Kyberturvan kehitys Kaupunkiliikenne Oy:ssä

Rata 2023

Heikki Viika, Salar Mohammad

17.1.2023

KAUPUNKILIIKENNE
STADSTRAFIK

Pääkaupunkiseudun Kaupunkiliikenne Oy

Miljoonien matkojen mahdollistaja

- Hallinnoimme Helsingin joukkoliikenneinfraa ja omistamme raitiovaunukaluston.
- Vastaamme joukkoliikenteen kokonaisuuden kehittämisestä ja kunnossapidosta.
- Liikennöimme raitiovaunua ja tuotamme metron liikennöintiä palveluna.
- Järjestämme lisäksi Suomenlinnan lautan liikenteen sekä Helsingin kaupunkipyöräpalvelun.

- **152 milj. joukkoliikennematkaa / vuosi**
- **48,3 km raitiotietä**
- **42 km kaksisuuntaista metrorataa**
- **1207 työntekijää**
- **238 pyöräasemaa**
- **3450 kaupunkipyörää**

HKL:n toiminta siirtyi Pääkaupunkiseudun Kaupunkiliikenne Oy:hyn 1.2.2022.

KAUPUNKILIIKENNE
STADSTRAFIK

Kyberturvan kehitys Kaupunkiliikenne Oy:ssä

- HKL päätti vuonna 2020 kyberturvavalmiuksiensa kehittämisestä.
- Taustatekijöinä oli Traficom kesällä 2020 julkaisema suositus kyberturvallisuuden edistämisestä raideliikenteessä.
- Rinnakkaisesti HKL oli aloittanut metron kapasiteettihankkeen liikenteenohjauksen jatkokehittämiseksi
  - Hanke oli käynnistänyt vuosina 2017 ja 2019 käyttöönotettujen uusien asetinlaite- ja liikenteenohjausjärjestelmien kyberturvan arvioinnin
  - Arvio valmistui marraskuussa 2020.

- Traficomin suositusten ja liikenteenohjausjärjestelmän kyberturvan arvioinnin seurauksena käynnistettiin yrityksenlaajuinen kyberturvan kehittämishanke
- Tavoitteina oli
  - käydä läpi yhtiön toimintaprosessit
  - arvioida tarpeet niiden kehittämiseksi yhteensopiviksi vaatimusten kanssa
  - toteuttaa tarvittavat toimintojen parantamiset

KAUPUNKILIIKENNE
STADSTRAFIK

Kyberturvallisuusarvioinnin suosittelema kehittämispolku

1. **vaiheessa** nykyisen tietoturvan arviointi ja parantaminen niin sisäisesti kuin sidosryhmäkumppanien kanssa
   - Kolme tärkeintä prioriteettia riskienhallinta, turvallisuusmäärittely ja toimittajien ohjaus.
   - Laiteympäristössä nähdään tarvittavaksi toimenpiteiksi tietoliikenteen seuranta, laitteiden konfiguraatioiden tietoturva, sekä pääsyjen- ja yhteyksien verifioinnit.
2. **vaiheessa** kehitetään tietoturvanäkyvyyttä ja lisätään tietoturvaa.
   - Metron liikenteenohjausjärjestelmään pitäisi hankkia uhkanäkyvyyden parantamiseksi uutta tietoturvatekniikkaa ja lisätä henkilöstön koulutusta.
   - Hallinnollisina toimenpiteinä vuosille 2021-2023 suositellaan pääsy-, koulutus-, monitorointi-, ja toimintasuunnitelmien sekä niihin liittyvien prosessien luomista.
3. **vaiheessa** suositellaan hankittavaksi Information Security Management System (ISMS) -järjestelmä osaksi metron liikenteenohjausjärjestelmää.
   - Kokonaisvaltaisella tietoturvanhallintajärjestelmällä saadaan tukea mm. muutos-, henkilöturvallisuus- ja tietoturvan testaus prosesseihin.
   - Tässä yhteydessä pienimuotoisen Security Operation Center (SOC) luominen voisi olla luontevaa.

KAUPUNKILIIKENNE
STADSTRAFIK

Kyberturvan kehityshanke

- Hanke tunnisti kyberturvavaatimukset ja määritteli yhtiön kyberturvallisuusperiaatteet ja –tavoitteet.
- Kyberturvan kohteiksi tunnistettiin osa-alueina henkilöstöturvallisuus, tietojärjestelmien ja teknisen ympäristön turvallisuus, fyysinen tilaturvallisuus, sekä tietoturva ml. tiedon tietoturvatason mukainen luokittelu.
- Näiden pohjalta päätettiin, mitä toimenpiteitä tarvitaan tavoitteiden saavuttamiseksi.
- Hankkeessa kehitettiin tietoturvallisuustason parantamiseksi ensisijaisesti olemassa olevia prosesseja.
  - Valittujen osa-alueiden turvallisuuteen on määritelty toimintamallit perustuen tehtyihin riskiarvioihin.
  - Lisäksi jouduttiin kehittämään myös joitain uusia prosesseja, ja mm. määrittelemään kyberturvaan liittyvät vastuut ja vastuutahot.
  - Prosessit on integroitu osaksi Kaupunkiliikenteen TLY-järjestelmää (Turvallisuus, Laatu, Ympäristö).
- Lisäksi on käynnistetty liikenteenohjausjärjestelmän kyberturvan tekninen kehittäminen.

KAUPUNKILIIKENNE
STADSTRAFIK

Kaupunkiliikenteen tietoturvavaatimukset

Yhtiötä koskevia tietoturvavaatimuksia tulee kansallisista laeista ja standardeista.

- Tärkeimpiä tietoturvallista toimintaa ohjaavia normeja ovat:
  - ISO 27001-standardi
  - Vahti-ohjeisto
  - Katakri 2020-auditointikriteeristö
- Tietoturvan teknisiä vaatimuksia ohjaavia normeja ovat:
  - IEC 62443-standardi
  - EN 50701-standardi
  - Traficomin suositukset kryptografisista standardeista ja salasanoista

- Tärkeimpiä vaatimuksia antavia lakeja ja sidosryhmiä ovat:
  - Raideliikennelaki
  - Traficom
  - Helsingin kaupunki
  - Fintraffic Raide Oy

KAUPUNKILIIKENNE
STADSTRAFIK

Kaupunkiliikenne Oy:n kyberturvallisuusperiaatteet

- TLY-järjestelmän yleiset turvallisuustavoitteet ohjaavat tietoturvatavoitteiden asettamista. Näissä korostuvat erityisesti metro- ja raitioliikenteen turvallisuus.
- Tietoturvallisuutta kehitetään ja ohjataan suunnitelmallisesti ja riskilähtöisesti.
- Henkilöstöllä on velvollisuus noudattaa annettuja tietoturvaohjeita sekä raportoida havaitsemistaan tietoturvaheikkouksista.
- Organisaatiossa noudatetaan tietojen luokitteluperiaatetta ja toteutetaan sen mukaisia vaatimuksia ja toimenpiteitä tiedon käsittelyssä koko tiedon elinkaaren ajan.
- Toimintaan kohdistuvat tietoturvavaatimukset sisällytetään soveltuvin osin kaikkiin sopimuksiin. Toimittajien palveluiden tulee täyttää sopimuksissa määritellyt tietoturvavaatimukset ja toimittajien henkilöstön tulee noudattaa Kaupunkiliikenne Oy:n tietoturvaohjeita tuottaessaan palveluja.
- Organisaatiossa tapahtuvat ja organisaatioon kohdistuvat tietoturvaloukkaukset ilmoitetaan valvontaviranomaisille ja annetaan tarvittaessa poliisin tutkittaviksi.

KAUPUNKILIIKENNE
STADSTRAFIK

Teknisen kyberturvan kehittäminen operatiivisiin järjestelmiin

- Syksyllä 2020 tehdyn Helsingin Metron liikenteenohjausjärjestelmän kyberturvallisuusarvioinnin pohjalta Kaupunkiliikenteessä päätettiin, että Metron kapasiteettihanke toimii pilottina operatiivisten järjestelmien kyberturvan kehittämisessä.
- Kehityshankkeessa laadittiin tekniset vaatimukset sekä tietotekniikan että operatiivisen teknologian vaatimuksiksi IEC 62443- ja EN 50701-standardien mukaisesti.
- Lisäksi huomioitiin Traficomin kansallisen kyberturvakeskuksen suositukset mm. kryptografisista standardeista ja salasanoista.
- Ohjeistus sisältää sekä sisäiseen käyttöön tarkoitetun ohjeistuksen, että mahdollisille toimittajille suunnatun vaatimusluettelon.
- Vaatimusluettelossa on huomioitu teknisten vaatimusten lisäksi myös osaamisvaatimukset ja järjestelmän elinkaaren hallintaan liittyviä näkökohtia.

KAUPUNKILIIKENNE
STADSTRAFIK

Teknisen kyberturvan pilottiasennus metron liikenteenohjaus-järjestelmään

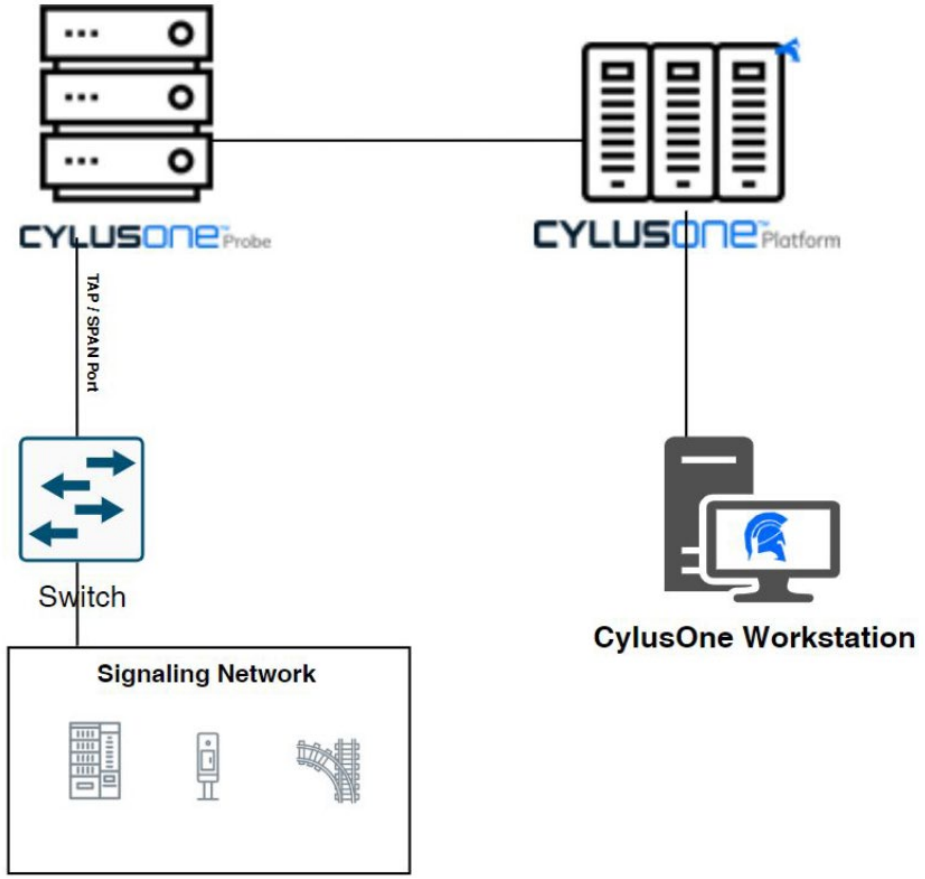
KAUPUNKILIIKENNE
STADSTRAFIK

Taustaa

- Liikenteenohjausjärjestelmän tietoliikenneverkon kyberturvan varmistaminen tunnistettiin kriittiseksi tekijäksi
  - Asetinlaitteet käsittelevät junaturvallisuuden varmistavia komentoja
  - Niiden kyberturva usein nojautuu ns. suljettuihin verkkoihin.
  - Nykyään kuitenkin on harvinaista, että tietoverkko olisi todellisuudessa täysin suljettu.
- Näin ollen järjestelmän kyberturvakyvykkyyden kohottamiseen päätettiin ryhtyä.
- Pilottijärjestelmän tavoitteena on tuottaa selkeä kuva liikenteenohjausjärjestelmän laitteista ja tietoverkoista, niiden liikennöintimääristä, ja mahdollisista haavoittuvuuksista.
- Tämän tiedon pohjalta on mahdollista varmistaa, että järjestelmän avoimet haavoittuvuudet pystytään korjaamaan.

KAUPUNKILIIKENNE
STADSTRAFIK

Cylus One IDS asennus liikenteenohjaukseen



KAUPUNKILIIKENNE
STADSTRAFIK

IDS pilotin opit

- Nykyiset OT-järjestelmät I/O → IoT / IP
- Ohjausjärjestelmät ovat usein kehitetty oletuksella, että niitä käytetään suljetuissa verkoissa. Näin ollen kyberturvapiirteisiin ei ole välttämättä kiinnitetty riittävää huomioita
- OT-järjestelmien OS-päivitys haasteet
- Standardin puute
- Protokollien päivittäminen uusiin versioihin aiheuttaa laaja päivitystä ja konfiguraatiota

Tunnistettuja ongelmia

- Järjestelmässä tuotteita ja komponentteja, joissa on tunnistettuja haavoittuvuuksia
- Arkaluontoista tietoa lähetetään ”suljetun jakeluverkon” sisällä kryptaamattomana
- Ohjausjärjestelmän palautuminen ja uudelleen muodostaminen epäonnistuu
- Konfiguraatioheikkouksia

Jatkotoimenpiteet

Kaupunkiliikenne on hankkeen aikana kehittänyt uutta ohjeistoa, jonka perehdyttäminen henkilöstölle on käynnissä.

Kehitystoimenpiteet ovat tuoneet uutta osaamista, ja näiden oppien soveltaminen nykyisiä ratkaisuja tarkasteltaessa ja uusia ratkaisuja luotaessa mahdollistavat jatkuvan kyberturvan kehityksen.

KAUPUNKILIIKENNE
STADSTRAFIK

Jatkotoimenpiteet 2

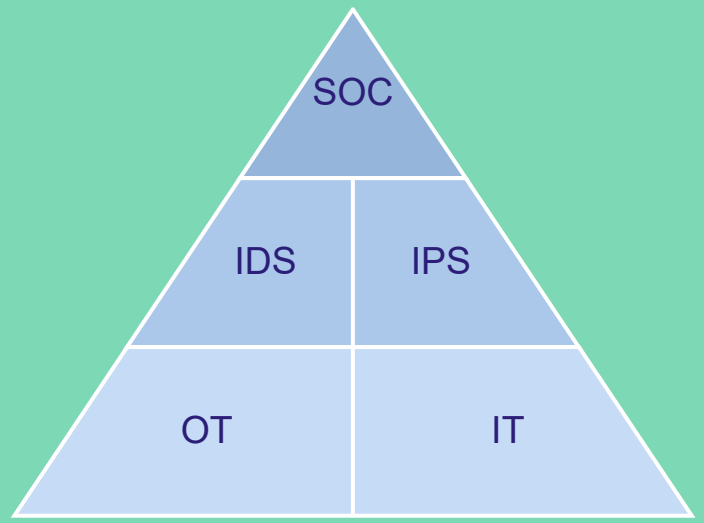
OT-järjestelmät

Passiivinen valvonta
(IDS ratkaisu)

IT-järjestelmät

Aktiivinen valvonta
(IPS ratkaisu)

Security Operation Center
(SOC)



KAUPUNKILIIKENNE
STADSTRAFIK

Kiitos!

Heikki Viika
Hankejohtaja
SKAR
heikki.viika@kaupunkiliikenne.fi
+358 40 664 0879

Salar Mohammad
Projektijohtaja
SKAR
salar.mohammad@kaupunkiliikenne.fi
+358 40 XXX XXXX

KAUPUNKILIIKENNE
STADSTRAFIK