Vesilaitosten kyber-fyysiset riskit

Vesiyhdistyksen Vesihuoltojaoston syysseminaari

6.11.2019 Helsinki

VTT:n työryhmä: Työryhmä Riitta Molarius, Liisa Poussa, Tero Välisalo ja Heimo Pentikäinen

Teknologian tutkimuskeskus VTT Oy
Heimo Pentikäinen

Mitä on kyber?

Mitä on kyber? Dosentti Rauno Kuusisto:

**"*Kyber on maasto, jossa tehdään operaatioita. Operaatiot laitetaan toimeen ne mahdollistavilla työkaluilla ja menetelmillä ja osaamisella. Operaatioita johtavat ihmiset.*
Operaation menestyksen määrittää se asetelma ja ne voimavarat, jotka ennen operaatioita on rakennettu."**

Tämä määrittely löytyy Viestiupseeriyhdistys ry:n ja Maanpuolustuksen Viestisäätiö sr:n kustantamasta Kyberajan viestitaktiikka-kirjasta (2018).

Huomioita, kyber-vesihankkeesta (2016-2018)

- Kyberturvallisuutta ei rakenneta kerralla vaan se on jatkuva prosessi (ei projektiluonteinen työ), jatkuvan parantamisen periaate.
- Vesihuoltolaitoksia on monenlaisia ja monen kokoisia,
  - onneksi tekniset kyberturvallisuuden perussuojaukset ovat samanlaisia organisaation koosta riippumatta (mm. automaatiosta ei suoraa internet-yhteyttä ja tiukka palomuuri automaatio- ja toimistoverkon välille).
- Käyttäjän/sosiaalinen manipulointi (social engineering) herätti mielenkiintoa.
- Hankintojen ja palveluiden asema korostuu vesihuollon kyberturvallisuudessa.
- Yleisturvallisuus on vesihuoltolaitoksilla hyvin ymmärretty ja tähän on hyvä rakentaa myös kyberturvallisuutta, joka voidaan nähdä osana kokonaisturvallisuutta.

Internetissä jokainen päivä on aprillipäivä!

Ohjeet

- AI-tekniikat IDS-järjestelmien tukena vesihuoltolaitosten tietoturvan parantamisessa
- Lyhyet kyberturvallisuusohjeet vesihuoltolaitoksille
- Vesihuoltolaitoksen kyberturvallisuuden hallinta
- Vesihuoltolaitosten etäyhteysratkaisut
- Vesihuoltolaitosten radio-, mobiili- ja IoT-laitteiden kyberturvallisuus
- Vesihuoltolaitosten **kyberfyysinen** turvallisuus
- *Tekninen katsaus:* Versionhallinta

Ohjeet ja työkalut ovat saatavilla Vesilaitosyhdistyksen extranetissä:

- www.vvy.fi/extranet/julkaisut/varautuminen/kyberturvallisuus/

Lyhyet kyberturvallisuusohjeet vesihuoltolaitoksille

- Vähimmäisvaatimukset
- Fyysinen pääsynvalvonta
- Ohje vierailijoille
- Verkon pääsynhallinta
- Prosessin ohjausjärjestelmien salasanat valvomossa
- Sähköpostin käyttö
- Sosiaalinen manipulointi
- Automaatiojärjestelmän elinkaari, arkkitehtuuri ja koventaminen
- Kannettavat tietokoneet ja oheislaitteet
- Langattomat laitteet vedenkäsittelyprosessin tiloissa
- Internetin käyttö tuotantoalueella
- Etäyhteydet
- Laitetilat, -kaapit, laitteet, johdot
- Ohjelmistojen asennus
- IoT –anturit
- Sopimukset
- Kyberturvallisuuspolitiikka

Vesihuoltolaitosten kyberfyysinen turvallisuus

- Tavoitteena on tuoda esille fyysisiä asioita, joilla voi olla vaikutusta kyberturvallisuuteen.
- Finanssiala ry:n ohjeet sekä valtionhallinnon VAHTI-ohjeet antavat erittäin hyviä ja mietittyjä selkeitä ohjeita, joita voi käyttää myös vesihuollossa.
- Esimerkkejä mahdollisista tapahtumista:

4.2 Puutteellinen lukitus etäasemalla

- **Tapahtuma:** Etäpumppaamolla oli huono lukitus ja ilkivallan tekijä pääsi varastamaan radiomodeemin.
- **Seuraus:** Pumppaamon tilaa ei saatu selville valvomosta, vaan piti mennä paikan päälle. Koska ei ollut varalaitteena valmiiksi konfiguroitua radiomodeemia, jouduttiin etäpumppaamoa hoitamaan pumppaamolla yli työpäivän, kunnes saatiin uusi radiomodeemi asennettua.
- **Suojaus:** Kunnollinen Finanssialan suosittelema lukitus sekä valmiiksi konfiguroitu varalaite.

VTT

1) Kokonaisturvallisuuden hallinta

2) Jatkuvasti päivittyvä ja kehittyvä riskienhallintaprosessi

3) Ennakointi, varautuminen ja palautuminen

Tekniikka & Talous 25.1.2019

Vesihuolto heräsi kyberuhkiin

Palvelunestohyökkäys valpastutti Vaasan, HSY:llä murtoyrityksiä jatkuvasti

VESIHUOLTO / Vesihuoltolaitokset saivat viime vuoden lopussa räntälöydyt ohjeet kyberuhkian varautumiseksi, kun Huoltovarmuuskeskuksen, Vesilaitosyhdistyksen ja VTT:n kaksivuotinen Kyber-vesi-hanke päättyi.

Pääkaupunkiseudulla toimivalla HSY:llä kybertarvaan alettiin kiinnittää enemmän huomiota jo muutama vuosi sitten.

"Meillä herättiin siihen, että käytössä on paljon vanhaa teknologiaa ja käyttäjiä, jotka voisivat olla turvallisempia", sanoo tietohallintopäällikkö **Mikko Lindholm**.

Konsultin tekemässä kartoituksessa nousi esiin, että kybertarva-asiat eivät kuuluneet oikein kenellekään eikä selkeitä toimintapoja ollut.

"Kybertarva-asioille nimettiin vastuuhenkilö, ja teimme tietoturvapolitiikan."

Parhaillaan HSY:lle ollaan palkkaamassa ensimmäistä varsinaista tietoturva-asiantuntijaa.

"Nyt meillä alkavat olla edellytykset kunnossa", Lindholm sanoo.

HSY OLI yksi Kyber-vesi-hankkeeseen osallistuneista vesilaitoksista.

"Siinä kartoitettiin laitosten automaatiojärjestelmiä ja saimme hyödyllistä tietoa, jota olemme alkaneet soveltaa toiminnassa."

Selvityksen kohteena olivat riskipaikat ja se, miten riskejä voidaan pienentää.

"Vesihuoltolaitoksilla on erittäin hyvä pohja, koska ne ymmärtävät kokonaisturvallisuuden ja asemansa Suomen kriittisessä infrastruktuurissa", sanoo hanketta koordinoinut **Helmo Pentikäinen** VTT:ltä.

Huoltovarmuuskeskuksen valmiusasiamies **Riku Juhola** puolestaan korostaa, että kybertarvallisuuden on oltava osa laitoksen kokonaisturvallisuutta.

"Uhkakuva ei ole stabiili. Kyseessä ei ole projekti vaan prosessi, jonka tulee jatkua koko ajan ja jota pitää päivittää."

PETTERI PAALASMAA

VESIHUOLTOLAITOKSIA koskevat samanlaiset uhat kuin muitakin yrityksiä: rahan saantiin pyrkivät haittaohjelmat ja kiristys- sekä huijausohjelmat, valeilaskut ja palvelunestohyökkäykset.

Lisäksi vesihuolto ja etenkin juomavedenjakelu yhteiskunnan peruspalveluna voivat olla vakavan häiritsemisyrityksen kohde.

"Jos juomavedentuotantoa kohtaan hyökätään, motiivina voi olla terrorimi tai toisen valtion aiheuttama häiriintä. Nämä ovat ehkä vakavimpia uhkia. Siksi on motiivina ei ole saada rahaa, vaan pyrkiä häiritsemään toimintaa ja luoda epävakautta", Lindholm sanoo.

Vesihuoltopiireissä näistä uhkista puhutaan Lindholmin mukaan melko paljon, mutta vakavilta hyökkäysyrityksiltä on Suomessa välttyty.

"Kyberhyökkäyksiä vesilaitoksia vastaan on tehty maailmalla, mutta ei Suomessa", hän sanoo.

Palomuureista sen sijaan yritetään HSY:lläkin tulla ahkerasti läpi.

"Se on ihan normaalia, ja näitä murtoyrityksiä on jatkuvasti, kuten varmasti joka yrityksessä. Niihin varautuminen on arkipäivää", Lindholm sanoo.

> "Joitakin vuosia sitten oltiin vähän ruususen unessa."

SUOMEN SUURIMPANA vesilaitoksena HSY:llä on hyvät eväät huolehtia kyberturvasta. Vesilaitoksia on Suomessa kuitenkin noin 1 500, joista suurin osa on hyvin pienilä.

"Pienemmät itsenäiset vesilaitokset ovat haasteellisen paikan edessä. Niillä ei välttämättä ole pätevämpiä it-henkilöitä lainkaan. Toisaalta ne eivät ehkä ole yhtä kiinnostavia kohteita", Lindholm pohtii.

Kyber-vesi-hankkeen yhteydessä syntyi myös vesialalle oma Kybertarvallisuuskeskuksen alainen Isac-ryhmä (Information Sharing and Analysis Centre) tiedonvaihtoa varten.

"Jos meillä on hyviä kokemuksia tai käyttäjiä, voimme jakaa niitä muille. Laitosten kesken on oikeesti siinä hyvä perime", Lindholm sanoo.

Isac-ryhmissä tietoturva-asioita käsitellään luottamuksellisesti osallistujien kesken. Samalla lisätään organisaatioiden tietoturvaosaamista ja Kybertarvallisuuskeskus pyssy kärryillä kokonaistilanteesta.

LINDHOLMIN mukaan muutamassa vuodessa vesialalla on tapahtunut suuri muutos ajatteluta vassa.

"Joitakin vuosia sitten oltiin vähän ruususen unessa ja asiaan suhtauduttiin aika huolettomasti."

Esimerkiksi Vaasan vesi herätki kyberuhkiin muutama vuosi sitten, kun siihen kohdistui palvelunestohyökkäys.

"Huomasimme, että joku yrittäi päästä serverille. Sen jälkeen aloimme panostaa kybertarvallisuuteen", kertoo verkostopäällikkö **Jari Jantunen**.

Laitoksen koneet ovat irti valtakunnan verkosta, ja panostuksia kybertarvaan on tehty etenkin vedentuotannon puolella.

"Tietoturva on siitä hankala asia, että niin kauan kuin kaikki on hyvin, kukaan ei huomaa mittään. Se näkyy vasta, jos joitain ikävää tapahtuu", Lindholm sanoo.

MIINA RAUTIAINEN

Isac-ryhmät

- Elintarviketuotanto ja -jakelu: 25 jäsentä
- Energia-ala: 19
- Internet-palvelun-tarjoajat: 21
- Kemia- ja metsäteollisuus: 17
- Media: 19
- Sote: 16
- Valtionhallinto: aktiivisia osallistujia noin 40
- Vesi: 21
- Logistiikka: alkaa vuonna 2019
- Pankit: ryhmä uudistuu laajemmaksi finanssialan ryhmäksi
- Ohjelmistovalmistajat: sähköpostilista, jolla 170 vastaanottajaa

LAAJA KENTTÄ. HSY:llä on hyvät mahdollisuudet huolehtia kybertarvastaan. Tietohallintopäällikkö Mikko Lindholmin mukaan kyberuhka aiheuttaa enemmän pääänvaivaa pienille itsenäisille vesilaitoksille, joita on Suomessa satoja.

Huoltoväli harvenee iot:lla

Tietoturva on yhä ajankohtaisempaa, kun vesihuoltoa digitalisoidaan. Uusin iot-sovellus ovat älykkäät vesimittarit, jotka lähettävät kulutustietoa vesilaitoksille jopa reaaliaikaisesti.

Verkko-operaattori Digita rakentaa Suomeen iot-tiedonsiirtoverkkoa, joka soveltuu pienten laitteiden kuten vesimittareiden keräämän datan siirtoon. Käytössä on Lorawan-teknologia, joka on melko uusi langaton iot-tiedonsiirtoteknologia.

"Se tarjoaa hyvät eväät tietoturvallisiin ratkaisuihin. Verkko on täysin'erillinen. Anturit eivät ymmärrä internet-protokollasta mittään, eli ne ovat teknologiamuurin eristämiä internetistä", sanoo Digitan iot-palvelujohtaja **Ari Kuukka**.

Laitteet eivät voi edes teoriassa olla yhteydessä internettiin, eikä niihin pääse ulkopuoleita käsiksi. Lisäksi tieto on vahvasti salattu. Vaikka tiedonsiirto mittarilta laskutukseen onnistuisi, tietoturvan täytyy olla kunnossa myös siellä, missä dataa hallitaan ja varastoidaan.

"Tietoturva on monen tekijän summa. Kaikkien ketjun lenkkien pitää olla vahvoja."

Vesimittareiden lisäksi iot-ratkaisu soveltuu esimerkiksi pohjaveden pinnankorkeuksien tai putkistojen paineiden seurantaan.

Tähän asti anturoiden käyttö ei ole kannattanut, koska ne ovat vaatineet huoltoa tai paristojen vaihtoa liian usein. Uuden teknologian avulla laitteet pysyvät toimintakuntoisina jopa 5–10 vuotta.

Yksi Digitan asiakkaista on Vaasan vesi, joka otti viime vuonna käyttöön ensimmäiset 50 mittaria. Tieto vedenkulutuksesta siirtyy kotimittarista suoraan laskutukseen, mikä vähentää työtä vesilaitoksella.

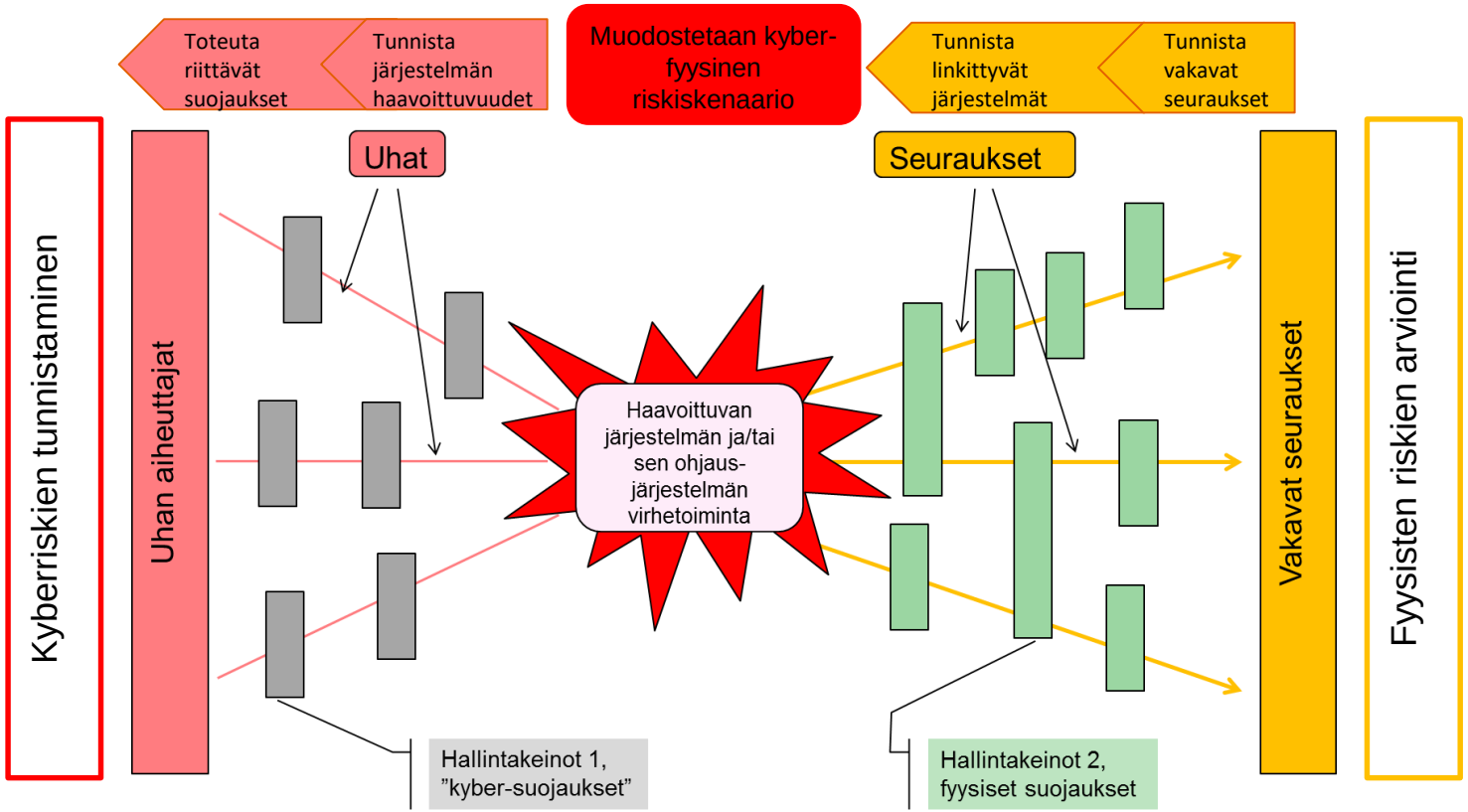
Taustaa kyberfyysiseen näkökulmaan

- Fyysisen infrastruktuurin lisäksi osa kriittistä infrastruktuuria on kriittinen informaatioinfrastruktuuri (CII).
- Infrastruktuuri on enenevässä määrin verkostomainen fyysisten laitteiden, rakennusten ja informaatioverkostojen systeemi, jonka rajoja on haastava määrittää.
- Yleisesti teknisiä järjestelmiä ja tieto-/automaatiojärjestelmiä koskevaa riskienhallintaa toteutetaan erillään toisistaan.
- Verkottuneessa toimintamallissa tarve yhdistää em. riskienhallintaprosessit
- **Kehitetään menettelytapa, joka tukee riskien tunnistamista kyber-fyysisessä ympäristössä**

Riski käsitteenä

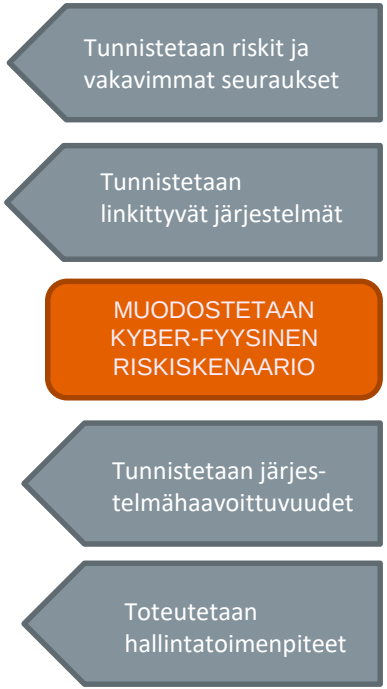
INFORMAATIO-INFRASTRUKTUURI		FYYSINEN INFRASTRUKTUURI
Ei konkreettinen, vaikea määritellä	**Kohteen määrittely**	Konkreettinen rakenne, rajat määritettävissä
1-20 vuotta	**Elinkaari**	20-100 vuotta
Muuttuvat jatkuvasti	**Uhkat ja haavoittuvuudet**	Staattisempia, muutokset hitaita
Vaikea arvioida	**Toteutumisen todennäköisyys**	Arvioitavissa
Vaikea hahmottaa ja arvioida	**Seuraukset**	Hahmotettavissa ja suuruus arvioitavissa

Kyber-fyysinen lähestymistapa



Menettely kyber-fyysisten riskien tunnistamiseen

- Fyysisten riskien tunnistaminen kohteeseen soveltuvalla menetelmällä. Valitaan seurauksiltaan pahimmat riskit.
- Tunnistetaan fyysiset laitteet, hallinta- ja tietojärjestelmät, jotka linkittyvät tunnistettuun riskiin.
- Kuvataan kyber-fyysinen riskiskenaario, joka yhdistää prosessi-/laitoshenkilöstön ja tietojärjestelmä-asiantuntijoiden näkemykset – Kuinka riski voisi toteutua?
- Tunnistetaan tieto- ja hallintajärjestelmiin liittyvät haavoittuvuudet sekä fyysisen järjestelmän rajoitteet.
- Päätetään ja toteutetaan riskienhallintatoimenpiteet.



Menettelyn testaaminen

- Menetelmää on testattu vesihuoltolaitoksessa. Testaaminen tehtiin työpajatyöskentelynä, johon osallistui 12 henkilöä. Edustus sekä prosessi että ICT puolelta.
- Analyysin tarkoitus: Tunnistaa riskit, joilla on vaikutusta veden laatuun tai määrään vedenpuhdistusprosessin loppupäässä (aktiivihiilisuodatuksesta verkostoon pumppaamiseen).
- Fyysisten riskien tunnistaminen ja arviointi VTT:n kehittämällä HAZSCAN–turvallisuusanalyysimenetelmällä (Hazard Scanning), joka hyödyntää POA:a (Potentiaalisten Ongelmien Analyysi) ja tarkistuslistoja sekä toimintaprosessien kuvaamisen.
  - Tietotarpeita: prosessikaaviot, laitteet, virtaamat, käytetyt kemikaalit, työkäytännöt, aikaisemmat riskianalyysit.
- Keskityttiin vain pahimpiin seurauksiin (oletettiin, että esikäsitelty vesi on puhdasta lähtötilanteessa – oletuksia voi tehdä).
- Tunnistettiin kriittisiin kohteisin liittyvät ohjausjärjestelmät ja laitteet sekä verkkoyhteydet sekä arvioitiin kriittisten laitteiden haavoittuvuutta.
  - Tietotarpeita: tietoverkon rakenne, järjestelmäkaaviot, automaatioyhteydet, yhteydet muihin järjestelmiin, laitteiden mallit ja toimittajat.

Yleisiä tuloksia menetelmän testaamisesta

- Tärkein osa kyberfyysistä riskianalyysiä on kyberfyysisen riskiskenaarion muodostaminen, koska se konkretisoi seuraukset ja niiden toteutumismekanismit sekä luo yhteisen ”kielen ja kartan” analyysiin osallistujille.
- Tarkoituksellisen haitanteon näkökulma tuotava mukaan analyysiin heti alusta alkaen.
- Luontainen turvallisuus (Inherent safety) -periaate laitossuunnittelussa on hyvä asia myös kyberriskien hallinnassa (esim. kemikaalipumppujen kapasiteetti, säiliöiden maksimi tilavuus).
- Mikäli hakkeri pystyy tunkeutumaan hallinta ja ohjausjärjestelmiin, potentiaalisia vaikutuskohteita löytyy useita. Veden määrään helpompi vaikuttaa kuin laatuun.
- Julkisuus voi mahdollistaa haavoittuvuuksien hyödyntämisen (esim. opinnäytetyöt, kilpailutukset).
- Julkisesti saatavia tietoja etsitään mm. OSINT-analyysillä (Open Source INTellicence gathering).

Yhteystiedot

- VTT on innokas käyttämään ja edelleen kehittämään tässä esiteltyä menetelmää vesihuollon hyväksi.

- Ota rohkeasti yhteyttä:
  - Liisa Poussa, s-posti: Liisa.Poussa@vtt.fi
  - Tero Välisalo, s-posti: Tero.Valisalo@vtt.fi
  - Sami Noponen, s-posti: Sami.Noponen@vtt.fi
  - Riitta Molarius, s-posti: Riitta.Molarius@vtt.fi
  - Heimo Pentikäinen, s-posti: Heimo.Pentikainen@vtt.fi

Kiitos!