

## Lehdistölyhennelmä

1. tilaisuus: Vesihuolto 2018
2. päivämäärä: 24.5.2018
3. esityksen otsikko: Kyberturvallisuus vesihuollossa, kyber-turva-vesihanke
4. esitelmöitsijän nimi: Heimo Pentikäinen
5. titteli: projektipäällikkö
6. organisaatio: Teknologian tutkimuskeskus VTT Oy
7. s-posti: heimo.pentikainen@vtt.fi
8. osoite: PL 1100, Kaitoväylä 1, 90570 Oulu

Kyber-turva-vesihankkeen tavoitteena on vesihuoltolaitosten automaatiojärjestelmien ja niihin liittyvien rajapintojen riskienhallinnan ja turvallisuuden kehittäminen. Painopiste on kyberturvallisuudessa. Hanke on 2 vuotinen, ajoittuen välille; kesä 2016 - kesä 2018. Osallistujina on kuusi vesihuoltolaitosta, rahoittajina osallistujien lisäksi ovat Huoltovarmuuskeskus ja Vesihuoltolaitosten kehittämisrahasto. Hankkeen toteuttaa Teknologian tutkimuskeskus VTT Oy.

Hankkeessa tehdään sekä yhteisiä ohjeita ja raportteja koko vesihuoltoalalle että osallistuville vesihuoltolaitoksille luottamuksellisia tehtäviä.

Hankkeessa on laadittu seuraavat ohjeet / raportit:

- i) Vaatimuspatteristo, jonka avulla voidaan selvittää säännöllisesti laitoksen kyberturvallisuuden tila. Patteristossa on runsaat sata vaatimusta jakaantuen hallinnollisiin ja teknisiin vaatimuksiin sekä vähimmäisvaatimuksiin, joita on n. 20. Patteristoa pystyy käyttämään yksinään tai asiantuntijan kanssa. Vaatimuspatteristo on taulukkolaskennan sovellus.
- ii) Lyhyet kyberturvallisuusohjeet vesihuoltolaitoksille, näitä A4-kokoisia ohjeita on 24 kappaletta. Tavoitteena, että lyhyistä ohjeista pystyy nopeasti katsomaan tärkeät kohdat.
- iii) Fyysinen turvallisuus kyberturvallisuuden näkökulmasta. Vesihuolto on usein luonnollisista syistä hajaantunut laajalle maantieteelliselle alueelle, tämä korostaa fyysisen turvallisuuden osuutta myös kyberturvallisuudessa,
- iv) Radiomodeemien, radiolinkkien sekä mobiili- että IoT-laitteiden kyberturvallinen käyttö vesihuollossa. Radiotekniikat ovat olleet merkittävässä asemassa vesihuollon arkipäivässä ja nykyisiä mobiilitekniikoita käytetään lisääntyvässä määrin myös vesihuollossa, raportissa luodaan katsaus näihin.
- v) Kyberturvallisuuden hallinta. Kyberturvallisuuden hallinnasta on luotu lyhyt hallintamalli, jossa hyödynnetään vuosikello-ajattelua.
- vi) Etäyhteydet. Etäyhteyksiä tarvitaan, mm. laajan alueen takia sekä päivystäjä että automaatiotoimittaja tarvitsevat usein yhteyden automaatioon. Raportissa tuodaan muutama esimerkki turvallisesta etäyhteydestä.
- vii) IDS:n (Intrusion Detection System - tunkeutumisen havaitsemisjärjestelmä) käyttö vesihuollossa. Raportti luo katsauksen tämän hetken IDS-sovelluksiin.

Eräänä yhteisenä asiana näissä ohjeissa ja raporteissa korostuu elinkaaren ja omaisuuden hallinnan tärkeys, joka onkin alkanut saada enenevässä määrin huomiota osakseen. Tarkka tieto automaatio-omaisuudesta, mm. laitteistot ja ohjelmistot versiotietoineen, antaa hyvän pohjan kyberturvallisuuden hallintaan ja kehittämiseen.

Hankkeessa on pidetty kyberturvallisuuden puolustamistyöpaja ja automaation elinkaarityöpaja. Kyberturvallisuuden puolustamistyöpajassa näytettiin tyypillisiä hyökkäysmenetelmiä ja harjoiteltiin niihin puolustamista. Automaation elinkaarityöpajassa oli teollisuuden edustajia mukana alustuksineen. Lisäksi johtoryhmän kokouksissa on ollut esityksiä kyberturvallisuuteen liittyvistä asioista, mm. turvallisuuskulttuurista ja IoT:stä sekä Viestintäviraston Kyberturvallisuuskeskuksen palveluista.