Kyberturvallisuus pienillä laitoksilla

Katja Kotalampi
Vesihuoltoyksikkö, Patamäenkatu 24, Tampere

Tausta

Katja Kotalampi, jätevesiasiantuntija, KVVY Tutkimus Oy

- Aloittanut KVVY Tutkimus Oy:lla 25.4.2022 alkaen
- Toiminut aiemmin Virtain kaupungin vesihuoltopäällikkönä 5 vuotta, Ikaalisten Vesi Oy:lla vuoden määräaikaisena työhön osallistuvana työnjohtajana
- Vesihuollossa töissä jo yli kymmenen vuotta (esim. verkostokartoitukset)
- Koulutustausta: Ympäristöteknologian insinööri 2014, Vesihuoltomestari 2021

Kyberturvallisuus pienillä laitoksilla

Kyberrikollisuus vs. kyberturvallisuus

- Kyberrikollisuus on rikollisuutta, joka kohdistuu tietoverkkoihin ja tietojärjestelmiin, tai tehdään niitä hyödyntäen. Kyberrikoksia ovat esimerkiksi tietojenkalastelu, palvelunestohyökkäykset, tai suora sabotaasi järjestelmiin.

- Tietomurrot, haittaohjelmat ja sosiaaliset huijaukset ovat tyypillisimpiä keinoja varastaa ja hyväksikäyttää esim. salasanoja, käyttäjälleen tärkeitä tietoja tai estää kriittisten tietojärjestelmien toiminta.

- Kyberturvallisuus taas on tilanne, jossa kybertoimintaympäristön toiminta on turvattu ja siihen voidaan luottaa. Kyberturvallisuuteen sisältyy toimenpiteet, joilla voidaan ennaltaehkäistä ja sietää kyberuhkia ja niiden aiheuttamia vaikutuksia. Kyberhyökkäyksen tapahtuessa on olemassa toimintamalli, jonka avulla toiminta pystytään palauttamaan.

Kyberturvallisuus pienillä laitoksilla

Miksi kyberturvallisuus on nykyaikana tärkeää myös pienillä laitoksilla?

- Nykyaikana kaikki internetiä käyttävät ovat verkkorikollisten kohteita. Verkkorikolliset voivat tehdä kohdennettuja hyökkäyksiä isoihin organisaatioihin mutta myös pieniin.
- Nykyajan yhteiskunta on erityisen riippuvainen toimivista tietojärjestelmistä sekä internetistä. Kyberhyökkäyksellä voidaan vaurioittaa laitosten toimintaa, tai jopa pysäyttää kaikki tietojärjestelmien ohjaukset.
- Kyberrikosten määrä on kasvanut niin arkipäiväiseksi toiminnaksi, ettei edes suurinta osaa tietomurroista pystytä enää selvittämään.
  - Yle Uutiset : Tietomurtoja tapahtuu nyt enemmän kuin koskaan, mutta rikollisia ei saada kiinni – Viime vuonna 96 prosenttia tapauksista jäi selvittämättä (27.8.2022)
- Erityisesti Ukrainassa käytävä sota on lisännyt kyberturvallisuuden huomiointia, sillä maailmantilanne on epävarma.
- Tärkein toimintamalli on ehkäistä hyökkäyksiä ja varmistaa omien järjestelmien takaisin palauttaminen mahdollisimman nopeasti.

Kyberturvallisuus pienillä laitoksilla

Yksinkertaisimmat muistisäännöt ja toimenpiteet, joita jokainen yksilö voi tehdä

- Käytä jokaisessa käyttäjätilissä vahvaa ja ainutkertaista salasanaa. Tärkein muistisääntö on, että salasana on riittävän pitkä, mieluiten 15 merkkiä. Mitä pidempi salasana on, sitä haastavampi se on murtaa.
- Lisäksi tulee muistaa, että salasanassa ei käytä mitään liian tunnistettavia henkilöön liittyviä sanoja tai sanayhdistelmiä.
- Käytä kaksivaiheista tunnistusta aina kun se on mahdollista.
- Mikään organisaatio, yritys, tai sovellus ei kysy käyttäjän salasanoja, pankkitietoja, tai lähetä epämääräisiä linkkejä klikattavaksi.
- Myös huijaussoitot ovat moninkertaistuneet, jolloin on tärkeää muistaa varmistaa, että soitto on aito. Jos puheluita ulkomailta ei ole odotettavissa, kannattaa tarkistaa numero ennen vastaamista.

Kyberturvallisuus pienillä laitoksilla

Yksinkertaisimmat muistisäännöt ja toimenpiteet, joita jokainen yksilö voi tehdä

- Käytä vain virallisilta sivuilta tai virallisista sovelluskaupoista saatavia ohjelmistoja.
- Pidä ohjelmistot kaikissa laitteissa ajan tasalla, sillä päivityksillä varmistetaan, että uudet tietoturva-aukot korjataan
- Käytä luotettavia tietoturvaohjelmistoja
- Älä koske tuntemattomiin tai epäilyttäviin linkkeihin
- Nykyaikana jokainen työntekijä on työnantajalleen voimavara mutta myös tietoturvariski, jos näihin asioihin ei kiinnitetä huomiota. Tietomurto voi tapahtua kenen tahansa kautta.

Kyberturvallisuus pienillä laitoksilla

Kriittiset järjestelmät

- Valvomokoneen toiminnan varmistaminen tehdään yksinkertaisilla asioilla:
- Valvomokonetta käytetään ainoastaan laitoksen ohjaukseen, eikä sillä käytetä internetiä normaalitilanteessa
- Valvomokoneelle ei asenneta ylimääräisiä ohjelmistoja ja sen ohjelmat pidetään jatkuvasti ajan tasalla. päivityksissä korjataan havaittuja tietoturvariskejä ja ennakoidaan uusien syntymistä.
- Jos valvomokoneelle on salasanoja, ne ovat mieluiten yksilöityjä jokaiselle käyttäjälle. Näin voidaan tarvittaessa löytää tapa, jolla tietomurto on pystytty tekemään.
- Käyttäjätunnuksia sekä salasanoja ei säilytetä missään näkyvissä (pöydillä, kalentereissa, puhelimissa). Erilliset salasanoja varten luodut säilytysjärjestelmät ovat eri asia.
- Valvomokoneelle ei ole fyysisesti ulkopuolisilla suoraa pääsyä.

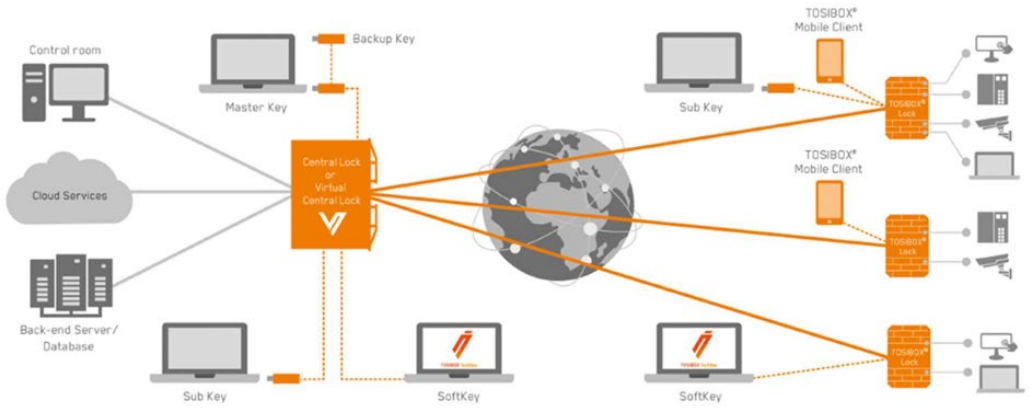
Kyberturvallisuus pienillä laitoksilla

Kriittiset järjestelmät

- Isoissa organisaatioissa (kunnissa yms.) olisi tärkeää, että valvomokoneen tai koko vesihuollon internet/tietojärjestelmät eivät ole suoraan yhteydessä muihin kunnan organisaation järjestelmiin. Ne on suositeltavaa irrottaa niin sanotusti omiksi kokonaisuuksikseen.
  - Riskit kasvavat, mitäs enemmän riskialttiita käyttäjiä on olemassa. Vertaa esim. 300 käyttäjää vs. 3-10 henkilöä.
- Laitokselle ja valvomokoneelle, jos otetaan etäyhteys esim. TeamViewerin kautta, tulee olla määriteltynä kellä on oikeudet kirjautua etänä ja/tai muodostaa oikeudet laitekohtaisesti. Tässäkin tapauksessa salasanojen tulee olla ns. vahvoja.
- Tosi-Box on kaksivaiheinen tunnistautuminen, jolla varmistetaan, ettei laitoksen järjestelmiin päästä helposti. Sen käyttäminen on suositeltavaa, jos muuta vahvennettua tunnistautumista ei ole käytössä. Tosibox:n toimintaperiaate muistuttaa mekaanisen lukon ja avaimen toimintaa.

Kyberturvallisuus pienillä laitoksilla

Kuva: Verkkokauppa.com



Kuva 8. Tosiboxin topologia: yhteys voidaan muodostaa suoraan Lukkoon tai välityspalvelunkautta Keskuslukolla. [11.]

Lähde: Hirvikallio, Joni. 2020.
Rakennusautomaatiojärjestelmän etävalvomo ja sen käyttöönotto
Insinöörityö

Kyberturvallisuus pienillä laitoksilla

Kriittiset järjestelmät

- VPN – Eli virtuaalinen erillisverkko, on tehokas tapa yksityisyyden turvaamiseen internetissä. Käytännössä VPN toimii ns. tunnelina internetyhteydellesi, jolloin kukaan ulkopuolinen ei voi nähdä mitä teet internetissä.

- Sen sijaan, että yhdistäisit suoraan internetiin, yhteytesi kulkee VPN-palvelimen kautta, joka salaa verkkoliikenteesi. Kun VPN-yhteys piilottaa IP-osoitteesi, voit suojata sillä yhteytesi myös julkisissa WiFi-verkoissa.

- VPN-palveluntarjoaja pitää valita tarkkaan, ja varmistaa, että heitä velvoittavat vahvat tietosuojalait, jotta tietoja ei käytetä väärin. VPN-yhteyden voi parhaimmillaan rakentaa myös itse.

Kyberturvallisuus pienillä laitoksilla

Kriittiset järjestelmät, entä jos jotain tapahtuu?

- Käytännöllisiä perusratkaisuja on esimerkiksi se, että valvomokoneesta on olemassa täydellinen fyysinen kopio. Tai käytännössä vanhempi valvomokone, joka on päivityksen yhteydessä jätetty varakoneeksi.
- Valvomokoneen sisällöstä on olemassa aina kopio pilvessä, kovalevyllä tai jossain kunhan se on olemassa. Kunta organisaatioissa on yleensä olemassa vakiona koneiden varmuuskopiointi, mutta sekin kannattaa varmistaa.
- Organisaation sisällä on olemassa toimintamalli, mitä tehdään, jos järjestelmät ajetaan hyökkäyksen yhteydessä alas. Mistä saadaan apua, varaosia tai osaamista?
- Käykää keskustelua niin organisaation oman tietohallinnon kuin ulkopuolisten osaajien kanssa, jotta löydätte omalle toiminnallenne parhaat tavat toimia.

Kyberturvallisuus pienillä laitoksilla

Kriittiset järjestelmät, entä jos jotain tapahtuu?

- Suosittelen piirtämään käyttämäistänne yhteyksistä ”kartan”, jossa nähdään kaikki yhteydet eri suuntiin ja niiden vaikutukset/merkitykset. Tällä tavoin kyberturvallisuutta voi lähteä kehittämään parhaiten, kun tiedetään sen kokonaisrakenne.

- Samalla opitte järjestelmien sidonnaisuudet ja toisaalta oman toiminnan herkät kohdat.

- Saadun tiedon pohjalta voidaan myös varautua siihen, minkälaisia kriittisiä varaosia pitää olla omassa varastossa, jos jotain tapahtuu.

- Asiaa voidaan laajentaa myös yhteisten toimijoiden kanssa keskusteluksi, mihin laitoksella on varauduttava, jos jollain toimittajalla tapahtuu kyberhyökkäys.

Kyberturvallisuus pienillä laitoksilla

Linkkejä uutisiin

- Pohjolan Voima ja Kemijoki Oy kyberuhkista: kaikkeen pyritään varautumaan, odottamattomaankin
  - https://yle.fi/uutiset/3-12643785
- Asiantuntija penää yritysten johdon vastuuta tietoturvasta: "Nyt pitäisi herätä" (Vastaamon tapaus)
  - https://yle.fi/uutiset/3-11610288
- Useat suomalaiset ovat haksahtaneet Omakanta-huijaukseen – Kelan mukaan huijausmainoksia saatu poistettua netistä
  - https://yle.fi/uutiset/3-12138550
- Vuosi sitten Lahdessa tapahtui jotain merkillistä ja koko kaupunki pysähtyi – näin taisteltiin miljoonavahingot aiheuttanutta tuntematonta hyökkääjää vastaan
  - https://www.mtvuutiset.fi/artikkeli/vuosi-sitten-lahdessa-tapahtui-jotain-merkillista-ja-koko-kaupunki-pysahtyi-nain-taisteltiin-miljoonavahingot-aiheuttanutta-tuntematonta-hyokkaajaa-vastaan/7839558

Ympäristövastuuta yhdessä

Katja Kotalampi, Jätevesiasiantuntija,
Patamäenkatu 24, 33101 Tampere, puh. 050 4722 656

KVVY-Tampere
Patamäenkatu 24
PL 265
33101 Tampere
puh. 03 2461 111

KVVY-Botnialab
Opistonkatu 7
65100 Vaasa
Puh. 06 312 0020

KVVY-Jyväskylä
Appiukontie 14
40530 Jyväskylä
puh. 03 246 1267

KVVY-Porilab
Tiedepuisto 4
A-rakennus, 3. kerros
28600 Pori
puh. 03 2461 277

KVVY-Raumalab
Lensunkatu 9
26100 Rauma
puh. 03 2461 276

KVVY-Tavastlab
Visamäentie 33
Visatalo
13100 Hämeenlinna
puh. 03 2461 233

KVVY-Sastalab
Tampereentie 7 A,
38200 Sastamala
puh. 03 2461 275

Asiakaspalvelun ollessa suljettuna, päivystys puh. 03 246 1299.