-alueista muodostuva hyvä omaisuudenhallinta toimii kyberturvallisuuden mahdollistajana. Kyberturvallisuus voidaan toisaalta kytkeä hyvin läheisesti omaisuustietoon ja vesihuoltolaitoksen tietojärjestelmiin, toisaalta myös osaksi johtamista, resursseja ja osaamista sekä palveluiden järjestämistä. Kyberturvallisuus on myös tärkeä osa vesihuoltolaitoksen riskienhallintaa sekä palvelutasovaatimusten määrittämistä. Toiminnan lähtökohtana on tietoisuus kyberturvallisuuden tärkeydestä ja kyberturvallisuustilanteesta.



Kuva 1. Omaisuudenhallinnan kokonaisuuden kytkeytyminen Kybermittariin. *(Paavilainen 2019 perusteella)*

Selvityksen keskeiset havainnot

Tässä raportissa esitetyn selvityksen perusteella vesihuoltolaitosten kyberturvallisuus on osin puutteellista ja tilanteen paranemisen edessä on esteitä. Osa vesihuoltolaitosten kyberturvallisuuteen liittyvistä puutteista on luonteeltaan teknisiä, käytännössä kunnan IT:n tai ulkoisen palveluntarjoajan hoidettavaksi tulevia toimia. Tällaisia ovat Kybermittarissa mainituista toimista esimerkiksi haavoittuvuusarviointien tekeminen ja lokitietojen kerääminen. Kuitenkin monet kyberturvallisuuden parantamiseksi vaadittavat toimet, myös tekniseltä kalskahtavat, edellyttävät koko vesihuoltolaitoksen toiminnan systemaattisuuden parantamista. Tällaisia ovat esimerkiksi kriteeristön määrittäminen kyberhäiriöille ja laiterekisteriin tehtävien muutosten arviointi ja hyväksyttäminen.

Vesihuoltolaitoksilla tehdään jo nyt paljon kyberturvallisuuteen liittyviä toimenpiteitä. Tämänhetkinen kyberturvallisuustekeminen on kuitenkin hajanaista. Laitoksilla voi olla paljonkin suullista ohjeistusta, mutta parannettavaa on ohjeistuksien, toimintamallien ja prosessien dokumentaatiossa. Lisäksi parannettavaa on kyberturvallisuuden huomioimisessa sopimuksissa, kunnan IT:n ja vesihuoltolaitoksen yhteistyössä sekä kyberturvallisuuteen liittyvän koulutuksen, harjoitusten ja yleisesti tietoisuuden lisäämisessä.

Projektiin osallistuneiden vesihuoltolaitosten ja tukkuvesiyhtiöiden määrä, 15 laitosta, oli varsin pieni, mikä aiheuttaa epävarmuutta tulosten yleistettävyyteen. Tulokset ovat kuitenkin samansuuntaisia kuin vuoden 2022 toimialakohtaisen selvityksen vesihuoltoa koskevat havainnot *(Huoltovarmuuskeskus 2022)*.

Selvityksessä suurimpana, taustalla vaikuttavana kehityksen esteenä esiin nousi resurssipula, joka on paikoin huutava. Vesihuoltolaitosten resurssien ollessa vähäiset laitosten henkilöstö joutuu priorisoimaan aikansa perustoiminnan ylläpitämiseen. Muita keskeisiä puutteita on se, että kyberturvallisuus koetaan hankalaksi aihepiiriksi, jonka merkitykseen ei ole vielä täysin herätty, ja se, ettei vesihuoltolaitosten ja kunnan tai kaupungin IT:n välillä ole riittävästi yhteistyötä. Resurssipula on jo aiemmin tunnistettu olennaiseksi kehittämistarpeeksi esimerkiksi Kansallisen vesihuoltouudistuksen ohjelmassa *(Maa- ja metsätalousministeriö 2021)*. Resurssipulasta kertoo tämän projektin toteutuksessa jo se, ettei suurta osaa Varsinais-Suomen ja Satakunnan vesihuoltolaitoksista edes tavoitettu tärkeän selvityksen tekemiseen ja osallistuneillakin oli vaikeuksia saada sovitettua projektia aikatauluihinsa. Myös haastateltavat ilmaisivat resurssipulan yhdeksi esteeksi kyberturvallisuuden kehittämiselle. Jos Kybermittarin täyttäminen on ylivoimaista useimmille laitoksille, on suuri vaara, että myös kyberturvallisuuden eteen tehtävät toimet jäävät vähäisiksi. Osaltaan resurssipula on puutetta henkilöresursseista ja rahasta, mutta myös kyberturvallisuusosaamisesta.

Selvityksen perusteella kyberturvallisuus nähdään vesihuoltolaitoksilla usein vaikeasti lähestyttävänä ja vesihuollon ydintekemisestä irrallisena

asiana. Etenkin johdolle tarvittaisiin lisää koulutusta erilaisten kyberhäiriöiden ja -hyökkäysten vaikutuksesta toiminnan jatkuvuuteen ja jatkuvan riskienhallinnan merkityksestä häiriöihin varautumisessa. Kyberturvallisuuskoulutusta tarvitsevat myös omistajat ja kuntapäättäjät. Tilanteen parantamisessa olennaista on, että vesihuoltolaitosten lisäksi myös vesihuollon järjestämisestä vastaavat kunnat ottavat vastuun kyberturvallisuudesta. Vesihuoltolaitoksen johdon tehtäväksi jää viestiä tehokkaasti ja ymmärrettävästi kyberturvallisuuteen liittyvät tarpeet. Monilla haastatelluista vesilaitoksista ohjaavat dokumentit kuten riskienhallintasuunnitelma laaditaan koko kunnan tasolla. Tällöin on tärkeää, että ymmärretään vesihuollon merkitys huoltovarmuuden keskiössä ja huomioidaan suunnitelmassa vesihuollon tarpeet kokonaisuudessaan, myös kyberturvallisuuden osalta.

Kyberturvallisuus edellyttää vesihuoltolaitoksen toiminnan kokonaisvaltaista kehittämistä ja on siten vaativa tehtävä. Tämänhetkinen lainsäädäntö ei aseta selväsanaisia vaatimuksia kyberturvallisuuden suhteen ja tuleva NIS2-lainsäädäntö muuttaa tätä vain suurten laitosten kohdalla. Kyberturvallisuuden kehittäminen olisi luontevimmin kytkettävissä omaisuudenhallinnan kehittämiseen. Tilannetta sekä kyberturvallisuuden että yleisesti omaisuudenhallinnan osalta ei voida parantaa kertaluontoisilla toimilla esimerkiksi ulkoisen rahoituksen voimin, vaan nämä edellyttävät laajamittaista toiminnan systemaattisuuden parantamista ja riittävien resurssien turvaamista.

Kyberturvallisuuden tason kartoittamiseen selvityksessä käytetty Kybermittari todettiin hyväksi työkaluksi, vaikka siihen saatiinkin muokkausehdotuksia. Kybermittari koettiin turhan laajaksi ja raskaaksi käyttää, mutta tämä johtui ainakin osittain siitä, ettei kyberturvallisuus usein ollut aiheena kovin tuttu eikä tiedostettu, kuinka monenlaisia toimia kyberturvallisuudesta huolehtiminen edellyttää.

Johtopäätökset ja suositukset toimenpiteiksi

Selvityksen keskeiset päätelmät vesihuoltolaitosten kyberturvallisuustilanteesta ja sen parantamisesta on esitetty taulukossa 1.

Taulukko 1. Projektissa tunnistetut kehitystarpeet ja niihin liittyvät keskeiset johtopäätökset.

Kehitystarve	Keskeiset johtopäätökset
Resursointi	Monilla vesihuoltolaitoksilla on pulaa niin henkilöresursseista, rahasta kuin kyberturvallisuuteen liittyvästä osaamisesta. Resurssit on saatettava kuntoon kyberturvallisuuden varmistamiseksi.
Tietoisuus	Vesihuoltolaitosten, alan muiden toimijoiden ja kuntapäättäjien kyberturvallisuusosaamista on kasvatettava, jotta on selvää, kuinka keskeinen tekijä kyberturvallisuus on vesihuoltopalveluiden häiriöttömälle tarjoamiselle. Tietoisuuden lisääminen edellyttää myös jokaisen vesihuoltolaitoksen kyberturvallisuustilanteen kartoittamista.
Omaisuudenhallinta	Kyberturvallisuuden hallinnan parantaminen edellyttää omaisuudenhallinnan ja riskienhallinnan käytänteiden vahvistamista.

Kaikkein keskeisin kehitystarve on useimmilla vesihuoltolaitoksilla riittävien resurssien turvaaminen. Vesihuoltolaitokset ovat usein kuntien ja kaupunkien omistamia ja on näiden vastuulla turvata huoltovarmuuden keskiössä olevalle vesihuollolle resurssit, jotka riittävät myös toiminnan kyberturvallisuuden takaamiseen. Resurssitilanteen parantamiseen yksi vaihtoehto on laitoskoon kasvattaminen. Viime kädessä on kuitenkin omistajan ratkaistavissa, miten palvelut järjestetään kyberturvallisesti.

Vesihuoltolaitosten kyberturvallisuusosaamista on kasvatettava, jotta on selvää, kuinka keskeinen tekijä kyberturvallisuus on vesihuoltopalveluiden häiriöttömälle tarjoamiselle. Henkilöresurssien ja toiminnan rahoituksen lisäksi on kasvatettava alan kyberturvallisuusosaamista esimerkiksi koulutusten ja kyberturvallisuusharjoitusten kautta. Vesihuoltolaitosten ohella osaamista tarvitaan myös alan kumppanuusverkoston toimijoilla.

Tietoisuuden lisäämiseksi tarvitaan paitsi resursseja, myös tilannekuvan muodostamista kunkin vesihuoltolaitoksen kyberturvallisuudesta. Huolimatta siitä, että projektissa tuli Kybermittariin muokkausehdotuksia, Kybermittari todettiin toimivaksi apuvälineeksi tilannekuvan saamiseen ja tueksi osallistujien ymmärryksen parantamiseen. Keskeistä oli, että tilannekartoituksessa oli läsnä sekä vesihuollon että kunnan IT:n osaajia. Kybermittaria tuntevan ulkopuolisen asiantuntijan tuesta oli etua Kybermittarin täytössä ja tuettu vastaaminen olikin yksi projektissa tunnistetuista hyvistä käytännöistä.

Kyberturvallisuuden tasoon on alettu kiinnittää huomiota ja kyberturvallisuutta lähdetään edelleen kehittämään selvityksen tulosten pohjalta. Vesihuoltolaitosten toiminnan systemaattisuutta täytyy parantaa ja liittää kyberturvallisuuden hallinta vahvemmin osaksi vesihuoltolaitoksen omaisuudenhallintaa ja kuntien riskienhallintaa. Vesihuoltoa koskevissa vaatimuksissa ja ohjeissa on tarve tuoda kyberturvallisuus nykyistä selkeämmin esiin. Omaisuudenhallinnan viitekehys tarjoaa puitteet toiminnan jatkuvalle parantamiselle myös kyberturvallisuuden osalta ja omaisuudenhallinnan perusprosesseja tulisi siksi vahvistaa. Tällaisia ovat esimerkiksi strategioiden, suunnitelmien, kriteeristöjen ja rekisterien laatiminen ja päivittäminen sekä toimintatapojen määrittäminen. Vastaavasti tulisi vahvistaa riskienhallinnan menettelyjä ja huomioida vesihuollon erityistarpeet kattavasti kuntien riskienhallintasuunnitelmissa.

Lähteet

Huoltovarmuuskeskus 2022. Toimialojen kyberkypsyyden selvitys 2022. Kansallinen koosteraportti.

Huoltovarmuusorganisaatio 2016. Vesihuoltolaitoksen opas häiriötilanteisiin varautumiseen. Huoltovarmuusorganisaatio, Vesihuoltopooli. Helsinki.

Kuivamäki, R., Kuulas, A., Makkonen, E., Renko, T. ja Laitala, R. 2023. Selvitys vesihuollon organisoinnista. Vesilaitosyhdistyksen monistesarja nro 87. Helsinki 2023.

Kuntalaki (410/2015) https://www.finlex.fi/fi/laki/ajantasa/2015/20150410

Kuntaliitto 2013. Kuntalain sisäistä valvontaa ja riskienhallintaa koskevien säännösten toimeenpano. Suositus. Korento, S., Ylitalo, M.-L. https://www.kuntaliitto.fi/sites/default/files/media/file/Sisainen_valvonta_09122013.pdf.

Maa- ja metsätalousministeriö 2021. Kansallisen vesihuoltouudistuksen ohjelma. Maa- ja metsätalousministeriön julkaisuja 2021:7. Helsinki 2021 https://mmm.fi/documents/1410837/6164691/KansallisenVesihuoltouudistuksenOhjelma.pdf/c0e480ef-cbd0-c63e-6f37-fb61621421a0/KansallisenVesihuoltouudistuksenOhjelma.pdf?t=1623735510993

Paavilainen, J. 2019. Vesihuoltolaitoksen omaisuudenhallinnan käsikirja. Vesilaitosyhdistyksen monistesarja nro 55. Helsinki 2019.

Sosiaali- ja terveysministeriön asetustalousveden laadusta ja valvonnasta sekä rakennusten vesilaitteistojen riskienhallinnasta (1352/2015). https://www.finlex.fi/fi/laki/ajantasa/2015/20151352

Terveydensuojelulaki (763/1994). https://www.finlex.fi/fi/laki/ajantasa/1994/19940763

Turvallisuuskomitea 2019. Suomen kyberturvallisuusstrategia 2019. Valtioneuvoston periaatepäätös 3.10.2019. https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia-2019/

Valmiuslaki (1552/2011) https://www.finlex.fi/fi/laki/ajantasa/2011/20111552

Valtioneuvoston asetus talousveden tuotantoketjun riskienhallinnasta ja omavalvonnasta (7/2023). https://www.finlex.fi/fi/laki/alkup/2023/20230007

Vesihuoltolaki (119/2001) https://finlex.fi/fi/laki/ajantasa/2001/20010119

Ympäristönsuojelulaki (527/2014). https://www.finlex.fi/fi/laki/ajantasa/2014/20140527

Kuvailulehti

Julkaisusarjan nimi ja numero: Raportteja 62/2023

Vastuualue: Ympäristö ja luonnonvarat

Tekijät: Ramboll Finland Oy

Julkaisun nimi: Kyberturvallisuus vesihuollossa, Suomen vesihuoltolaitosten kyberturvallisuustilanne ja sen kartoittamisen keinot

Tiivistelmä :
Kyberturvallisuus on olennaista yhteiskunnan välttämättömien toimintojen kuten vesihuollon kannalta. Kyberturvallisuuden parantamista edellyttävät sekä toimintaympäristön muutokset että EU-lainsäädäntö, jossa NIS2-direktiivi ja CER-direktiivi asettavat uusia vaatimuksia myös vesihuoltolaitosten toiminnalle.

Tässä raportissa esitetään suomalaisten vesihuoltolaitosten kyberturvallisuutta kartoittaneen projektin tuloksia. Projektissa kyberturvallisuuden tilan selvittämiseen käytettiin Kyberturvallisuuskeskuksen laatimaa Kybermittari -työkalua, joka on vapaasti saatavilla Kyberturvallisuuskeskuksen verkkosivuilta. Huolimatta siitä, että projektissa tuli Kybermittariin muokkausehdotuksia, Kybermittari todettiin toimivaksi apuvälineeksi tilannekuvan saamiseen ja tueksi osallistujien aihepiirin ymmärryksen parantamiseen. Kattavan tilannekuvan saamisessa keskeistä oli, että kartoituksessa oli läsnä sekä vesihuollon että kunnan IT:n osaajia.

Selvityksen perusteella vesihuollossa on toteutettu kyberturvallisuutta koskevia toimenpiteitä, mutta kyberturvallisuuden kehittämiseksi tarvitaan vielä lisää toimia. Tällaisia ovat esimerkiksi dokumentoinnin parantaminen ja kumppanuusverkon parempi hallinta. Vesihuoltolaitoksen ja kunnan IT:n välistä yhteistyötä on tarve kehittää ja alan kaikki toimijat sekä omistajat tarvitsevat kyberturvallisuuteen liittyvän koulutuksen ja tietoisuuden lisäämistä.

Selvityksessä suurimpana, taustalla vaikuttavana kehityksen esteenä esiin nousi vesihuollon paikoin huutava resurssipula. Resurssien suhteen ratkaisevassa asemassa on kuntaomistaja. Vesihuoltolaitokset ovat viime kädessä usein kuntien ja kaupunkien omistamia ja on näiden vastuulla turvata huoltovarmuuden keskiössä olevalle vesihuollolle resurssit, jotka riittävät myös toiminnan kyberturvallisuuden takaamiseen.

Kyberturvallisuuden tasoon on alettu kiinnittää huomiota ja kyberturvallisuutta kehitetään edelleen selvityksen tulosten pohjalta. Kyberturvallisuuden hallinta tulee liittää vahvemmin osaksi vesihuoltolaitoksen omaisuudenhallintaa ja kuntien riskienhallintaa, sillä ne tukevat toiminnan systemaattisuuden parantamista ja riskien minimointia. Vesihuoltoa koskevissa vaatimuksissa ja ohjeissa on tarve tuoda kyberturvallisuus nykyistä selkeämmin esiin.

Asiasanat: kyberturvallisuus, vesihuolto, huoltovarmuus

ISBN (PDF) 978-952-398-181-2
ISSN (verkkojulkaisu) 2242-2854
URN:ISBN: 978-952-398-181-2

Julkaisun osoite: www.doria.fi/ely-keskus

Sivumäärä: 15

Kieli: suomi

Kustantaja / Julkaisija: Etelä-Savon elinkeino-, liikenne- ja ympäristökeskus

Kustannuspaikka ja -aika: Mikkeli 6.10.2023

Presentationsblad

Publikationens serie och nummer: Rapporter 62/2023

Ansvarsområde: Miljö och naturresurser

Författare: Ramboll Finland Ab

Publikationens titel: Cybersäkerhet i vattenförsörjning, cybersäkerhetsläget i finska VA-anläggningar och metoder att kartlägga läget

Sammandrag:
Cybersäkerhet är grundläggande för samhällets nödvändiga funktioner, såsom vattenförsörjning. Förbättring av cybersäkerheten krävs p.g.a. förändringar i både verksamhetsmiljön och EU-lagstiftningen, där NIS2-direktivet och CER-direktivet ställer nya krav även på verksamheten hos vatten- och avloppsverk.

I denna rapport presenteras resultaten av ett projekt som kartlade cybersäkerheten hos finska vatten- och avloppsverk. I projektet bedömdes nivån på cybersäkerhet med hjälp av Cybersäkerhetscentrets Cybermätare-verktyg, som är fritt tillgängligt på Cybersäkerhetscentrets internetsida. Trots att det kom in förändringsförslag för att modifiera Cybermätaren under projektet, konstaterades det vara ett användbart verktyg för att bedöma den nuvarande situationen och för att förbättra deltagarnas förståelse av ämnet. En viktig aspekt för att få en heltäckande förståelse av den befintliga situationen, var att experter inom både vattenförsörjning och kommunal IT var närvarande under bedömningen.

Enligt bedömningen har cybersäkerhetsåtgärder genomförts inom vattenförsörjningen, men det krävs ytterligare åtgärder för att förbättra cybersäkerheten. Sådana åtgärder innebär till exempel förbättring av dokumentation och bättre förvaltning av leverantörer och övriga intressegrupper. Samarbetet mellan vatten- och avloppsverk och kommunal IT måste förstärkas, och alla aktörer och ägare inom branschen behöver utbildning och en ökad medvetenhet om cybersäkerhet.

Bedömningen identifierade som ett betydande hinder för utvecklingen en ställvis skriande brist på resurser inom vattenförsörjningen. När det gäller resurser spelar det kommunala ägarskapet en avgörande roll. Vatten- och avloppsverk ägs oftast av kommuner och städer, och det är deras ansvar att säkra resurser för den vattenförsörjning som är avgörande för försörjningsberedskapen. Dessa resurser bör även vara tillräckliga för att säkerställa verksamhetens cybersäkerhet.

Man har fäst uppmärksamhet på cybersäkerhetsnivån och cybersäkerheten utvecklas ytterligare baserat på rapportens resultat. Hanteringen av cybersäkerhet bör integreras mer i förvaltningen av tillgångar hos vatten- och avloppsverk samt i den kommunala riskhanteringen. Detta stöder en mer systematisk verksamhet samt en minimering av risker. Kraven och riktlinjerna för vattenförsörjning bör lyfta fram cybersäkerheten tydligare.

Nyckelord: cybersäkerhet, vatten och avlopp, försörjningsberedskap

ISBN (PDF) 978-952-398-181-2

ISSN (webbpublikation): 2242-2854

URN: URN:ISBN:978-952-398-181-2

Julkaisun osoite: www.doria.fi/ely-keskus

Språk: Finska

Sidantal: 15

Utgivare / Förläggare: Närings-, trafik- och miljöcentralen i Södra Savolax

Förläggningsort och datum: St Michel 6.10.2023

Documentation page

Publication serie and number: Reports 62/2023

Publication serie and number: Environment and Natural Resources

Author: Ramboll Finland Ltd

Title of publication: Water sector cyber security, the cyber security status of Finnish water utilities and the means to map it

Abstract:
Cyber security is essential for critical societal functions, such as water and wastewater services. The improvement of cyber security is necessitated by changes in the operating environment and EU legislation, in which the NIS2 directive and CER directive impose new requirements on the operations of water and wastewater utilities.

This report presents the results of a project that assessed the cyber security of Finnish water and wastewater utilities. In the project, the level of cyber security was assessed with the Kybermittari (Cybermeter) tool, which is developed by the National Cyber Security Centre and freely available on their website. Despite some proposed modifications to the tool during the project, it was found to be useful for assessing the current situation and improving the participants' understanding of the topic. It was found relevant that both water professionals and municipal IT experts were present during the assessment to get a full overview of the cyber security status.

According to the assessment, measures related to cyber security have been implemented in the sector, but further actions are needed. These actions include, for example, improvement of documentation and better management of third-party service providers. Collaboration between water and wastewater utilities and municipal IT needs to be strengthened, and all stakeholders and owners in the sector need training and increased awareness of cyber security.

The assessment identified a significant need for more resources at the utilities, which was seen as a major obstacle to development. Municipal ownership plays a crucial role in determining resource allocation. Water and wastewater utilities are often owned by municipalities and cities, and it is their responsibility to enable resources that ensure a sufficient level of cyber security.

Increased attention is being paid on cyber security, and further developments will be made based on the results of the project. Cyber security needs to be more clearly integrated into utilities' asset management and municipal risk management processes. These processes support a systematic approach and minimize risks. Additionally, aspects related to cyber security need to be addressed in the manuals and guidelines provided for the sector.

Keywords: cyber security, water services, security of supply

ISBN (PDF) 978-952-398-181-2

ISSN (online): 2242-2854

URN: URN:ISBN:978-952-398-181-2

Distributor: www.doria.fi/ely-keskus

Language: Finnish

Number of pages: 15

Publisher: Centre for Economic Development, Transport and the Environment for South Savo

Place of publication and date: the City of Mikkeli 6.10.2023

RAPORTTEJA 62 | 2023

KYBERTURVALLISUUS VESIHUOLLOSSA
SUOMEN VESIHUOLTOLAITOSTEN KYBERTURVALLISUUSTILANNE
JA SEN KARTOITTAMISEN KEINOT

Etelä-Savon elinkeino-, liikenne- ja ympäristökeskus

ISBN 978-952-398-181-2 (PDF)

ISSN 2242-2854 (verkkojulkaisu)

URN:ISBN:978-952-398-181-2

www.doria.fi/ely-keskus | www.ely-keskus.fi