RAIDELIIKENTEEN KYBERTURVALLISUUS

Työvälineet kyberturvallisuuden perustason saavuttamiselle

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulun opinnäytetyö

Liikenneala, insinööri (AMK)

Kevät 2022

Mikko Aarnio

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Liikennealan koulutus — Tiivistelmä
Tekijä Mikko Aarnio — Vuosi 2022

Työn nimi Raideliikenteen kyberturvallisuus – Työvälineet kyberturvallisuuden perustason saavuttamiselle

Ohjaajat Teppo Sotavalta (HAMK), Ville Lahti (Traficom)

Raideliikenteen toimiala on digitalisoitumassa. Suomessa nykyisen junien kulunvalvontajärjestelmän käyttöiän on arvioitu päättyvän 2020-luvun aikana. Digirata-hankkeen selvitystyön pohjalta on ehdotettu, että Suomessa otettaisiin käyttöön moderni radioverkkopohjainen junien kulunvalvontajärjestelmä. Moderni järjestelmä tulisi perustumaan 5G-teknologiaan ja IP-protokollaan, jolloin kyberturvallisuuden vaatimukset tulevat korostumaan entisestään. Modernin kulunvalvontajärjestelmän ja uuden teknologian tuomien mahdollisuuksien lisääntyessä myös kyberturvallisuusuhkien määrä kasvaa.

Kansallisella lainsäädännöllä sekä EU-tason direktiiveillä ja asetuksilla ohjataan kyberturvallisuuteen liittyvää toimintaa esimerkiksi suositusten ja vaatimusten myötä. Suomessa Liikenne ja viestintävirasto Traficom koordinoi kyberturvallisuuteen liittyvää työtä ja toimii myös ohjeistavana ja tukea antavana tahona. Opinnäytetyö pohjautuu Traficomin toimeksiantoon selvittää kyberturvallisuuden hallinnoinnin ja kypsyystason arvioinnin työvälineiden käyttöä Suomessa toimivien uusien raideliikenteen operaattoreiden organisaatioissa.

Opinnäytetyöhön tutkimukseen valittuja kyberturvallisuuden työvälineitä ovat Euroopan komission teettämä kyberturvallisuuden välineistö, Traficomin julkaisema suositus kyberturvallisuuden edistämisestä raideliikenteessä sekä Kyberturvallisuuskeskuksen toteuttama Kybermittari. Raideliikenteen operaattoreiden edustajia haastateltiin heidän organisaatioidensa valmiudesta vastata kyberturvallisuuden haasteisiin sekä valittujen työkalujen hyödyntämisestä kyberturvallisuuden hallinnoinnissa sekä toiminnan kehittämisessä.

Tutkimuksessa selvisi, että organisaatioissa on osittain huomioitu opinnäytetyön piiriin valittujen kyberturvallisuuden työvälineiden käyttö ja niitä on hyödynnetty omaan toimintaan. Kaikki työvälineet eivät kuitenkaan olleet sellaisinaan tuttuja, mutta niiden asiasisällöt olivat kuitenkin jo huomioituja organisaation toiminnassa muussa yhteydessä. Kansallisten kyberturvallisuuden viranomaisten rooli nähtiin tärkeänä ja koordinointityö arvokkaana. Kyberturvallisuuden haasteisiin vastaamiseen organisaatiot tarvitsevat jatkossakin tukea.

Avainsanat Kyberturvallisuus, raideliikenne, operaattori, hallinnointi, työväline
Sivut 65 sivua ja liitteitä 4 sivua

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Name of Degree Programme Abstract
Author Mikko Aarnio Year 2022
Subject Cybersecurity in rail transport – Tools for achieving a basic level of cybersecurity
Supervisors Teppo Sotavalta (HAMK), Ville Lahti (Traficom)

The railway industry is transforming more and more digitalized. In Finland the current train control system must be replaced during the 2020s. Based on the study of the Digirata-program the new train control system would be modern radio-based system. The modern system will be based on 5G technology and the IP protocol which probably will increase amount of requirements for cybersecurity management.

Transport and Communications Agency Traficom mission is to coordinate cybersecurity work nationwide. Agency also provides support and guidance about cybersecurity issues to organisations. This thesis is based on Traficom's assignment. The purpose of the work is to study management and knowledge level of the cybersecurity in the organizations of new rail transport operators in Finland. In addition, the usage of the selected cybersecurity management tools have been explored as well.

The selected cybersecurity tools are provided by European Comission, Traficom and National Cyber Security Centre of Finland. The tools are Cybersecurity toolkit, Recommendation on promoting cybersecurity in rail transport and Cybermeter. Representatives of rail transport operators were interviewed about the readiness of their organizations to meet the challenges of cyber security and about the level of use of selected cybersecurity tools.

The study found that organizations have considered almost all selected cybersecurity tools in their operations. However, not all tools were familiar as such, but their substance was already taken into account in the organization's management activities in other contexts. The role of national authorities is seen as important in cybersecurity matters. Organizations will gladly continue the cooperation with the national cybersecurity authorities.

Keywords Cybersecurity, rail transport operator, management, tool
Pages 65 pages and appendices 4 pages

Sisällys

Liitteet

1 Johdanto

Raideliikenteen toimiala on digitalisoitumassa. Suomessa raideliikenteen liikenteenhallinnassa ollaan siirtymässä radioverkkopohjaisiin ratkaisuihin, joka tarkoittaa samalla järjestelmän digitalisoitumista. Raideliikenteen operaattorin kyydissä matkustavalle henkilölle tärkeää on saada hankittua matkalippu toimivalla järjestelmällä sekä saada matkan ajaksi käyttöön luotettava internet-yhteys. Matkanteon reaaliaikaisen etenemisen seuranta on tarpeen erityisesti silloin, kun toteutettava matkaketju jatkuu vielä junamatkan jälkeen. Raideliikenteeseen liittyvien järjestelmien kirjo on kuitenkin paljon laajempi matkustajalle suunnattujen järjestelmien lisäksi. Useimmat raideliikenteen järjestelmistä liittyvät komento-, viesti- tai valvontajärjestelmiin tai raiteilla kulkevan yksikön kulunvalvonnan järjestelmiin. Taustalla toimii myös suuri määrä hallinnoimisen kokonaisuutta ja toimintaa avustavia järjestelmiä. Käytettävät järjestelmät voivat liittyä kalustoon tai ne ovat raide- tai radanvarsijärjestelmiä. Lisäksi käyttötoimintaan, hallintaan ja ylläpitoon ovat omat järjestelmänsä käytössä (Pylvänäinen ym., 2020, s. 57).

Digitaalisen murroksen yhteydessä kyberturvallisuuteen tulee kiinnittää entistä enemmän huomiota, sillä rikollisten toiminta muuntautuu samanaikaisesti yhä digitaalisemmaksi. Kun laitteita ja järjestelmiä kytketään enemmän verkkoon, samalla myös potentiaalisten haavoittuvuuksien määrä kasvaa. Digitaalisessa ympäröistössä tahallinen tai tahatonkin häirintä ei ole enää sidoksissa fyysiseen sijaintiin. Rikosten tai häiriöitä aiheuttavien tekijöiden täytyi ennen päästä fyysisesti paikanpäälle kohteeseen, mutta maailmanlaajuisen tietoliikenneverkon avulla toteuttajat voivat sijaita fyysisesti esimerkiksi toisella puolella maapalloa. Organisaation kasvaessa ja sen toiminnan laajetessa on sen kybertietoisuuden kasvettava samassa suhteessa. Tällöin kyvykkyys uhkien kehittymisen seurantaan pysyy teknologian kehittymisen mukana. Uhkien kehittymiseen ja muuttumiseen voi varautua parantamalla omaa ennakointikykyään sekä kehittämällä valvonnan prosesseja, panostamalla kyberturvallisuuden osa-alueen toimintoihin ja hankkimalla käyttöön tuotteita tai palveluita, jotka tukevat suojautumista.

Organisaation toimintaa säätelevät lait, asetukset sekä suositukset. Organisaatio on itse vastuussa oman kyberturvallisuutensa huolehtimisesta. Rikosten tekijät todennäköisemmin

onnistuvat kyberhyökkäyksissään, mikäli järjestemiä ei ole suojattu asianmukaisesti. Mikäli suojaukset ovat ajantasalla sekä niiden valvonta on aktiivisena, voi murtautuminen silti onnistua. Tämän vuoksi organisaatiolla tulee olla laadittuna esimerkiksi toiminnan palautumissuunnitelma sekä suunnitelma viestinnästä kyberhyökkäyksen uhriksi joutumisen jälkeen, jotta esimerkiksi voidaan minimoida mahdollinen imagotappio.

Kyberhyökkäystä ei välttämättä koeta konkreettiseksi uhkaksi, mikäli sellaisen kohteeksi ei ole aiemmin joutunut. Tällöin organisaation voi olla hankala tunnistaa todellisia uhkia ja riskejä. Organisaatiolla voi olla myös haasteita pysyä ajantasalla jatkuvasti muuttuvassa kyberturvallisuuden riski- ja uhkakentässä. Kyberhyökkäyksiä ei mahdollisesti pystytä täysin estämään, mutta niiden havainnoinnin sekä kyberhyökkäksestä palautumisen kehittämisen avulla on mahdollista saavuttaa valmiudet toiminnan nopeaan normalisoitumiseen, mikäli jokin kyberturvallisuuden uhka toteutuu.

Kyberturvallisuudesta huolehtimisen vaatimukset on hyvä yhtenäistää liiketoiminnan prosesseihin tai organisaation toimintaan ylipäätään Esimerkiksi toiminnanohjausjärjestelmät, rahaliikenteen ja kirjanpidon järjestelmät, projektityöt ja niiden tuotokset niin työpaikoilla kuin opiskelujen yhteydessä ovat riippuaisia digitaalisista järjestelmistä. Organisaatiolle on osoitettu tietosuoja-asetuksen myötä vaatimuksia toiminnan ja tietojen turvaamiseksi sanktioiden uhalla. Mikäli uhkia kuitenkin pääsee syntymään, niin organisaatiolla tulee olla ennalta suunniteltu ja päätetty toimintatapa tilanteesta selviämiselle. (Puro, 2017)

Kansallisella lainsäädännöllä sekä EU-tason direktiiveillä ja asetuksilla sekä säännöillä ohjataan kyberturvallisuuteen liittyvää toimintaa. Raideliikenteeseen liittyvien standardien kautta on mahdollista kehittää toimintaa yhteensopivaksi useiden toimijoiden kanssa. Suomessa ohjeistusta ja parhaiden käytäntöjen tietoa antaa Liikenne ja viestintävirasto Traficom ja EU-tasolla vastaavana raideliikenteen toimijoita yhdistävänä tahona toimivat ENISA eli Euroopan unionin kyberturvallisuusvirasto sekä ERA eli Euroopan rautatievirasto. Laajan yhteistyöverkon seasta asiakokonaisuuden hallintaa parhaiten tukevan tahon löytäminen ja yhteyden saaminen voi olla haasteellista etenkin pienemmille organisaatioille, joilla ei ole mahdollista kohdistaa tarpeeksi resursseja kyberturvallisuuden hallintaan ja

muuhun selvittelyyn. Onneksi kuitenkin työvälineitä kyberturvallisuuden hallintaan on olemassa sekä saatavilla ja niiden avulla pienemmälläkin resurssilla toimivalla organisaatiolla on mahdollisuus oman toimintansa kehittämiseen.

1.1 Tavoite ja tarkoitus

Tämän opinnäytetyön tavoitteena on tuottaa raideliikenteen operaattoreiden organisaatioissa kyberturvallisuuteen varautumiselle ja sen hallinnoinnille parhaat toimintatavat, jotka voidaan yhteensovittaa päivittäiseen liiketoimintaan sekä säännölliseen kehitystyöhön. Opinnäytetyön tarkoituksena on selvittää raideliikenteen operaattoreiden tämänhetkinen tietämys tarjolla olevista kyberturvallisuuden työvälineistä sekä niiden mahdollisesta hyödyntämisestä organisaation toiminnassa, kyberturvallisuuden kypsyystason arvioinnissa sekä kehityskohteiden tunnistamisessa.

Opinnäytetyössä selvitetään, miten raideliikenteen operaattorit huomioivat päivittäisessä toiminnassaan kyberturvallisuuteen liittyvät asiat sekä mitä kyberturvallisuuden työvälineitä he tuntevat ja käyttävät jo tällä hetkellä toiminnan tukemiseksi. Operaattoreiden edustajien kanssa käydyissä henkilöhaastatteluissa pyrittiin selvittämään organisaation kyberturvallisuuden hallinnoinnin nykytilaa ja mahdollisia ilmenneitä poikkeustilanteita. Lisäksi haastattelussa käytiin läpi organisaation kyberturvallisuusasioista vastaavien henkilöiden rooleja sekä työnjakoa ja miten organisaatiossa yleensä huolehditaan sekä turvataan kyberturvallisuuden tietämyksen ja osaamisen jakaminen sekä ylläpito myös muun henkilöstön osalta.

1.2 Tutkimus ja työn toteuttaminen

Liikenne- ja viestintävirasto Traficomin kyberturvallisuuden erityisasiantuntija oli yhteydessä Hämeen ammattikorkeakoulun liikennealan opinto-ohjaajaan kartoittaakseen opiskelijayhteistyön mahdollisuutta. Opinnäytetyön tekeminen käynnistyi keväällä 2021 Euroopan Euroopan unionin verkko- ja tietoturvavirasto ENISA:n sekä Euroopan rautatievirasto ERA:n järjestämän virtuaalisen Cybersecurity in Railways -konferensin myötä.

Konferensin sisältö oli monipuolinen ja sen aikana tilannekuvaa rautatiealan kyberturvallisuuden hallinnoimisen käytännöistä ja kehittämistarpeista.

Kevään 2021 konferensin jälkeen alkoi työhön liittyvän lähdeaineiston kerääminen. Aihealueeseen tarkempi tutustuminen jatkui kesän ajan. Opinnäytetyön varsinainen työstäminen lähti käyntiin syksyllä 2021. Henkilöhaastattelut rautatieliikenteen operaattoreiden edustajien kanssa käytiin marraskuussa 2021 ja vuoden 2022 puolella tammikuussa. Työn aineistojen käsittely, kokoaminen ja opinnäytetyön dokumentin viimeistely sekä loppuseminaari suoritettiin kevätlukukauden 2022 aikana.

Tämän opinnäytetyön toimeksiantajana oli Liikenne ja viestintävirasto Traficom, jonka edustajana toimi kyberturvallisuuden erityisasiantuntija Ville Lahti. HAMKin puolelta työtä ohjasi lehtori Teppo Sotavalta.

2 Raideliikenne Suomessa

2.1 Rautatiesektorin toimijat

Rautatiesektorilla on useita toimijoita, joiden kesken on jaettu toimialan tehtäviä ja vastuita. Suomen liikenne- ja viestintäverkkojen ja väylien sekä verkkomarkkinoiden toiminnasta vastaa Liikenne- ja viestintäministeriö. Ministeriön vastuulla on kaksi laajaa sektoria, jotka ovat liikennepolitiikka ja viestintäpolitiikka. Ministeriö vastaa toimialansa EU-asioista ja liikennesektorin osalta esimerkiksi liikennejärjestelmistä, liikenneverkoista, tavara- ja henkilöliikenteestä ja liikenneturvallisuudesta. (Palkeet, 16.2.2022) EU-sääntelyyn pohjautuen Suomessa rautatiejärjestelmän kansallisena turvallisuusviranomaisena toimii Liikenne- ja viestintävirasto Traficom. Traficomin tehtäviä ovat rautatieliikenteen harjoittajien turvallisuustodistusten ja rataverkon haltijoiden turvallisuuslupien hyväksymiset, lupaviranomaisena toimiminen rataverkon ja kaluston käyttöönottojen yhteydessä sekä hyväksyy esimerkiksi rautatieyrityksien toimiluvat ja myöntää veturinkuljettajien lupakirjat. Traficom osallistuu rautatiejärjestelmän ja sitä koskevan sääntelyn kehittämiseen niin kansallisella kuin EU-tasollakin sekä toimii myös järjestelmän valvovana osapuolena. Traficomin tehtävät ulottuvat myös kaupunkiraideliikenteen puolelle. (Traficom, 2019)

Väyläviraston tehtävinä ovat tie-, rata- ja meriliikenteen väyläverkon suunnittelu, kehitys ja ylläpito sekä maankäytön ja liikenteen sovittamisen koordinointi. Lisäksi Väyläviraston vastuulla on liikenteenohjauksen sekä talvimerenkulun järjestäminen. (Palkeet, 11.2.2022) Väyläviraston vastaa Suomen valtion rataverkosta ja sillä toimimisesta, joten myös osallistuu liikennejärjestelmän kehittämiseen. Väylävirasto toimii myös valtion rataverkon haltijana, joka tekee yhteistyötä muiden rataverkolla liikennöivien rautatieliikenteen harjoittajien sekä valtion rataverkkoon kytkeytyvien yksityisraiteiden haltijoiden kanssa. Väylävirasto vastaa rataverkon haltijan roolissaan rataverkon käytöstä, kunnosta, kehittämisestä sekä sen kapasiteetin jakamisesta toimijoiden kesken. (Traficom, 2019)

Fintraffic-konserni ohjaa liikennettä maalla, merellä ja ilmassa. Tie- ja meriliikenteen sekä lennonvarmistuksen hallinta ovat konsernin kolmen muun tytäryhtiön vastuulla ja

rautatieliikenteen ohjauksesta ja hallinnasta vastaa Fintraffic Raide Oy. (Fintraffic, n.d.) Lisäksi Fintraffic Raide Oy:n tehtävänä on varmistaa matkustajien ja tavaraliikenteen turvallinen pääsy määränpäähänsä. Yrityksen palveluiden perustana ovat rautateiden liikenteenohjaus, liikennesuunnittelu ratatöiden aikaisen liikenteen yhteensovittaminen, kapasiteetin hallinta, käyttökeskustoiminta sekä junamatkustukseen liittyvät asemien ja laitureiden matkustainformaation palvelut. Fintrafic Raide Oy:n vastuulla ovat turvavalvomo sekä tekninen valvomo. Yritys tarjoaa muun toimintansa ohella myös asiantuntija- ja koulutuspalveluita. (Fintraffic Raide, n.d.)

Traficomin yhteydessä toimii rautatiealan sääntelyelin, jonka tehtävänä on seurata, valvoa ja edistää rautatiemarkkinoiden toimivuutta sekä tasapuolisuutta ja syrjimättömyyttä. Sääntelyelin tekee päätöksensä itsenäisesti ja sen päätökset sitovat kaikkia asianosaisia. Jokaiseen EU:n jäsenvaltioon on perustettu rautatiealan sääntelyelin, jonka tehtäviin kuuluu huolehtia alan toimijoiden kohtelusta tasapuolisesti ja syrjimättömästi. Eurooppalaisten itsenäisten rautatiealan sääntelyelinten ryhmä IRG-Rail perustettiin vuonna 2011. Ryhmä pyrkii vaikuttamaan aktiivisesti EU:n päätöksentekoon ja se toimii kansallisten rautatiealan sääntelyelinten yhteistyöfoorumina tiedon, kokemuksien sekä parhaiden käytäntöjen jakamiselle. (Rautatiealan Sääntelyelin, 2020)

Ranskassa toimiva Euroopan rautatievirasto ERA eli European Union Agency for Railways on EU:n erillisvirasto, joka edistää Euroopan rautatiejärjestelmien yhteentoimivuutta ja turvallisuutta. ERA on mukana EU-sääntelyn valmistelussa sekä rautatiejärjestelmän toiminnan kehittämisessä. Vuoden 2019 ERA:n toimivaltaa kasvatettiin ja se on toiminut siitä lähtien myös kansallisten viranomaisten rinnalla vaihtoehtoisena lupaviranomaisena, jonka vastuualueella ovat rautatieliikenteen harjoittajien turvallisuustodistusten ja kalustoyksikköjen sekä -tyyppien markkinoillesaattamisluvat. (Traficom, 2019)

Vuonna 2004 perustettu EU:n kyberturvallisuusvirasto ENISA eli European Union Agency for Cybersecurityn toiminnan visiona on edistää yhteistyössä luotettavaa ja kyberturvallista Eurooppaa. ENISA tekee yhteistyötä jäsenvaltioiden sekä EU:n toimielinten kanssa ja on täten myös ERA:n kanssa tiiviissä yhteistyössä rautatie- ja kyberturvallisuusden sääntelyiden toteutumisen varmistamiseksi. (Traficom, 2019) ERA toteutti yhdessä ENISA:n kanssa

rautateiden kyberturvallisuutta käsittelevän webinaarin keväällä 2021, jossa käsiteltiin kyberturvallisuustilanteen kehittymistä sekä siihen liittyviä huolenaiheita rautateiden sidosryhmien keskuudessa. (ERA, n.d.)

Suomessa on vuoden 2018 lopussa liikennöidyn rataverkon pituus ollut Väyläviraston raportoinnin mukaan 5926 kilometriä, josta sähköistetyn radan osuus on ollut hieman yli puolet eli 3330 kilometriä. Kaksi- tai useampiraiteista osuutta on tällöin ollut 692 kilometriä. Raideyhteydet Suomen puolelta on Ruotsiin Tornion kautta sekä itärajan yli Vainikkalasta, Imatrankoskelta, Niiralasta sekä Vartiuksesta. (Väylävirasto, 2021) Suomen rautateillä toimivia rautatieliikenteenharjoittajia on kymmeniä, joista koko valtion rataverkolla toimivia rautatieyrityksiä on kolme. Nämä yritykset ovat Fenniarail Oy, Operail Finland sekä VR-Yhtymä Oy. Rautateiden tavarakuljetuksien osalta toimiluvat on myönnetty Imatran alueella paikallisesti toimivalle Ratarahti Oy:lle sekä valtion ratapihoilla vaihtotyöliikennettä harjoittavalle Aurora Rail Oy:lle. (Rautatiealan Sääntelyelin, 2020) Traficomin kesän 2018 tilastojen mukaan rautatieliikenteen harjoittajia olivat rautatieyrityksien lisäksi museoliikenteen harjoittajat, radan kunnossapitoa harjoittavat yritykset sekä vaihtotyötoimijat. (Traficom, 2021)

2.1.1 Rautatieliikenteen operaattorit

Vuoden 2007 alussa Suomen kansallinen rautateiden tavaraliikenne avattiin kilpailulle. Suomen ja Venäjän yhdysliikenne avautui puolestaan vuoden 2016 lopulla. Rataverkolla toimii kolme rautatieyritystä, joita ovat VR-Yhtymä Oy, Fenniarail Oy ja Operail Finland. Toimilupa rautateiden tavarakuljetuksiin on lisäksi myönnetty myös Ratarahti Oy:lle ja Aurora Rail Oy:lle. (Rautatiealan Sääntelyelin, 2020)

Tämän opinnäytetyön ensisijaisena kohderyhmänä ovat Suomessa 2007 kilpailun avauduttua markkinoille tulleet uudet rautatieliikenteen operaattorit, joita ovat Fenniarail Oy, Operail Finland Oy, Aurora Rail Oy ja Ratarahti Oy. Fenniarail Oy on perustettu vuonna 2009 ja se on yksityinen rautateiden tavaraliikenteen operaattori, jonka toiminta-alueena on koko Suomen rataverkko (Fenniarail, n.d.). Operail Finland Oy on tavaraliikenteen harjoittaja, joka aloitti kaupallisen liikenteen vuoden 2020 lopulla. Yritys kuuluu Viron valtion omistamaan Operail

AS -konserniin. (Operail, n.d.) Aurora Rail Oy aloitti itsenäisenä yksikkönä toimimisen vuoden 2017 alussa Venäjän yhdysliikenteen vapauduttua. Yrityksen toimipiste on Kouvolassa ja sillä on toimintaa myös itärajan tuntumassa sijaitsevassa Niiralassa. (Aurorarail, n.d.) Ratarahti Oy on saanut toimiluvan rautateiden tavarakuljetuksiin keväällä 2012. Yrityksellä oli tuolloin tavoitteena aloittaa saman vuoden syksyllä tavaran kuljettaminen vaihtotyönä Imatran liikennepaikalla Kaukopään tehtaan sekä Pelkolan välillä. (LVM, 2012)

2.1.2 Muut toimijat

Suomessa satamat, teollisuusyritykset, kaupungit ja kunnat ovat usein myös yksityisraiteiden haltijoita. Valtion rataverkkoon kuulumattomia yksityisraiteita, joita Väylävirasto ei hallinnoi, on Suomessa noin tuhat kilometriä. Liittymäkohtia yksityisraiteiden sekä valtion rataverkon yhdistämiseksi on yli 500. Suomen rataverkonhaltijoilla on muutaman kerran vuodessa kokoontuva yhteistyöryhmä, jonka kokouksissa ryhmän jäsenet käyvät läpi ajankohtaisia ja kiinnostavia rataverkon omistamiseen ja hallinnointiin liittyviä asioita. (Väylävirasto, n.d. -b) Yksityisraiteiden haltijoita voi olla myös useampia samalla alueella. Liikenne ja viestintäministeriön vuoden 2011 Yksityisraiteet ja ratamaksusääntely -julkaisussa on esimerkin asemaan nostettu Haminan satama-alue, jossa yksityisraiteiden kokonaispituus on kymmeniä kilometrejä ja niistä suurimman osan haltija on Haminan Satama Oy, mutta lukuisilla alueella toimivilla yrityksillä on omat pistoraiteensa. Silloisen Liikenteen turvallisuusviraston ja nykyisen Traficomin selvityksien mukaan toimijoita oli alueella lähes parikymmentä, joihin lukeutuvat esimerkiksi Neste Oil Oyj, Nurminen Logistics Oyj, DHL Freight Finland Oy sekä VR-Yhtymä Oy. (Tervonen, 2011, s. 6)

2.2 Turvallisuusohjelma

Liikenne- ja viestintävirasto Traficom pyrkii raideliikenteen turvallisuusohjelmalla edistämään raideliikenteen kokonaisturvallisuutta. Jokaisen raideliikenteen toimijan tulee vastata huolellisesti toimintansa turvallisuudesta kokonaisuutena kuten sääntelyssä ja toimijan turvallisuuden johtamisjärjestelmässä ja turvallisuuden hallintajärjestelmässä kuvataan. Turvallisuusohjelman eri toimenpiteiden tavoitteena on turvallisuuden parantamisen lisäksi kehityksen jatkuvuuden takaaminen toimijoiden

turvallisuusjohtamisjärjestelmän ja turvallisuuden hallintajärjestelmän sekä viranomaistoiminnan osalta. Traficom huomioi ja huolehtii vastuualueelleen kuuluvan valvonnan lisäksi turvallisuusohjelmaan kytkettyjen toimenpiteiden vaikutuksia. (Traficom, 2021)

Rautatietoimijoiden turvallisuusjohtamisjärjestelmä on rautatieliikenteen toimijalle keskeinen työväline turvallisuuden hallinnoimisessa. Turvallisuusjohtamisjärjestelmää tarvitsevat rautatieliikenteen harjoittajat sekä rataverkon haltijat, jotka voivat järjestelmän myötä hallinnoida riskejä ja kehittää toimintaansa. Turvallisuusjohtamisjärjestelmän sisällön vaatimukset tulevat EU-komission asetuksesta 2018/762. Rautatietoimijoiden on tunnistettava ja hallittava kattavasti kaikkiin toimintoihinsa kuuluvat riskit, jotta ne pystyvät toimimaan turvallisesti. Menestyksekäs turvallisuusjohtamisjärjestelmän käyttö vaatii toimijalta järjestelmällistä lähestymistapaa, jolla turvataan toimintojen ja riskien jatkuva hallinta. Traficom toimii viranomaisena, joka antaa tarvittaessa lisätietoja ja neuvontaa rautatieliikenteen toimijalle turvallisuusjohtamisjärjestelmään liittyen. (Traficom, 2019) Valtiovarainministeriön alaisuudessa toimiva Turvallisuuskomitea ylläpitää kansallista kyberturvallisuusstrategiaa, josta on vuonna 2019 julkaistu tuorein versio. (Turvallisuuskomitea, 2019).

Turvallisuusjohtamisen kehittämisen osalta Traficomin tavoitteena on kehittää riskienhallintaa, edistää turvallisuuskulttuuria, tehostaa valvontatoimenpiteitään ja valvontatulosten hyödyntämistä sekä edistää raideliikenteen toimijoiden välistä yhteistyötä selkeiden vastuujakojen myötä. Toimintavarmuuden kehittämisen saralla Traficomin tavoitteena on edesauttaa raideliikenteen yhteyteen toimintavarmuuteen tähtäävän toimintakulttuurin muodostumista. Lisäksi tavoitteena on turvallisuuden parantaminen vaarallisten aineiden kuljettamisessa, onnettomuus- ja vaaratilannetiedon hyödyntämisen tehostaminen sekä raideliikenteen kyberturvallisuuden kehittäminen kokonaisvaltaisesti. (Traficom, 2021)

Kyberturvallisuuden kehittämisen edellytyksiä Traficom on tunnistanut tarkemmalla tasolla. Kyberturvallisuuden yhteistyöryhmän toiminta pyritään vakiinnuttamaan ja alan toimijoiden yhteistyön kehittämiseksi ja aiheen keskustelujen tukemiseksi järjestettiin esimerkiksi

työpaja raideliikenteen kyberturvallisuudesta kesäkuun alussa vuonna 2021. Traficomin järjestämään tilaisuuteen osallistui kyberturvallisuuden edustajia ja asiantuntijoita Väylävirastolta, Fintraffic Oy:ltä, Digirata-hankkeen osalta sekä Kyberturvallisuuskeskuksen puolelta. (Traficom, 2021) Liikenne- ja viestintäministeriön linjaukset huomioiden raideliikenteen toimintojen kyberturvallisuustyön kehittämistä edistetään muun muassa ohjeistuksien, standardien sekä määräyksien puitteissa. EU-tasolla käytävään raideliikennettä koskevaan kyberturvallisuuden kehittämiseen liittyvään keskusteluun osallistutaan aktiivisesti. Traficomin tavoitteena on myös vaikuttaa siihen, että kyberturvallisuuden koulutusta on saatavilla raideliikenteen toimijoiden tarpeiden mukaisesti. (Traficom, 2021)

Vastaava suljettu ja erittäin säädelty toimiala on esimerkiksi ydinenergia-ala, johon kuuluvat Suomessa muun muassa käytössä olevat kaksi Loviisan sekä kaksi Olkiluodon ydinvoimalaitosta. Ydinenergia-alalla toimivalta edellytetään kattavaa sekä intensiivistä sääntelyä ja valvontaa huomioiden ydinenergian käytön riskit. Näillä toimilla voidaan taata ydinenergian käytön turvallisuus ihmisten ja ympäristön kannalta sekä varmistaa energian tuotannosta syntyvän jätteen käsittely ja loppusijoittamisen asianmukaiset käytännöt. Kansainvälisellä valvonnalla varmistetaan ydinenergian käyttö rauhanomaiseen tarkoitukseen. (TEM, 2021)

Suomessa ydinenergia-alan ylin johtaminen ja valvonta kuuluvat työ- ja elinkeinoministeriölle, joka edustaa Suomea kansainvälisissä järjestöissä ja osallistuu kansainvälisten sopimusten neuvottelemiseen sekä niiden toteutumisen valvontaan ja seurantaan. Suomen Säteilyturvakeskus puolestaan vastaa ydinturvallisuuden ja -säteilyn käytön valvonnasta ja sen määräykset ja ohjeet ovat osa ydinenergia-alan säädöskokonaisuutta. Varsinaisten ydinlaitosten valvontaan ja niitä koskevaan päätöksentekoon osallistuvat muun muassa valtionhallinnon ja aluehallinnon organisaatiot sekä laitoksien sijaintikunnat. (TEM, 2021)

2.3 Rautatiemarkkinoiden kehittyminen

Euroopan komissio julkaisee muutaman vuoden välein kertomuksen Euroopan parlamentille ja neuvostolle rautatiemarkkinoiden kehityksen suunnasta. Seuranta perustuu Euroopan parlamentin ja neuvoston direktiiviin 2012/34/EU 15 artiklan 4 kohtaan. Vuonna 2021 julkaistu kertomus oli järjestyksessään seitsemäs. Tämä kertomus kattaa tiedot vuoteen 2018 asti, joten siinä ei ole vielä tietoja koronapandemian vaikutuksista rautatiealaan. (Euroopan komissio, 2021, s. 2)

Kertomuksessa käsiteltävään alueeseen kuuluu EU:n jäsenvaltioiden lisäksi Norja sekä Yhdistynyt kuningaskunta, joka oli vuoden 2020 tammikuun 31. päivään asti myös EU-jäsen. Kertomuksessa esitetään yleiskatsaus rautatiealan markkinoiden kehittymisestä tutkittavalla alueella. Aiheita ovat esimerkiksi rautatieyritysten käytössä oleva infrastruktuuri sekä palvelut, rataverkon tilanne, käyttöoikeuksien käyttö sekä tehokkaamman rautatieliikenteen kehittämisen esteet. (Euroopan komissio, 2021, s. 2) Digitalisoinnin edistämisen myötä rautatieliikenne voitaisiin nähdä yrityksen kannalta houkuttelevampana vaihtoehtoina tavaraliikenteelle. Uuden sähköisten eFTI-kuljetustietojen asetuksen myötä yritysten ja viranomaisten välinen tietojenvaihto on mahdollista toteuttaa myös digitaalisesti. (Euroopan komissio, 2021, s. 19)

Monien eri toimijoiden osalta on yritetty laatia kattavia ohjeistuksia, menettelytapoja sekä työkaluja kyberturvallisuuteen liittyen. Yksi yhteistyöhön keskittyvä EU:n kumppanuustaho on EU:n itsensä rahoittama Shift2Rail (S2R), jonka pyrkimyksenä on huomioida ja ohjeistaa kyberturvallisuuden osalta muun muassa CYRAIL-projektissa, joka on puolestaan osa EU:n yhteistä Horizon 2020 -ohjelmaa. (Traficom, 2020, s. 5) Shift2Rail-yhteisyrityksen kanssa solmittavan kumppanuuden myötä voidaan keskittyä kehittämistyöhön digitalisaation ja automaation avulla (Euroopan komissio, 2021, s. 19).

Suomessa raideliikenteen ohjauksen modernisointiin liittyen on käynnistetty Digirata-hanke vuonna 2019. Hankkeen selvitysvaihe sekä valmisteluvaihe ovat jo päättyneitä ja tällä hetkellä käynnissä on kehitys- ja verifiointivaihe, joka on alkanut syksyllä 2021. (Digirata, n.d.) Ensimmäinen modernilla raideliikenteenohjauksen järjestelmällä varustettu osuus on

suunniteltu Tampere-Pori/Rauma -rataosuudelle. Rakennusajan on suunniteltu tapahtuvan vuosina 2025 ja 2026. Uudella järjestelmällä varustetun osuuden varsinainen käyttöönoton ajankohta olisi suunnitelman mukaan vuoden 2026 toisella neljänneksellä. (Digirata, 2021).

2.3.1 Raideliikenteen digitalisoituminen Suomessa

Suomessa nykyisin käytössä olevan junien kulunvalvontajärjestelmän eli JKV:n käyttöiän on arvioitu päättyvän 2020-luvun lopussa. Uuden korvaavan teknologian osalta on tehty laaja Digirata-hankkeen selvitystyö, jossa on tutkittu vaihtoehtoja JKV:n korvaajaksi. Selvityksen tuloksena on saatu hankkeelta ehdotus, joka puoltaisi modernin radioverkkopohjaisen junien kulunvalvontajärjestelmä käyttöönottoa Suomessa. EU-sääntelyyn perustuvien velvoitteiden myötä Suomen on otettava käyttöön ratkaisu, joka lähentäisi toimintaa Euroopan yhtenäisen rautatiealueen kanssa. (Valtioneuvosto, 2.4.2020)

Digirata-hankkeen selvitysvaiheessa raideliikenteen digitalisaation ja modernin radioverkkopohjaisen järjestelmän on arivoitu tuovan useampia hyötyjä. Tulevaisuudessa käytössä olevan digitaalisen alustan uskotaan mahdollistavan hyvät lähtökohdat uusien teknologioiden hyödyntämiselle liikenteenhallinnan sekä kaluston ja verkon kunnossapidon osalta. Rautatieliikenteen houkuttelevuudella ja sen myötä markkinaosuuden kasvattamisella voidaan vaikuttaa liikenteen päästöihin, joiden puollittamiseen vuoteen 2030 mennessä Suomi on joka tapauksessa jo sitoutunut. Ratakapasiteetin kasvattaminen olisi mahdollista uuden järjestelmän myötä, kun esimerkiksi junavälejä voidaan lyhentää. Ratakapasiteetin lisäyksellä voidaan vähentää rataverkon pullonkauloja, palauttaa liikenne nopeammin normaaliksi häiriötilanteiden jälkeen. Lisäksi parantuneen täsmällisyyden myötä on mahdollista tehostaa aikataulusuunnittelua. Radioverkkopohjainen reaaliaikainen rataverkon liikenteen rajoitteiden asettaminen tuo lisää turvallisuutta raiteiden junaliikenteelle sekä ratatöiden tekijöille. Täsmällisyyden ja tiheiden vuorovälien myötä matkustajille on mahdollisuus kehittää ja tuottaa parempaa palvelutasoa. (Valtioneuvosto, 2.4.2020)

2.3.2 Digirata-hanke

Digirata-hanke käynnistyi vuoden 2019 toukokuussa selvitys- ja valmisteluvaiheella, joka päättyi toukokuussa 2021. Nykyisen käytössä olevan junien kulunvalvonnan järjestelmän käyttöiän on arvioitu päättyvän 2030-luvun puoliväliin mennessä. Digirata-hankkeen tavoitteena on uudistaa junien kulunvalvonta, joka on elinkaarensa lopussa. Lisäksi tavoitteena on mahdollistaa turvallinen ja sujuva junaliikenne paremmalla palvelutasolla sekä kapasiteetin lisäämismahdollisuudella. Lisäksi EU:n puolelta tulevat linjaukset velvoittavat ja tuovat painetta uudenlaiseen ERTMS-toteutustavan kulunvalvontaan siirtymiselle. (Väylävirasto, n.d. -a) ERTMS muodostuu sanoista European Rail Traffic Management System ja sen kehittäminen on aloitettu jo 1980-lvulla. Euroopan rautatievirasto ERA eli European Railway Agency on asettanut perusvaatimukset sekä määritelmät ERTMS:lle ja valvoo niiden toteuttamista. (Pylvänäinen ym., 2020, s. 18)

Tällä hetkellä hankkeen kehitys- ja verifiointivaihe on käynnissä ja sen toteutuksen on suunniteltu olevan valmis vuonna 2028. Varsinaiseen hankinnan ja toteutuksen vaiheeseen on tarkoitus käynnistää vuonna 2028. Digirata-hankkeessa yhteistyökumppaneina toimivat Väylävirasto, Fintraffic, HSL, Liikenne- ja viestintäministeriö LVM, Traficom, VR sekä muita rautatieliikenteenharjoittajia. Väylävirasto ilmoittaa sivuillaan, että hankkeen tavoite on uudistaa elinkaarensa lopussa olevan junien kulunvalvonnan. Tavoitteena on myös mahdollistaa turvallisen ja sujuvan junaliikenteen, paremman palvelutason sekä kapasiteetin lisääminen. (Väylävirasto, n.d. -a)

Uusi moderni junien kulunvalvonta rakennetaan Suomeen eurooppalaisten yhteentoimivuusvaatiimusten mukaisesti ja toteutettava kulunvalvonta perustuu radioverkkopohjaiseen toteutukseen. Nykyisen junien kulunvalvonnan JKV:n tietoliikenneyhteydet on toteutettu kiinteällä verkolla. Tietoliikenteen eheyteen sekä kyberturvallisuuteen liittyen on huomioitava, että aiemmin tiedonsiirtoverkon toteutustapa on ollut piirikytkentäinen, joka poikkeaa IP-protokollaan perustuvista järjestelmistä. IP-verkossa kyberturvallisuuteen tulee kiinnittää enemmän huomiota, sillä verkkoon voidaan kytkeytyä useammalla eri tavalla. (Pylvänäinen ym., 2020, s. 41-42)

Modernissa radioverkkopohjaisessa valvontajärjestelmässä kulunvalvonta on mahdollista toteuttaa ilman näkyviä opastimia. Tämä järjestelmä on European Train Control System ETCS, jonka on tarkoituksena toimia jatkossa kestävänä teknologisena kehityspohjana. Tulevaisuudessa sen avulla on esimerkiksi mahdollisuus kasvattaa raidekapasiteettia nykyisestä. ETCS:n myötä junaliikenteen täsmällisyyttä voidaan parantaa sekä mahdollistaa junien ja matkustajien kasvava määrä nykyisellä rataverkolla. Uudella järjestelmällä junaliikenteen häiriöiden vaikutuksiet ja niiden kestot saadaan minimoitua sekä tasoristeysten ja ratatöiden turvallisuutta voidaan parantaa. (Pylvänäinen ym., 2020, s. 100)

Digirata-hankkeen selvitysprojektin yhteydessä lisäselvitysten ja suunnitelmien tekemisen jatkamista suositeltiin kahdeksan eri osa-alueeseen liittyen. Kyberturvallisuus sekä varautuminen olivat yhden osa-alueen aiheina, johon kuuluivat myös esimerkiksi kokonaisarkkitehtuurin suunnittelu, uudet paikannusteknologiat, radioverkko sekä aloitetun modernin jatkuvatoimisen paikannusjärjestelmän jatkokehittäminen. (Pylvänäinen ym., 2020, s. 98)

ERTMS-järjestelmän kyberturvallisuudesta huolehtiminen liittyy olennaisesti myös koko rautatiehallintajärjestelmän kyberturvallisuuteen. Valvontajärjestelmän yhteentoimivuuden, tekniset eritelmät ja vaatimukset on asetettu koskemaan ERTMS:ää, mutta erityisesti radioviestijärjestelmän kyberturvallisuudelle. Täydentäviä eritelmiä ja standardeja voidaan säätää myös pakollisesti noudatatettavaksi. Eurooppalainen sähköalan standardoimisjärjestö CENELEC on mukana ERTMS-järjestelmätason kyberturvallisuuden standardoimisessa ja se on tuottanut julkaisussaan Railway Applications – Cybersecurity kuvan rautatieliikenteen järjestelmäkokonaisuudesta. Kuvassa 1 on luokiteltu järjestelmiä perustuen niiden käyttötarkoituksen ja sijaintiin rautatieliikenteen toteuttamisen kokonaiskuvassa. ERTMS:n varsinainen vaikutusalue ulottuu enimmäkseen raidejärjestelmiin, mutta kulunvalvonta ulottuu myös radanvarsijärjestelmiin sekä rautatiekaluston käyttämiin järjestelmiin. (Pylvänäinen ym., 2020, s. 53, 57)

Kuva 1. CENELEC prTS 50701:2019 Railway Applications – Cybersecurity (Pylvänäinen ym., 2020, s. 57).

3 Kyberturvallisuus

Kyberturvallisuudella tarkoitetaan yhteiskunnan ja organisaatioiden toimintojen digitalisoitumisen myötä ilmeneviin uudenlaisiin turvallisuushaasteisiin. Meitä ympäröivä yhteiskunta on jatkuvasti riippuvaisempi erilsistista digitaalisesti toteutetuista järjestelmistä ja palveluista sekä niiden integroitumisista toisiinsa. Digitaaliseen kokonaisuuteen kohdistuvat kyberuhkat lisääntyvät myös jatkuvasti. Hyvin rakennettu ja ylläpidetty kyberturvallisuus suojaa toimintakykyä ja varmistaa digitaalisten ratkaisujen hyödyntämisen jatkuvuuden. (Traficom, 2020, s. 3-4) Kyberympäristö koostuu yhdestä tai useammasta toisiinsa kytkeytyneistä tietojärjestelmästä. Tietojärjestelmän parissa voi toimia useita ihmisiä samanaikaisesti käyttämässä samoja toimintoja. Henkilöstöllä on käytössä tietokoneita, jotka ovat kytkettynä toisiinsa sekä palvelimiin tiedonsiirtolaitteilla sisäisessä tietoverkossa sekä myös ulkoiseen verkkoon ja muihin tietojärjestelmiin. (Huoltovarmuusorganisaatio, n.d.)

Tietoturva käsittää tietojärjestelmässä jo olevat tiedot ja niiden käytettävyyden sekä suojauksen. Tietojen pitää olla saatavilla silloin, kun niitä tarvitaan ja niihin saa olla pääsy vain valtuuteutuilla henkilöillä. Tiedon pitää olla luotettavaa ja se ei saa olla vahingon tai tahallisen toiminnan seurauksena muutettua. Mikäli turvatoimet pettävät, voi seurauksena olla kyberympäristön toiminnan muuttuminen toisenlaiseksi, kuin on alun perin ollut tarkoitus. Kyberturvallisuudesta huolehtimalla varmistetaan, ettei kyberympäristöstä aiheudu haittaa, vaaraa tai häiriötä siitä riippuvalle toiminnalle. (Huoltovarmuusorganisaatio, n.d.)

3.1 Kyberturvallisuuden keskeisiä käsitteitä

Kyberturvallisuuden yhteydessä kriittisellä infrastruktuurilla tarkoitetaan kaikkia niitä rakenteita, järjestelmiä ja palveluita, jotka ovat elintärkeitä yhteiskunnan toiminnalle. Kriittiseen infrastruktuuriin kuuluvat esimerkiksi sähköverkko ja liikenteen ohjausjärjestelmät. Kyberuhkalla tarkoitetaan kybermaailmaan vaikuttavaa tekoa tai tapahtumaa, joka vaarantaa toteutuessaan kybermaailman oikean ja virheettömän toiminnan. Kybertoimintaympäristöä käytetään digitaalisen informaation käsittelyyn ja se

muodostuu toisiinsa yhteydessä olevista tietokoneista ja muista laitteista sekä tietoverkoista. Kyberpuolustus on kyberturvallisuuden maanpuolustuksellinen osa-alue, josta vastaa Suomessa Puolustusvoimat. Kyberpuolustukseen kuuluvat kybermaailmassa tapahtuva tiedustelu, maanpuolustuksen kannalta merkityksellisten kyberympäristöjen suojaaminen ja niihin vaikuttaminen. (Lönnqvist & Moilanen, n.d., s. 4, 7)

Palvelunestohyökkäys on verkossa tapahtuvaaa hyökkäys, jossa pyritään estämään tietyn verkkopalvelun varsinainen käyttö. Yleinen tapa toteuttaa palvelunestohyökkäys on kohdistaa kyseiseen palveluun niin paljon verkkoliikennettä, että palvelu ei enää toimi kuormittuessaan liikaa. Tietojenkalastelua kutsutaan usein englanninkielisellä termillä phishing, jossa pyritään saamaan kohteelta haltuun luottamuksellisia tietoja esiintyen tietojen saamisen oikeutettuna tahona esimerkiksi viranomaisena. (Lönnqvist & Moilanen, n.d., s. 9)

Kyberturvallisuuden yhteydessä käytetään usein CIA triad -termiä, joka muodostuu englanninkielisistä sanoista Confidentiality, Integrity ja Availability. Suomeksi lyhenteen sanat ovat luottamuksellisuus, eheys sekä saatavuus. Näitä voidaan luonnehtia kyberturvallisuuden kolmeksi peruspilariksi. Yksityisiin tai luottamuksellisiin tietoihin ei saa olla luvatonta pääsyä. Käytettävien järjestelmien ja niiden tietojen pitää olla eheitä ja järjestelmen toiminnan tulee olla sillä tasolla, että valtuutetut käyttäjät pääsevät tarvittaviin tietoihin nopeasti kiinni. (Microsoft, n.d. -a)

Sosiaalisessa mediassa, internetin keskustelupalstoilla ja kommentointiosastoilla saattaa toimia niinkutsuttu trolli, jonka tarkoituksena on vain aiheuttaa ristiriitoja sekä ärsyttää ihmisiä. Trolli voi toimia itsenäisesti omaksi ajankulukseen tai suunnitelmallisemmin esimerkiksi toimiessaan jonkin tahon puolestapuhujana. Toimintatapa perustuu siihen, että trollaaja tuo keskusteluun erittäin voimakkaan tai äärimmäisen mielipiteen samalla halventaen niiden vastustajien mielipiteitä ja argumentteja. (Lönnqvist & Moilanen, n.d., s. 10) Toimintansa perusteella trollia voisi kutsua myös riidankylväjäksi. Trollin tunnistaminen ei ole välttämättä helppoa ja suoraviivaista, mutta niiden olemassaolon tiedostaminen on hyvä pitää mielessä.

Informaatiovaikuttamisessa maalittamisella tarkoitetaan ilmiötä, jossa yksi tai useampi toimija yllyttää suurta joukkoa uhkailemaan tai hyökkäämään yhden henklilön tai instanssin kimppuun samanaikaisesti eri tapoja hyödyntäen. Kohdetta voidaan häiritä esimerkiksi lähettämällä paljon viestejä sähköpostilla tai sosiaalisessa mediassa. Kun maalittaminen kohdistuu yksittäiseen henkilöön, hyökkäyksessä useimmiten pyritään hyödyntämään henkilöstä selvitettyjä yksityiselämän tietoja ja tarvittaessa niitä väärentäen. Maalittamisen tarkoituksena on vaikuttaa henkilön taustalla olevan organisaation toimintaan tai päätöksentekoon. Maalittaminen tulkitaan järjestelmälliseksi häirinnäksi ja sen uhkan mahdollisuus on tunnistettava niin organisaatioissa kuin yksilötasolla. Mahdolliseen maalittamisen tilanteeseen tulisikin varautua jo ennakkoon suunnittelemalla ja kehittämällä toimintatapoja sekä ohjeistuksia henkilökunnalleen. (Sisäministeriö, n.d.)

3.2 Kyberturvallisuuden uhkia

Haittaohjelmilla on tarkoitus häiritä tietokonejärjestelmää ilman omistajan lupaa. Haittaohjelmat voivat esimerkiksi hidastaa tietokonetta, vakoilla sen toimintaa ja tuhota sieltä aineistoa, antaa koneen käyttöoikeudet luvattomalle käyttäjälle tai muuttavat asennettujen ohjelmien toimintaa. Kiristyshaittaohjelmaksi kutsutaan versiota, joka lukitsee laitteella olevat tiedostot ja vaativat sitten käyttäjältä lunnaita niiden vapauttamiseksi takaisin käyttöön. (Kaspersky, n.d.)

Motiivit haittaohjelmien levittämistä varten voivat olla esimerkiksi pilanteko, tuhoaminen tai vandalismi, raha tai vakoilu. Suurin osa haittaohjelmista on suunnattu yleisimmille käyttöjärjestelmille, mutta mikään järjestelmä ei ole niiltä täysin suojassa. Laitteen ja järjestelmän käyttäjä voi olla heikoin lenkki, koska hän viimekädessä päättää, minkä liitetiedoston avaa ja millä www-sivuilla vierailee. Haittaohjelmat voidaan kategorisoida ja niillä on erilaisia tominta- ja leviämistapoja. Haittaohjelmia ovat esimerkiksi madot, virukset, troijalaiset, rootkit- sekä vakoiluohjelmat. Edellämainittuja termejä saatetaan käyttää sekaisin, mutta useat nykyiset haittaohjelmat ovatkin usein edellä mainittujen ohjelmatyyppien yhdistelmiä eli hybridejä.

3.2.1 Yleisimpiä uhkia

Kiristyshaittaohjelmalle tyypillistä on laitteella olevien tietojen salaus ja manipulointi, jonka yhteydessä käyttäjältä vaaditaan salauksen purkamisesta ja tietojen palauttamisesta takaisin käyttöön. Kiristysohjelma voi kulkeutua tietokoneeseen esimerkiksi sähköpostin liitetiedostona. Kun käyttäjä avaa tiedoston ja kiristysohjelma latautuu koneelle. Kiristyshaittaohjelma muuttaa joidenkin hakemistojen tiedostoja salakirjoitettuun muotoon ja tarjoaa käyttäjälle salauksenpurkuavainta lunnaita vastaan. Lunnasvaatimusta voidaan koventaa uhkauksella levittää tai paljastaa luottamuksellista tietoa. Englanninkielistä termiä ransomware käytetään usein kiristyshaittohjelmien yhteydessä. (Sanastokeskus TSK ry, 2018, s. 32)

Madot ovat usein itsenäisesti toimivia ohjelmia, jotka kytkeytyvät toisiin ohjelmiin ja leviävät laitteista toiseen tietoverkkojen välityksellä. Madoille tunnusomaista leviämisen yhteydessä on tuhojen lisäksi verkon kuormittaminen. Yleensä madon saastutettua tietokoneen se alkaa etsiä seuraavaa kohdetta ja jatkaa leviämistään sen myötä. (F-secure, n.d. -a) Virukset ovat puolestaan jo itsessään ohjelmia tai osa ohjelmaa, joka luo itsestään uusia kopioita. Virukset tarvitsevat käyttäjältä jonkinlaisen toimenpiteen kuten liitetiedoston avaamisen sähköpostista. Tietokoneviruksille on ominaista levitä juuri sähköpostiviestien liitteiden tai pikaviestipalveluiden välityksellä. Virus on voitu naamioida liitetiedoston tai varsinaisen ajettavan tiedoston näköiseksi siten, että tiedostoa avatessa suoritukseen lähteekin viruksen oma koodi ennen varsinaista ohjelman koodia. (Microsoft, n.d. -b)

Troijalaiset ovat haittaohjelmien muoto, jossa ohjelma vaikuttaa olevan jokin hyötyohjelma tai peli, mutta todellisuudessa se kuitenkin tekee taustalla haitallisia toimintoja käyttäjän huomaamatta. Käyttäjä saadaan asentamaan troijalainen naamioimalla se esimerkiksi jonkin tunnetun ja luotetun ohjelman näköiseksi. Mikäli troijalainen on saatu asennetuksi, niin se tekee esimerkiksi laitteen asetuksiin muutoksia tai varastavaa laitteeseen tallennettuja tietoja. Troijalainen voi esimerkiksi vakoilla laitteella tehtäviä toimintoja ja sen sijaintitietoja tai verkkopalveluissa käytettäviä tunnuksia ja salasanoja, jotka se välittää eteenpäin. (F-Secure, n.d. -e)

Rootkit-tekniikkaa käytettäessä ohjelma piilotetaan järjestelmään niin, etteivät edes virustorjuntaohjelmistot havaitsisi sitä. Rootkit ei itsessään yritä levitä, mutta se pyrkii muokkaamaan esimerkiksi käyttöjärjestelmän ydintoimintoja piilottamalla sen prosesseja, tiedostoja, rekisteritietoja ja verkkoyhteyksiä. Rootkit-komponenttia hyödyntävät useat haittojelmat piiloutuakseen paremmin laitteeseen sekä suojautuakseen mahdolliselta torjuntaohjelmiston havaitsemiselta ja poistolta. Järjestelmästä voidaan havaita piilotettuja prosesseja ja tiedostoja, jotka voivat olla kuitenkin normaaleja sovelluksia. Rootkitin myötä laitteeseen asennetua ohjelmaa hyödyntäen hyökkääjä voi ottaa uhrin tietokoneen etähallintaansa siten, ettei varsinainen käyttäjä sitä edes huomaa. (F-Secure, n.d. -c)

Vakoilussa käytettävät Adware-haittaohjelmat asentuvat käyttäjän tietokoneelle esimerkiksi jonkin muun ohjelmiston yhteydessä. Tyypillisesti vakoiluohjelmalla yritetään varastaa käyttäjältä luottokorttitietoja, käyttäjätunnuksia ja niiden salasanoa, verkkopankkien tunnistetietoja sekä tietoa ylipäätään käyttäjän toiminnasta verkossa. Vakoilun lisäksi ohjelma voi olla kykenevä myös varastamaan käyttäjän tietoja. Adware näyttäytyy käyttäjälle esimerkiksi selaimen käytön yhteydessä näytölle ilmestyvillä ponnahdusikkunoden mainoksilla. (F-Secure, n.d. -d)

Euroopan neuvosto on julkaissut infografiikka-sivuillaan listauksen viidestä yleisimmästä kyberuhkista vuosien 2019-2020 välisenä aikana. Haittaohjelmat ovat olleet tutkitulla aikavälillä yleisimpiä uhkia. Yrityksistä ja järjestöistä 71 prosenttia on havainnut haittaohjelmatoimintaa, jossa ne leviävät työntekijältä toiselle. Tutkitulla aikavälillä on todettu esimerkiksi myös verkkourkinan määrän kasvaneen koronaviruspandemian aikana 667 prosenttia. (Euroopan unioni. n.d.)

3.2.2 Haitallisten ohjelmistojen jakelu

The Next Web on 2006 perustettu yhtiö, joka ylläpitää vuona 2009 avattua TNW-sivustoa. Sivustolla käsitellään uutta teknologiaa ja julkaistaan konfrenssien sarjoja sekä seurataan start-up yrittäjyyksiä. TNW julkaisi vuoden 2019 lokakuussa artikkelin, jossa kerrottiin Applen ja Googlen poistaneen mobiilisovelluskaupoistaan yhteensä yli 50 sovellusta, joiden oli havaittu näyttävän haitallisia mainoksia miljoonille käyttäjille. Google Play -sisältöpalvelun

kautta ladatut sovellukset keräsivät laitteen asetuksien ja asennettujen sovellusten tietoja. Tämä onnistui kiertämällä Google Playn asettamat turvatarkastukset. Applen iOS-järjestelmään asennetut haittaohjelman sisältäneet sovellukset kasvattivat keinotekoisesti mainostuloja painamalla kohdennettujen mainoksien linkkejä ilman varsinaisen käyttäjän toimia. (TNW, 2019)

TNW:n raportoimassa tapauksessa kyse oli haitallisista ohjelmista, jotka eivät varsinaista vahinkoa ole saaneet aikaan. Vastaavaa reittiä saataisiin myös vahingollisia sovelluksia käyttäjien laitteelle asennettua, mikäli Applen tai Googlen laaduntarkkailu pettää sovelluksien hyväksymisessä. Sovelluksien käyttötarvetta tulisikin pohtia sekä tarkastella huolellisesti ennen ja niiden lataamista ja asentamista laitteelle sekä käyttöoikeuksien ja -sopimuksien hyväksymistä. Haittaohjelmia sisältäneiden sovellusten asennuksia raportoitiin artikkelin mukaan olleen yli kahdeksan miljoonaa (TNW, 2019).

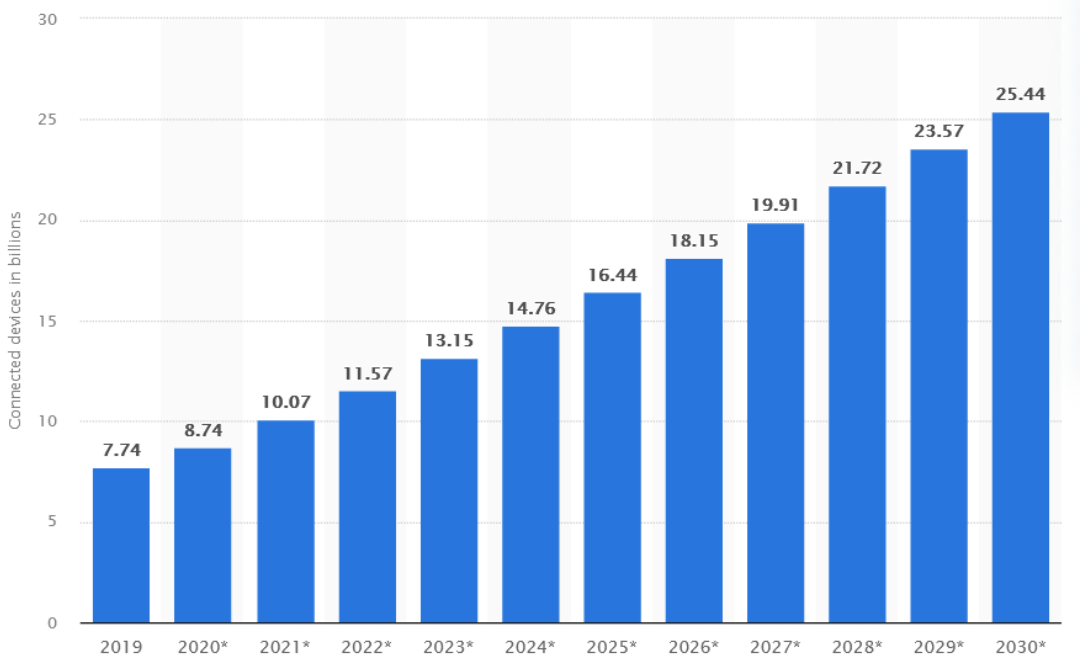
3.2.3 Esineiden internet - IoT

Esineiden internetin englanninkielinen lyhenne on IoT, joka muodostuu sanoista Internet of Things. Internetin käyttö laajentuu voimakkaasti laitteisiin ja koneisiin, joita voidaan ohjata sekä niiden toimintaa mitata verkon kautta. Esineiden internet on jo useimmille arkea sillä esimerkiksi kodinkoneet voivat jo olla yhteydessä internetiin. (Lönnqvist & Moilanen, n.d., s. 8) Osa kotiympäristössä käytettävistä laitteista on varmasti perustellusti kytkettyinä internetiin, esimerkiksi etähallittavat mittarit, älyrannekkeet sekä verkon yli ohjattavat turvajärjestelmät. Erilaisia IoT-laitteita hyödynnetään myös kodin ulkopuolella esimerkiksi terveydenhuollon, eri liikkumismuotojen ja palvelujen kehittämisen yhteydessä. IoT-laitteiden käytön ja hyödyntämisen yhteydessä pitää huolehtia, ettei laitteen tietoturva ole puutteellinen ja sen päivitykset ovat ajan tasalla. Traficom on jo muutama vuosi sitten havainnut, että haittaohjelman saastuttamista laitteista suurin osa kategorisoidaan juuri IoT-laitteiksi. (Partanen & Orkola, 2019)

Mitä käy laitteille, jotka eivät ole päivitettävissä ja saattavat unohtua verkkoon kytketyiksi, vaikka varsinaista käyttöä ei enää ole? Miten kuluttaja voisi tunnistaa haittaohjelmalla saastuneen IoT-laitteen huomataanko sitä ollenkaan? Statista-sivustolla on seuranta

verkkoon kytketyistä IoT-laitteiden määrän kehittymisestä maailmanlaajuisesti. Vuoden 2022 lukumäärän arvioidaan olevan 11,57 miljardia ja lukumäärän ennustetaan kasvavan voimakkaasti vuoteen 2030 mennessä. (Vailshery, 2022) Vuoden 2019 tilanne sekä ennuste vuoteen 2030 asti esitetään kuvassa 2.

Kuva 2. Maailmanlaajuisesti esineiden internetiin (IoT) yhdistettyjen laitteiden määrä vuodesta 2019 vuoteen 2030 (arvio). (Vailshery, 2022).



Palveluiden, sovelluksien sekä lisäksi myös erilaisten laitteiden käytön tarpeellisuutta pitäisi pystyä arvioimaan perusteellisesti ennen hankintaa ja varsinaista käyttöä niin yksityishenkilönä kuin esimerkiksi organisaation osalta päätöksiä tehtäessä.

3.3 Raideliikenteen kyberturvallisuuden riskit

Traficom on raideliikenteen kyberturvallisuuteen edistämisen suosituksessaan jaotellut liittyviä riskejä neljään pääluokkaan. Nämä luokat ovat ihmisten toiminta, järjestelmähäiriöt ja viat, epäonnistuneet sisäiset toiminnot sekä ulkoiset tapahtumat. Suosituksessa oleva luokittelu kyberriskien pääluokkiin perustuu Traficomin mukaan Cebula & Youngin 2010 teokseen. (Traficom, 2020, s. 6)

Ihmisten suorittama toiminta voi pohjautua tahattomuuteen, tahallisuuteen tai toimettomuuteen. Tahattomasti tuotettu riski voi olla virhe tai tehtävien laiminlyönti, mutta tahallisuuden kohdalla kyse voi olla suunnitelmallisesta sabotoinnista tai vandalismista. Toimettomuuden kategoriaan voi lukeutua toimia, joita ei ole huomioitu organisaatiossa syystä tai toisesta kunnolla. Esimerkiksi henkilön tiedot ja taidot ovat vanhentuneet, ja osaaminen ei vastaa enää nykyhetken vaatimuksia. (Traficom, 2020, s. 6) Järjestelmähäiriöt ja viat voivat koskea esimerkiksi laitteistoja, ohjelmistoja tai erilaisia järjestelmiä. Jos laitteiston ylläpito tai huolto ovat laiminlyötyjä, sillä ei voida enää vastata nykyhetken tarpeisiin. Ohjelmistojen kanssa yhteensopimuusongelmat sekä huonosti toteutettu muutoshallinta voivat nostaa riskitasoa. Järjestelmät voivat puolestaan olla erittäin monimutkaisia ja niiden kehittämisessä tai ylläpitotyössä on hankaluuksia saada järjestelmä vastaamaan asetettuja teknisiä vaatimuksia ja toimimaan integraatioiden myötä osana suurempaa hallittua järjestelmien kokonaisuutta. Epäonnistuneet sisäiset toiminnat tai prosessit voivat puolestaan johtua puutteellisesta toimintojen suunnittelusta ja toteutuksesta, niiden valvonnasta tai tukitoimien pettämisestä. (Traficom, 2020, s. 6)

Suosituksessa ulkoisiin tapahtumiin lasketaan kuuluvaksi katastrofit, lainsäädännölliset ongelmat, liiketoiminnan ongelmat, riippuvaisuussuhteet infrastruktuuriin ja pelastustoimiin. Katastrofeja voivat olla esimerkiksi äärimmäiset sääilmiöt, tulvat, levottomuudet sekä maailmanlaajuinen pandemia -tilanne. Lainsäädännöllisesti ongelmia voi ilmetä sääntelyn noudattamisen ja toimivuuden osalta tai esimerkiksi oikeudenkäyntien kautta. Liiketoiminnan ongelmat ilmenevät esimerkiksi markkinaolosuhteiden tai taloudellisen tilanteen kautta, mutta mahdollisesti myös alihankintaketjun häiriöiden kautta. (Traficom, 2020, s. 6)

3.4 Esimerkkejä raideliikenteeseen kohdistuneista kyberhyökkäyksistä

Vuoden 2021 heinäkuussa kyberhyökkäys lamaannutti Iranin kansallisen rautatieyhtiön IT-järjestelmät. Häiriö vaikutti matkustaja- sekä rahtiliikenteeseen. Paikallisten tiedotusvälineiden mukaan junien aikataulujen ja lippujen myynnin järjestelmä kaatui kokonaan. Alkuun tapahtumapäivänä IRIR:n eli Islamic Republic of Iran Railways:in tiedottaja kiisti huhut kyberhyökkäyksestä, vaikka asemien näyttötauluista oli tulkittavissa virheen

alkuperä. Tapahtumapäivän alkuiltaan mennessä teknisten ongelmien selvittämisessä oli edetty tilanteeseen, jossa matkustaja- sekä tavarajunat kulkivat normaalisti, mutta aikatauluistaan. Viranomaiset vahvistivat kyberhyökkäyksen seuraavana päivänä, koska kuvia vioittuneista yrityksen toimihenkilöiden työasemista oli levinnyt verkkoon. (Cimpanu, 2021)

Huhtikuun lopulla vuonna 2021 Iso-Britanniassa Liverpoolin alueella paikallisrataverkkoa hallinnoivan Merseyrail joutui Lockbit-kiristyshaittaohjelman kohteeksi. Hyökkääjät onnistuivat murtautumaan toimitusjohtajan Office 365-sähköpostitilille ja lähettämään hänen nimissään viestejä, joissa kerrottiin edellisen viikonlopun liikennekatkoksen johtuneen kiristyshaittaohjelman avulla tehdystä hyökkäyksestä. Viestien lähettämisen tarkoituksena uskotaan olleen tarkoitus painostaa organisaatiota maksamaan lunnaita. Hyökkäyksen yhteydessä työntekijöiden ja asiakkaiden tietoja varastettiin. Merseyrail vahvisti myöhemmin olleensa verkkohyökkäyksen kohde ja ilmoittaneensa siitä Iso-Britannian tietosuojaviranomaiselle Information Commissioner’s Office ICO:lle. (Cluley, 2021)

Yhdysvalloissa Bostonin lähijunaliikennettä operoiva Keolis Commuter Services joutui kiristyshaittaohjelman kohteeksi lokakuussa vuonna 2020. Hyökkäyksen yhteydessä mahdollisesti varastettiin yrityksen työntekijöiden tietoja. Yritys ei tallenna asiakkaiden matkustajatietoja, joten ne eivät vaarantuneet hyökkäyksen yhteydessä. Yrityksellä käytössä oleva uhkien havaitsemisjärjestelmä sulki verkon muutamassa tunnissa hyökkäyksestä. Yrityksen tiedottaja ilmoitti medialle, että kiristyshaittaohjelmat on poistettu käytöstä ja viranomaisille on asiasta ilmoitettu ja yritys on ryhtynyt jatkotoimiin. Keolis operoi Massachusetts Bay Transportation Authorityn (MBTA) lähiliikennerautatieverkostoa, mutta MBTA:n verkon puolelle hyökkäys ei ulottunut eikä sillä ollut vaikutusta junien operointiin. (IRJ, 2020)

Rautatiealaan erikoistunut Railway-technology.com-sivusto kokoaa alan uutisia, raportteja sekä artikkeleja ja yhdistää alan asiantuntijoita sekä toimijoita maailmanlaajuisesti. Elokuussa 2020 sivustolla raportoitiin International Railway Summit (IRS) -webinaariin liittyen, että raidelikenteen toimialaan kohdistuvien kyberhyökkäysten määrä on nousussa ja esille tuotiin tuoreet tapaukset Espanjasta sekä Sveitsistä. (Railway Technology, n.d.)

Espanjan valtion omistama rautatieinfrastruktuuria hallinnoivaan Adif:iin hyökättiin kahteen kertaan. Hyökkäyksissä hyödynnettiin REvil-kiristyshaittaohjelmaa ja niiden yhteydessä varastettiin yhteensä 800 gigatavun verran tietoja yrityksen viestinvaihdosta, sopimuksista ja kirjanpidollisista asioista. Heinäkuussa verkkorikolliset uhkasivat julkaista varastettuja tietoja, mikäli Adif ei taivu heidän vaatimuksiinsa. Espanjan rautateiden infrastruktuuriin ja operatiiviseen toimintaan kiristyshaittaohjelman ei todettu tuolloin vaikuttaneen. (Haworth, 2020)

Toukokuussa 2020 sveitsiläinen rautatiekaluston valmistaja Stadler ilmoitti tunnistaneensa omassa tietoverkkoympäristössään haittaohjelman ja ilmoitti olevan mahdollista, että tietoja olisi vuotanut. Yritys kieltäytyi maksamasta 6 miljoonan dollarin lunnaita, jolloin osa varastetuista tiedoista vuodettiin julkisuuteen. Stadler oli kykeneväinen palauttamaan käyttöön varmuuskopioistaan tarvittavat tiedot toimintansa jatkamiseksi normaalisti. (Railway Technology, 2020) Yhdysvaltalainen Cyble -kyberturvallisuusyritys selvitti tarkemmin Stadleriin kohdistunutta hyökkäystä ja sen yhteydessä varastetun aineiston sisältöä. Stadlerilta vietiin esimerkiksi talouden, tilauksien ja rahaliikenteen asiakirjoja. Netfilim-kiristyshaittasohjelmaoperaattor julkaisi kesäkuussa 2020 arviolta noin 3 gigatavun edestä Stadlerilta varastettuja tietoja ja heinäkuussa noin 28 gigatavun verran. (Cyble, 2020)

Omakohtaisesti en pysty tunnistamaan menneisyydestä tilannetta, jossa nimenomaan kyberhyökkäyksen takia esimerkiksi junalipun osto tai junamatka olisi jäänyt toteutumatta tai matkanteon viivästymisen tai kokonaan estymisen olisi ilmoitettu johtuneen kyberhyökkäyksestä. Olen noin viiden vuoden ajan käyttänyt aktiivisesti kaukojunia matkantekoon. Suurimmat haasteet ovat tulleet vastaan junalippujen ostamisessa kiireessä heikon verkkoyhteyden kanssa tai hankaluudet ovat liittyneet junamatkustamiseen Suomen talven sääolosuhteiden aiheuttamien viivästyksien kautta. Tämä on tietenkin vain näkökulma yksittäisen henkilön kokemuksien osalta. Mahdollisesti ja todennäköisesti taustalla on tehty ja tehdään edelleen paljon asiakkaille näkymätöntä työtä kyberuhkiin varautumiseksi ja varsinaisten kyberhyökkäysten torjumiseksi.

4 Työvälineet kyberturvallisuuden hallintaan ja kypsyystason mittaamiseen

4.1 EU Toolkit -välineistö kyberturvallisuuteen

Euroopan komission liikenteen ja liikkumisen pääososto MOVE on julkaissut EU:n kyberturvallisuuden välineistön, jonka avulla liikenne- ja kuljetusalan henkilöstöllä sekä alan johtajilla ja päätöksentekijöillä olisi mahdollisuus saada perusymmärrys kybeturvallisuuden uhkakuvista sekä riskien realisoitumisen jälkeisistä vaikutuksista liikennettä ohjaaviin järjestelmiin. Välineistön dokumenttia ja sen sisältöä kuvataan luonteeltaan ohjeellisiksi, joten sen sisältämät suositukset eivät ole vielä tässä vaiheessa pakollisia tai sitovia määräyksiä. EU välineistön kohderyhminä ovat koko liikennealalla toimiva henkilöstö sekä eri liikennemuotojen toimialojen päätöksentekijät. (Euroopan komissio, 2021, s. 2)

Liikenteen kyberturvallisuuden välineistössä käsitellään liikennealaan kohdistuvia kyberuhkia sekä eri kohderyhmille tarkoitettuja vaihtoehtoisia tapoja lisätä kyberturvallisuuteen liittyvää tietoisuutta. Kyberturvallisuuteen liittyvä uhkaympäristö muuttuu ja kehittyy jatkuvasti ja myös liikennealaan ja kaikkien eri liikennemuotojen palveluihin ja järjestelmiin on tunnistettavissa niihin kohdistuvia kyberuhkia. (Euroopan komissio, 2021, s. 4) Välineistön kohderyhmistä henkilöstölle annetaan ohjeistuksia liikennepalveluihin kohdistuvista kyberuhkista yleisen ymmärryksen sekä tietoisuuden kartuttamiseksi. Dokumentissa käydään läpi myös kyberuhkia, tapoja niiden tunnistamiselle ja niistä raportoimiselle sekä miten uhkia voi lieventää. Päätöksentekijöiden kohderyhmälle puolestaan tuodaan esille eri liikennemuodoille soveltuvia hyviä käytäntöjä ja organisaatiotasolla toimivien välineistöön tunnistaa ja havaita uusia kyberuhkia ja suojautua niiltä. (Euroopan komissio, 2021, s. 15)

4.1.1 Liikennealan uhkaympäristö

Kyberturvallisuuden välineistössä häiriöitä tai muita vaikutuksia liikennepalveluihin aiheuttavia toimijoita ovat esimerkiksi erilaiset ryhmittymät, kyberrikolliset ja -terroristit, aktivistit sekä sisäpiiriläiset. Kyberrilkolliset pyrkivät usein saamaan rahallista hyötyä toteuttaessaan laajoja hyökkäyskampanjoita, joilla on suuret vaikutukset palvelujen toimivuudelle. Organisaatiot ja niiden toiminnan tuntevat sisäpiiriläiset ovat yleensä tietoisia

tietoturva-aukoista, joita ei ole vielä onnistuttu poistamaan. Sisäpiiriläinen voi toimia ikään kuin konsulttina esimerkiksi laajemmalle kyberrikolliselle ryhmittymälle niiden etsiessä sopivaa kohdetta. Sisäpiiriläinen voi toimia myös organisaatiossaan tahattomasti tai huolimattomasti ja aiheuttaa siten toiminnallaan kyberturvallisuustapahtumien ketjun, joka vaarantaa liikennepalvelujen turvallisuuden. Välineistössä nostetaan myös esille, että kansallisvaltiot ja valtion tukevat ryhmät voivat nousta uhkaympäristössä tekijöiksi esimerkiksi maailmanlaajuisen tilanteen jännittyessä. Kyberuhkia esitellään välineistössä suuri määrä, mutta päätasolla niitä ovat haittaohjelmat, palvelunestäminen, tietojen luvaton käyttö ja varkaudet sekä ohjelmistojen manipulointi. (Euroopan komissio, 2021, s. 7-8)

Ensimmäiseksi uhkaksi välineistössä tuodaan esille haittaohjelmat, joilla on haitallisia vaikutuksia eri liikennemuotojen toiminnalle niin organisaatio- kuin henkilötasolla. Tyypillisesti haittaohjelma asentuu organisaatiossa henkilöstön sähköpostien liitteiden kautta. Käyttäjä voi asentaa haittaohjelman myös käyttäessään esimerkiksi manipuloitua USB-laitetta kytkemällä sen tietokoneeseensa. (Euroopan komissio, 2021, s. 10) Tietoturvayhtiö F-Secure luonnehti vuonna 2017 WannaCry:ta maailman levinneimmäksi kiristyshaittaohjelmaksi. Raportteja saastuneista koneista F-Secure oli saanut yli 60 maasta. Roskapostia käytettiin WannaCry:n levittämiseen ja organisaation verkkoon sisälle päästyään se levisi kuin mato-tyyppinen haittaohjelma. (F-secure, 2017)

Palvelunestohyökkäykset vaikuttavat palvelun tai järjestelmän saatavuuteen, jolloin niiden käyttö voi estyä kokonaan. Toiseksi merkittäväksi kyberuhkaksi välineistö esittää palvelunestohyökkäystä, josta käytetään englanninkielisiä lyhennettä DoS Denial of Service. Hajautetusta palvelunestohyökkäys on puolestaan Distributed Denial of Service DDoS. Hajautetussa hyökkäyksen toteutusvälineninä ja -kanavina hyödynnetään useita järjestelmiä samanaikaisesti, jotta kohteena oleva palvelu tai järjestelmä saadaan kaatumaan erittäin suurella pyyntöjen määrällä. Organisaation tietojärjestelmien ja tietokoneiden lisäksi haavoittuvuuksia ja siten hyödynnettäviä väyliä palvelunestohyökkäykselle voi löytyä esimerkiksi internetiin kytkettyjen laitteiden haavoittuvuuksista. (Euroopan komissio, 2021, s. 10) Myös tämän vuoksi kaikkien internetiin kytkettyjen laitteiden ohjelmistojen tietoturvapäivityksien täytyy olla ajan tasalla jatkuvasti ja luotettavasti.

EU:n kyberturvallisuuden välineistön esilletuomia kyberuhkia ovat myös luvaton käyttö ja varkaus sekä ohjelmistojen manipulointi. Luvattomalla käytöllä uhkatoimijoiden tavoitteena on päästä käsiksi esimerkiksi jonkin tietojärjestelmän tai sovelluksen arkaluontoisiin tietoihin tai resursseihin. Tiedot voidaan myös varastaa jatkokäyttöä varten. Luottamuksellisten ja arkaluontoisten tietojen saamiseksi voidaan hyödyntää tietoturva-aukkojen lisäksi käyttäjiä, jotka huolimattomasti tai tietämättään luovuttavat käyttäjätunnuksen ja salasanan yhdistelmänsä pääsyä varten. Identiteettivarkaudessa henkilötietoja sekä yksilöllisiä tunnistetietoja käytetään laittomasti ja tavoitteena on saada käyttöön esimerkiksi henkilön taloudellisia tai fyysisiä resursseja. (Euroopan komissio, 2021, s. 10)

Liikennepalvelujen ja -järjestelmien turvallisuuteen voidaan tahallisesti vaikuttaa esimerkiksi virheellisillä komponenteilla tai järjestelmän manipuloinnilla. Manipuloinnilla voidaan kyberhyökkäyksessä tarkoittaa ohjelmiston toiminnan tai sen sisällön muuttamista, jotta päästään arkaluonteisiin resursseihin kiinni. Manipulointi voi tapahtua esimerkiksi naamioimalla hyökkäys ohjelmistopäivitykseksi, joka on asennettuna kuitenkin lisävahinkoa aiheuttava haittaohjelmisto. (Euroopan komissio, 2021, s. 11)

4.1.2 Hyvät käytännöt ja turvallisuustoimenpiteet

EU:n kyberturvallisuuden välineistö on luokitellut sisältönsä koskemaan koko liikennealan henkilöstöä sekä liikenteen kyberturvallisuuden osalta vaikuttavia päätöksentekijöitä. Liikennealan organisaation henkilöstöllä tarkoitetaan toimijoita operatiivisten toiminnan asiantuntijoista aina hallintohenkilöstöön. Välineistö antaa henkilöstön puolella toimiville ohjeita kyberuhkien tunnistamiselle, raportoinnille sekä vaikutusten lieventämiselle ymmärryksen ja tietoisuuden lisäämiseksi. Päätöksentekijöiden osalta välineistö tuo voimakkaammin esille eri liikennemuotoihin sopivia hyviä käytäntöjä. Hyviä käytäntöjä voi soveltaa uusien kyberuhkien havaitsemiseen ja tunnistamiseen. Lisäksi käytännöt auttavat uhkilta suojautumisessa. (Euroopan komissio, 2021, s.15-16, 21)

Henkilöstön osalta välineistössä tuodaan hyviä käytäntöjä esille haittaohjelmien torjumiseksi, palvelunestohyökkäyksien torjumiseksi, luvattoman käytön sekä varkauksien ja ohjelmistojen manipuloinnin torjumiseksi. Haittaohjelmien torjumisen osalta myös niiden

leviämisen ennaltaehkäisy on tärkeä huomioida. Toivottuun tilanteeseen päästään, kun henkilöstö noudattaa annettuja turvallisuuskäytäntöjä, organisaatiossa huolehditaan tietojen asianmukaisesta varmuuskopioinnista, varmistetaan laitteiden suojaukset niin salasanoilla kuin fyysisillä ja digitaalisilla ratkaisuilla. Epäluotettavista lähteistä ohjelmistoja ei pidä asentaa ja niiden asentamisen mahdollisuus pitää estää käyttäjiltä muutenkin. Asennettujen ja käytössä olevien ohjelmistojen osalta niiden päivitysrutiinit täytyy huolehtia kuntoon. Henkilöstöllä on harvemmin varsinaisia teknisiä työvälineitä palvelunestohyökkäysten torjumiseen, mutta heillä on mahdollisuus havaita toimintaympäristössä tapahtuvia kummallisuuksia kuten palveluiden selkeä hidastuminen tai muutoin järjestelmien tai verkon odottamaton käyttäytyminen. Selkeimpänä oireena näyttäytyy esimerkiksi palvelun kaatuminen kokonaan tai verkkoyhteyden katkeaminen. Havainnoinnin lisäksi epämääräisessä tilanteessa henkilöstöltä vaaditaan toimia, joihin heillä pitää olla selkeä ohjeistus yhteydenottoon organisaation turvallisuudesta sekä tietotekniikasta vastaaville tahoille. (Euroopan komissio, 2021, s.17-18)

EU:n kyberturvallisuuden välineistön toinen kohderyhmä on liikennealan henkilöstö, joka on vastuussa organisaatioidensa päätöksenteosta turvallisuuteen ja kyberturvallisuuteen liittyen. Kyberturvallisuuden hyvät käytännöt sekä turvallisuustoimenpiteet ovat jaoteltuja liikennemuotojen mukaan ja jaoittelussa huomioidaan lentoliikenne, meriliikenne sekä maaliikenne, joista jälkimmäiseen sisältyy myös rautatieliikenne. Hallintoon liittyen välineistössä tuodaan esille yhteneväisesti liikennemuodosta riippumatta hyviä käytäntöjä. Hallinnollisten hyvien käytäntöjen osalta välineistö kattaa viestinnän johdon ja johtokunnan välillä, fyysisen turvallisuuden sekä kyberturvallisuuden vastuuhenkilöiden ja vastuualueiden määrittelyn. Lisäksi välineistössä hallinnon tavoitteiksi on laadittu kyberturvallisuuden hallinnan takaaminen muun muassa fyysisten ja digitaalisten rajapintojen osalta, kyberturvallisuuden hallinnan sekä vastuiden ulottamisesta turvallisuusratkaisujen ja -palvelujen koko elinkaaren ajalle, johon voidaan vaikuttaa esimerkiksi toimittajien kanssa tehdyillä palvelusopimuksilla. Raideliikenteen toimialaan liittyviä järjestelmiä ovat esimerkiksi operatiiviset järjestelmät, joita ovat ohjaus- ja hallintajärjestelmät sekä merkinantojärjestelmät sekä Euroopan rautatieliikenteen hallintajärjestelmä ERTMS. (Euroopan komissio, 2021, s.32-33)

Organisaation turvallisuudesta ja kyberturvallisuudesta vastaavien henkilöiden kohderyhmälle välineistöön on koottu pääkohdat toiminnalle. Näitä ovat kyberturvallisuusuhkien tunnistaminen sekä niiltä suojautuminen, kyberturvallisuusuhkien havaitseminen sekä varsinaisen kyberturvallisuuspoikkeamien tapahtuessa siihen reagoimisen ja elpymisen suunnittelu. (Euroopan komissio, 2021, s.34-38)

4.1.3 Yhteenveto kyberturvallisuuden välineistöstä

Opinnäytetyön aineistoon selvityksen piiriin kuuluvaan kyberturvallisuuden välineistöön tutustumisen aloitin englanninkielisestä versiosta, joka oli julkaistu joulukuussa 2020. Kansallisten kielien versiot julkaistiin 2021 kesän aikana. Dokumentissa on 47 sivua, ja se voi vaikuttaa lukijalle ensisilmäyksellä laajalta paketilta. Kuitenkin rakenne etenee selkeästi liikennealan kyberturvallisuuden tilanteen taustoittamisesta ja uhkista tarkemmalle tasolle eri liikennealojen erityispiirteisiin. Kyberturvallisuuden välineistön dokumentissa on pyritty tuomaan visualisoinnin avulla havainnollistavuutta ja yhdellä sivulla voi olla vain otsikkotieto tai tietoisku korostettuna esillä. Sisällön osalta välineistö pysyy tasolla, jonka ymmärtää ilman erillistä kyberturvallisuuden koulutusta tai aiempaa syvempää perehtymistä aiheeseen.

Opinnäytetyössä huomioitiin myös välineistöstä tuotettu erillinen yhdelle sivulle mahtuva tiivistetty versio, jota voi käyttää esimerkiksi julisteena tai tietoiskuna. Kootussa sisällössä toistuu varsinaisen välineistön teema, jossa tuodaan esille suositeltuja käytäntöjä kyberturvallisuuden parantamiseksi organisaatiossa. Julisteessa todetaan, että liikennepalveluihin ja -järjestelmiin kohdistuu paljon kyberuhkia, mutta organisaation jäsenet voivat auttaa organisaatiotaan noudattamalla ohjeita ja hyviä käytäntöjä ja mahdollisissa epäselvissä tapauksissa ovat osoitettuun vastuutahoon yhteydessä. Otsikkotasolla kyberturvallisuuden välineistön julisteessa nostetaan esille haittaohjelmilta suojautuminen, palvelunestohyökkäyksien tunnistaminen, pääsynhallinta ja tietojen suojaus sekä valveutuneisuus mahdollisten ohjelmistojen manipulaatioiden kanssa. Koen, että kyberturvallisuuden välineistöstä tehty tiivis paketti julisteen muodossa olisi luonteva väylä aloittaa aiheeseen perehtyminen ja sitten keskittyä laajempaan välineistön dokumenttiin.

4.2 Traficomin suositus kyberturvallisuuden edistämisestä raideliikenteessä

Vuoden 2020 keväällä Traficomilta Kaisa Sainio on koonnut viraston tavoitteita raideliikenteen kyberturvallisuudelle. Päätavoitteeksi tällöin on määritelty raideliikenteen kyberturvallisuuden kehittäminen kokonaisvaltaisesti, johon liittyvät tehtävät kyberturvallisuuden tietämyksen ja keskustelun lisäämisestä niin kansallisesti kuin EU-tasolla. Lisäksi tavoitteisiin lukeutuu koulutuksen saatavuuden parantaminen ja raideliikenteen toimijoiden päivittäisten työrutiinien päivittäminen siten, että kyberturvallisuudesta ja sen valvonnasta huolehtiminen olisi luonteva osa normaalia arkea. (Sainio, 2020)

Kesäkuussa 2020 Liikenne- ja viestintävirasto Traficom julkaisi antamansa suosituksen kyvberturvallisuuden edistämisessä raideliikenteessä. Suositus astui voimaan heti heinäkuun 1. päivä. Suosituksen tarkoituksena on lisätä raideliikenteen toimijoiden keskuudessa tietoisuutta kyberturvallisuudesta sekä ymmärrystä kyberturvallisuusriskeistä ja kyberhyökkäyksistä. Suositus ohjaa raideliikenteen toimijoita myös vastuullisesti varautumaan ja suojaamaan omaa toimintaansa uhkilta sekä kannustaa kaikkien raideliikenteen toimijoiden yhteistyön kehittämiseen. Suosituksen kohderyhmänä ovat niin rautatiejärjestelmän kuin kaupunkiraideliikenteen toteuttamiseen osallistuvat organisaatiot sekä viranomaiset. (Traficom, 2020, s. 2)

Raideliikenteen kyberturvallisuuden suositus muodostuu kahdesta osasta, joista ensimmäinen osa sisältää kyberturvallisuuden käsitteitä, termejä ja sanastoa sekä kuvauksia keskeisistä kyberturvallisuusuhkista ja -riskeistä ja niiden hallinnoinnista. Toisessa suosituksen osassa painotutaan Traficomin laatimiin suosituksiin, joita hyödyntämällä raideliikenteen toimijat voivat kehittää omaa kyberturvallisuuden ymmärrystä ja toimintaansa. (Traficom, 2020, s. 2)

4.2.1 Suositus kyberturvallisuuden edistämisestä raideliikenteessä

Kyberturvallisuuden hyökkäys voi kohdistua rautatiejärjestelmään tai kaupunkiraideliikennejärjestelmään, jolloin hyökkäyksenseuraamuksien maantieteellinen

rajautuminen voi vaihdella. Negatiiviset vaikutukset järjestelmien toimintaan sekä liikenteen turvallisuudelle voivat kuitenkin olla merkittäviä kohteena olevasta järjestelmästä riippumatta. Tarkoituksellisesti toteutetun hyökkäyksen suorittajina voivat olla esimerkiksi yksittäiset ihmiset, organisaatiot ja ryhmittymät tai mahdollisesti jopa vieraat valtiot. Myös kohdentamaton hyökkäys voi olla organisaatiolle ja sen toiminnalle vahingollinen. Kohdentamattomien hyökkäysten määrän tiedetään olevan suurempi kuin kohdennettujen hyökkäysten. Kyberturvallisuuden uhkan lähteenä voi olla eri taho kuin varsinaisen kyberturvallisuushyökkäyksen toteuttaja on. Varsinainen hyökkäyksen toteuttaja voi olla esimerkiksi organisaation sisäinen taho, organisaation kilpailija tai heillä toimiva alihankkija, verkkorikollinen tai niiden ryhmittymä, terroristiorganisaatio tai hakkeriryhmä. (Traficom, 2020, s. 4)

Rautatiejärjestelmää pyritään Euroopanlaajuisesti yhtenäistämään yhdeksi kokonaisuudeksi, mutta tällöin vastaavasti kyberturvallisuushyökkäys voi vaikuttaa laajasti yhtenäiseen järjestelmään ja aiheuttaa siten kattavia häiriöitä valtion rataverkon toimintaan. Mahdollisessa hyökkäyksessä myös kaupunkiraideliikennejärjestelmä voi olla kohteena, joten esimerkiksi metroliikennejärjestelmää koskettavat samat uhkakuvat. Traficomin suosituksessa kannustetaan kyberturvallisuuden edistämiseen yhdessä eri toimijoiden kanssa, jotta voidaan estää yhden osa-alueen haavoittuvuuden vaikutuksien leviäminen koskemaan koko liikennejärjestelmän turvallisuutta. Suosituksessa tuodaan esille keskeinen ajatus siitä, että ”Kyberturvallisuuden edistämisessä on keskeistä ymmärtää, että kyberturvallisuus on osa raide-liikennejärjestelmän turvallisuutta eikä kyberturvallisuutta tule kokea tai käsitellä erillisenä kokonaisuutena. ” Vaikka EU:n osalta sääntelyä ei vielä toteuteta kattavasti raideliikenteen kyberturvallisuuteen liittyen, on kyberturvallisuuden oltava raideliikenteen toimijan turvallisuusjohtamisjärjestelmässä tai turvallisuuden hallintajärjestelmässä omana osa-alueena sekä kuulua kokonaisturvallisuuden johtamisen ja hallinnoinnin piiriin. (Traficom, 2020, s. 4)

4.2.2 Yhteenveto Traficomin suosituksesta

Yleissilmäyksellä Traficomin suositukseen kyberturvallisuuden edistämisestä raideliikenteessä -dokumenttiin voi todeta sen olevan rakenteeltaan erittäin selkeä ja

jäsennelty. Sisältö koostuu dokumentin tarkoituksesta, sen sisältävistä käsitteistä, kyberturvallisuuden kytkeytymisestä raideliikenteeseen sekä konkreettiset työvaiheet kyberturvallisuuden kehittämiseksi. Dokumenttiin perehtyvän pitäisi saada selkeä kuva ja ymmärryks lähtökohdasta, toimenpiteistä ja tavoitteista, joiden saavuttamiseksi Traficom on suositukset kirjannut ja julkaissut.

Kyberturvallisuuteen ja tietoturvallisuuteen aiemmin perehtyneiden henkilöiden lisäksi suosituksen sisällön pitäisi olla hyvin myös muille organisaatiossa aihealueeseen edes jossain määrin perehtyneiden osalta ymmärrettää. Traficom on suositusta täydentänyt taulukoilla, joissa on tuotu esille enemmän käytännön asioita. Esimerkiksi Kyberturvallisuus raideliikenteessä -kappaleessa raideliikenteen kyberturvallisuusuhat ja -riskit on koottu omaan taulukkoon. Taulukossa tuodaan selkeästi esille konkreettisia riskejä, millä osa-alueella niitä voi ilmetä ja mitkä ovat seuraukset riskin toteutuessa. Esimerkkejä raideliikenteeseen mahdollisesti kohdistuvista kyberuhkista on listattu myös omaan taulukkoonsa.

Traficomin suosituksen kappaleessa 4 on koottu kehittämistoimenpiteiden suosituksia, jotka ovat osittain jo hyvin käytännönläheisiä. Suositukset kyberturvallisuuden kehittämiseksi on hyvä jatko dokumentin alkupuolen kyberturvallisuusasioiden käsittelylle. Uskoisin, että raideliikenteen kyberturvallisuuden edistämisen suosituksen tuella on mahdollisuus saada ymmärys kyberturvallisuuden nykytilasta sekä lähteä kehittämään sen hallinnointia omassa organisaatiossa.

4.3 Kyberturvallisuuskeskuksen Kybermittari

Liikenne- ja viestintävirasto Traficomin alaisuudessa toimii Kyberturvallisuuskeskus, jonka toiminta on käynnistetty vuoden 2014 alussa. (Traficom, 2021) Kyberturvallisuuskeskus kehittää ja valvoo viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta sekä lisäksi tuottaa tietoturvallisuuden tilannekuvaa. Keskuksen palveluihin kuuluvat tilannekuvan ja verkostojen lisäksi myös uhkien havainnointi ja avunanto, arvionnin, hyväksynnän ja neuvonnan palvelut sekä koordinoitu harjoitustoiminta. Kyberturvallisuuskeskus CERT:in toiminnan tehtävänä on ennaltaehkäistä tietoturvaloukkauksia ja tiedottaa tietoturva-

asioista. Keskuksen NCSA-toiminto huolehtii turvaluokitellun aineiston sähköiseen tiedonsiirtoon ja -käsittelyyn liittyvistä turvallisuusasioita. NCSA tulee englannin kielen sanoista National Communications Security Authority, joka tarkoittaa suomeksi käytännössä kansallista tietoturvaviranomaista. Kyberturvallisuuskeskus ylläpitää Tietoturva Nyt! -koostesivua ajankohtaisista tietoturvauutisista. (Traficom, n.d.)

4.3.1 Kybermittari

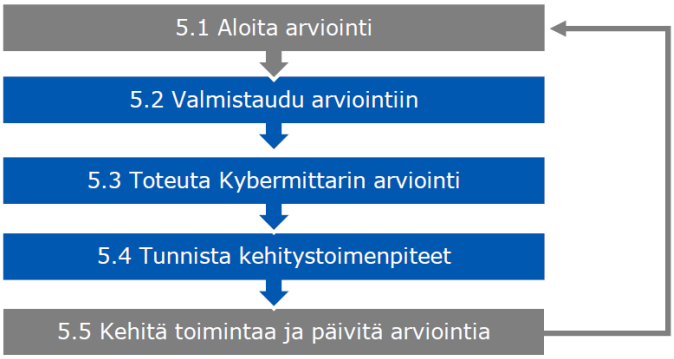
Kybertmittari on Kyberturvallisuuskeskuksen kehittämä ja se kuuluu keskuksen tilannekuvan ja verkostojohtamisen palveluun omana osa-alueenaan. Kybermittari on maksuton työkalu organisaatioiden kyberturvallisuuden arviointiin sekä kehittämiseen, ja sen kohderyhminä ovat organisaation johtotehtävissä sekä tietoturvan parissa työskentelevät asiantuntijat. Kybermittarin tavoitteena on parantaa yritysten ja organisaatioiden kykyä torjua kyberuhkia ja sen avulla organisaation johdolle voidaan toteuttaa näkymä toiminnalle tärkeiden osa-alueiden kyvykkyyksien tasoista kyberturvallisuuteen liittyen. Kybermittari esittää organisaation kyvykkyyden tason kyberriskien tunnistamisesta, suojautumisesta ja havainnoinnista sekä reagoinnin ja palautumisen osalta. (Traficom, 2022)

Kybermittari on rakennettu ensisijaisesti Suomessa toimivien yritysten ja organisaatioiden tarpeisiin, mutta se perustuu kansainvälisiin kyberkyvykkyyksien mittausmalleihin. Siihen liittyvää materiaalia ja dokumentaatiota julkaistaan suomen ja ruotsin lisäksi myös englannin kielellä. Kybermittari on toteutettu kansallisena ratkaisuna, jotta sen avulla on mahdollista vertailla suomalaisten yritysten ja organisaatioiden välillä kyberturvallisuuden kyvykkyyksiä toimialarajoista huolimatta. Yhdenmukaisen mittaamisen lisäksi Kybermittarilla voidaan saavuttaa selkeämpi lähtökohta tulevaisuuden kehittämistyölle. Yritykset, järjestöt ja julkiset toimijat sekä kaupalliset toimijat ja viranomaiset voivat vapaasti käyttää Kybermittaria. Kybermittarin perustana ovat toimineet kansainvälisesti käytetyt NIST Cybersecurity Framework sekä Cybersecurity Capability Maturity Model (C2M2). Kyberturvallisuuskeskus järjestää tapahtumia Kybermittarin käyttön tutustumiseen ja varsinaiseen käyttöönottoon liittyen. (Traficom, 2022)

4.3.2 Arviointityökalu

Kybermittarin kokonaisuuteen kuuluu olennaisena osana arviointityökalu, joka on totetutettu Excel-pohjaisena taulukkona. Ohjeistuksessa alkuun kuvataan Kybermittarin käyttöönoton vaatimukset organisaatiolta ja kuinka sitä voidaan parhaiten hyödyntää. Kybermittarin rakenne ja toimintaperiaatteet kuvataan ja ohjeistuksessa on osio yksityiskohtaisista ohjeista ja suosituksista, jotka ovat suunnattuja erityisesti arviointien vetäjille ja muille asianosaisille. Loppuosa sisältää sanaston termeistä, jota käytetään Kybermittarin käytön sekä yleensä kyberturvallisuuden yhteydessä. (Traficom, 2020, s. 4) Kybermittarin käytössä hyödynnettävä arviointiprosessi on muotoutunut työkalun käytön kartoituksesta saatujen kokemusten myötä. Kuvassa 3 esitetään arviointiprosessin viisi vaihetta, joista jokaisen osalta ohjeistuksesta löytyvät tarkemmin vaiheeseen suositeltavat osallistujat, tehtävät sekä tuotokset seuraavaan arviointiprosessin vaiheeseen hyödynnettäväksi. (Traficom, 2020, s. 5)

Kuva 3. Kyberturvallisuuden arvioinnin viisivaiheinen prosessi. (Traficom, 2020, s. 5).



Kybermittarin arviointimallin avulla arvioidaan organisaation kyvykkyyttä sekä kehittämisen kypsyysmallia kyberturvallisuuteen liittyen neljällä eri tasolla. Tasoilla kuvataan toiminnan nykytasoa asteikolla 0-3, jossa suurempi luku tarkoittaa parempaa ja tehokkaampaa toimintaa. Mikäli kategoriassa orgaisaation toiminta arvioidaan tasolla 0, niin se ei täytä kyberturvallisuuteen liittyvä vaatimuksia. Tasolla 1 toiminta täyttää vaatimukset, mutta voi olla osittain ajoittaista ja tasoltaan vaihtelevaa. Arvioinnissa tasolle 2 päästäkseen toiminnan pitä olla jo edistyneempää ja kyberturvallisuuden hallinnoinnin kuvaamiseen on käytetty myös selkeää dokumentaatiota käytännöistä. Lisäksi tarvittavat resurssit ovat käytettävissä

sekä roolit ja vastuut ovat määriteltyjä. Ylimmällä tasolla kaikki edellämainitut osa-alueet toteutuvat erittäin hyvin sekä toiminta on muutenkin edistynyttä ja kattavaa sekä kehitystyö on jatkuvaa. (Traficom, 2020, s. 10)

Kybermittarin käyttöohjeessa annetaan yksityiskohtaiset ohjeet arvioinnin vetäjälle sekä muille arviointiin osallistuville tahoille. Arvioinnissa avainhenkilöinä toimivat arvioinnin sponsorin ja vetäjän lisäksi asiantuntijoita organisaatiosta sekä mahdollisia muita kehitystyössä mukana olevia. Arvioinnin sponsorin tulee olla organisation sisäinen henkilö, joka käytännössä luo edellytykset arvioinnin toteuttamiselle sekä hoitaa organisaation johdolta tuen työskentelyyn ja varmistaa tarvittavan resursoinnin. Arvioinnin vetäjän toimenkuvaan kuuluu arvioinnin valmistelu, toteutus, käytännön järjestelyt sekä arvioinnin tulosten käsittely. Vetäjän vastuulla on myös arviointiin osallistuvien perehdyttäminen Kybermittarin ja arviointityökalun käyttöön. Arvioinnin vetäjällä tulee olla kyberturvallisuusosaamista ja rooliin voidaan nimetä esimerkiksi tietoturvapäällikkö, alan asiantuntija tai aihe-alueeseen muuten perehtynyt henkilö. Mikäli organisaatiosta ei löydy sopivaa arvioinnin vetäjää, niin myös ulkopuolisen palveluntarjoajan hyödyntäminen on mahdollista. Erityisesti pienien ja keskisuurien yritysten voi olla tarpeen hyödyntää ulkopuolista kokemusta kyberturvallisuuden kypsyysmallien käyttöön sekä kyberturvallisuuden keittämiseen. (Traficom, 2020, s. 14)

Organisaation asiantuntijoilla on tärkeä rooli tuoda yrityksen liiketoimintapuolelta sekä esimerkiksi tukitoimintojen osa-alueelta näkökulmaa ja tietäymystä arviointyöhön. Organisaation koko vaikuttaa tarvittavien asiantuntijoiden määrään, joka voi laajentua muutamasta avainhenkilöstä laajaan asiantuntijaryhmään. Arviointityön tuloksiin perustuva kehitystyö lähtee liikkeelle kehityssuunnitelmien omistajien toimesta. Tehtävään kuuluu kehityssuunnitelman laadinnan koordinointi sekä varmistaa kehitystoimenpiteille tarvittavat resurssit ja seurata suunnitelmien toteutumista. Roolissa toimivan on ohjeistuksen mukaan suositeltavaa olla organisaation sisäinen henkilö. (Traficom, 2020, s. 14-15)

Arviointiprosessin tuloksista työkalu tuottaa kolme raporttia, joita ovat yleistason raportti, tekninen raportti sekä yksityiskohtainen NIST Cybersecurity Framework Core -raportti. Yleistason raportti on suunnattu organisaation johdolle ja tekninen raportti organisaation

kyberturvallisuudesta sekä riskienhallinnasta ja muista teknisistä asioista vastaaville henkilöille. Tekninen raportti soveltuu erityisesti kyberturvallisuuden nykytilan ja tavoitetilan määrittämiseen sekä tarvittavien kehitystoimenpiteiden tunnistamiseen. NIST-raporttia voivat hyödyntää ne organisatiot, joilla on käytössä jokin toinen NIST-pohjainen arviointimalli ja haluavat hyödyntää mallia tuloksien analysointiin ja viestimiseen. (Traficom, 2020, s. 20)

4.3.3 Yhteenveto Kybermittari-työkalusta

Traficom on tehnyt suuren pohjatyön kehittässään Kybermittarin suomalaisille organisaatioille soveltuvaksi ja julkaistessaan sen kolmelle kielelle. Poiketen EU:n kyberturvallisuuden välineistöstä sekä Traficomin kyberturvallisuuden edistämisen suosituksista Kybermittari ei ole luettavissa ja koekäytettävissä yhdeltä istumalta. Kybermittariin liittyvää dokumentaatiota ovat arviointityökalun lisäksi käyttöehdot, käyttöohjeet, kybermittarin esittely sekä opas yrityksen hallituksen vastuista kyberturvallisuuteen liittyen. Opinnäytetyössä on keskitytty lähinnä itse arviointityökaluun ja sen käyttön ohjeistukseen, mutta kokonaisuus Kybermittariin liittyen on erittäin laaja ja varsinaiseen käyttöön olisi hyvä saada mukaan useampia henkilöitä organisaatiosta.

Pienemmissä yrityksissä, joissa henkilöstön resurssit ovat todennäköisesti sidottu pitkälti liiketoiminnan puolelle, voi olla hankaluuksia saada tarpeeksi resursseja mukaan Kybermittarin arviointiprosessiin. Lisäksi Kybermittarin sisältö vaatii jo syvällisempää tietämystä ja asiantuntijatason perehtyneisyyttä niin kyberturvallisuuteen kuin organisaation toimintaan ja sisäiseen hallinnointiin liittyen. Käytännössä prosessi vaatii useampien henkilöiden sitoutumista arviointiprosessin läpiviemiseen, jotta myös tulokset olisivat tarpeeksi luotettavia ja vertailukelpoisia. Kybermittarilla on varmasti tärkeä rooli suurempien yritysten ja konsernien kyberturvallisuuden kypsyystason arviointiin ja kehitystoiminnan tarpeiden kartoittamiseen. Muutaman kymmenen henkilön yritykselle tällaisena kokonaisuutena Kybermittarin käyttöä ei välttämättä pystytä resurssien puitteissa hyödyntämään ja sovittamaan käytäntöihin.

4.4 Muita välineitä kyberturvallisuuden hallinnoinnin tueksi

4.4.1 Soveltuvat standardit

Kansallisen Digirata-hankkeen osalta raideliikenteen kyberturvallisuuteen liittyviä ja käytäntöihin soveltuvia standardeja on kartoitettu ja tutkittu. Hankkeen valmisteluvaiheen loppuraportissa tuodaan esille kolme keskeisintä standardia, jotka on tunnistettu soveltuvien standardien tutkimustyön yhteydessä. Raideliikenteen toimialaan soveltuvia standardeja on tunnistettu olevan ISO 27001 -tietoturvastandardi, IEC 62443 automaatioympäristöihin keskittyvä standardi, sekä TS 50701 -standardi, joka on nimenomaan rautatieympäristöä silmälläpitäen kehitetty. Digirata-selvityksen loppuraportissa tiivistetään suunnitelmat, joiden mukaan information technologyn eli IT-järjestelmien toteuttamisen osalta käytettäisiin ISO 27001 standardia ja operational technologyn eli OT:n tai automaatiojärjestelmien toteutuksessa TS 50701 -standardia. Tarvittaessa IEC 62443 -standardia voisi käyttää tukena TS 50701 -standardille, mikäli IEC 62443:n määrityksissä ei ole soveltuvaa kuvausta rautatieympäristön toteutusta varten. (Pylvänäinen ym., 2021, s. 26)

Vuoden 2005 lokakuussa julkaistu ISO 27001 -standardi painottuu lähtökohtaisesti enemmän IT-alalle, mutta sitä voi soveltaa myös rautatiealalla. Standardi on kehittynyt 1990-luvulta lähtien ja tällä hetkellä sen päällimmäisenä tavoittena on antaa vaatimukset tietoturvan hallintajärjestelmän perustamiselle, toteuttamiselle, ylläpidolle sekä jatkuvalle kehitykselle. Tietoturvan hallintajärjestelmästä voidaan käyttää lyhennettä ISMS, joka muodostuu sanoista Information Security Management System. ISO 27001 -standardissa on käytetty voimakkaasti PDCA eli Plan-Do-Check-Act -mallia, johon kuulvat suunnittelun, toteutuksen, arvioinnin ja toiminnan -vaiheet. Vuonna 2013 päivitetyssä versiossa painotus on siirtynyt enemmän organisaation suorituskyvyn mittaamisen ja arvioinnin puolelle. (ISO 27000 Directory, n.d.) PDCA-mallia voi hyödyntää esimerkiksi kyberturvallisuusuhkien ja niiden eri muunnosten hallinnointiin sekä tietämyksen pitämisessä ajantasalla.

Toimialariippumaton IEC 62443 -standardi on kehitetty ensisijaisesti teollisuuden automaatio- ja ohjausjärjestelmien turvaamiseen ja se sisältää tällä hetkellä yhdeksän eri standardia sekä teknisiä raportteja ja eritelmiä. Standardi on siten sovellettavissa

toimialariippumattomasti. Tämän vuoksi myös tätä standardia voidaan hyödyntää esimerkiksi niin sähkönsiirron tai paperitehtaan toiminnan kuin rautateidenkin osalta. IT-standardit eivät välttämättä sovellu suoraan OT- eli operational technology-ympäristöihin, koska niiden ominaispiirteet ovat erilaisia ja suorituskyky- ja saatavuusvaatumukset ja laitteiden käyttöiät eroavat toisistaan. IT-järjestelmiin kohdistuva kyberhyökkäys todennäköisesti aiheuttaa enimmäkseen taloudellisia seuraamuksia, mutta kriittiseen infrastruktuuriin kohdistuvat kyberhyökkäykset voivat aiheuttaa myös ympäristöllisiä haittoja tai uhata ihmisten henkiä. IEC 62443 -standardin käyttöönotolla on mahdollista lieventää kyberhyökkäyksien vaikutuksia tai jopa estää niiden toteutuminen. Standardissa on ohjausjärjestelmän sisältävän tekniikan lisäksi huomioitu myös työprosesseja vastatoimia ja henkilöstöä. Kaikki riskit eivät välttämättä ole teknologiapohjaisia, joten esimerkiksi IACS:n henkilökunnalle on vaatimuksena tarvittava koulutus sekä tiedot ja taidot turvallisuudesta huolehtimisen takaamiseksi. IACS lyhenne on englanniksi Industrial Automation and Control Systems. Turvallisuuden vahvistaminen luo mahdollisuuden vähentää kohteen kustannuksia sen elinkaaren ajalta. (IEC, 2021)

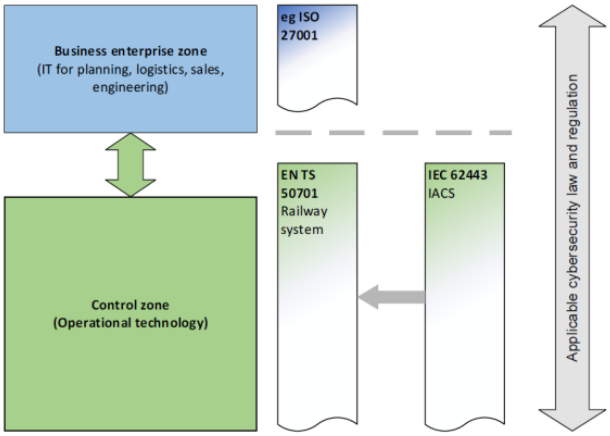
Samalla kun rautatiealalla pyritään digitaalisesti parantamaan liikenteen ja kapasiteetin hallintaa, energiatehokkuutta sekä verkon yli tapahtuvaa viestintää, mahdollisia kyberturvallisuusuhkia nousee enemmän esille. CENELEC on lähteyt toteuttamaan EU-tasoisesti TS 50701 -standardia, joka on suunniteltu vastaamaan juuri rautatiealan tarpeisiin ja vaatumuksiin. Standardia TS 50701 on nimetty ”Railway applications – Cybersecurity” -muotoon ja sen tärkein tehtävä on tarjota vaatimuksia sekä suosituksia rautatiealalle kyberturvallisuuden käsittelemiseksi ja turvaamiseksi yhtenäisellä tavalla. Standardi huomioi myös turvallisuuteen liittyvät näkökohdat ja soveltaa niitä rautatieympäristössä. TS 50701 kattaa useita rautatiealan keskeisiä aiheitä, joita ovat esimerkiksi riskien arviointi, turvasuunnittelu, kyberturvallisuuden varmistamisen ja järjestelmän hyväksymisen prosessit, haavoittuvuuksien hallinta sekä tietoturvakorjauksien hallinta. (CENELEC, 2021)

CENELEC on European Committee for Electrotechnical Standardization ja se toimii järjestönä, joka yhdistää 34 Euroopan maan sähköteknisen standardoimisen komiteat. CENELEC valmistelee sähkötekniikan alalla standardeja, joiden on tarkoitus helpottaa maiden välistä kauppaa luoden samalla uusia mahdollisia markkinoita. Standardeilla tuetaan Euroopan

yhtenäismarkkinoiden kehittymistä ja niiden avulla on mahdollista saada alaspäin myös vaatimuksien myötä muodostuvia kustannuksia. (CENELEC, n.d.) SESKO on Suomen sähköteknisen alan standardointijärjestö ja se toimii maamme kansallisena komiteana CENELEC:issä. SESKO huolehtii osaltaan, että edistettäviä standardeja valmistellaan yhdessä asiantuntijoiden, teollisuusliittojen sekä kuluttajien kanssa. (Sesko, n.d.)

Kuvassa 4 havainnollistetaan raidejärjestelmän eri osa-alueiden kytkeytyminen toisiinsa sekä osa-alueisiin liittyvien standardien kytkeytiminen toisiinsa. Vihreällä EN TS 500701 Railway system koostuu kyberturvallisuudesta raidejärjestelmässä ja siihen kytkeytyy operatiivisen turvallisuuden järjestelmä IEC 62443 IACS:n kautta. Vihreästä poikkeavalla sinisellä värillä on havainnollistettu liiketoimitapuolen käyttämät hallinnolliset järjestelmät, joihin puolestaan esimerkiksi ISO 27001 perustuu. Oikean reunan harmaa kahdensuuntainen nuoli kuvaa sovellettavia kyberturvallisuuslakeja ja -määräyksiä ja niiden huomioimista sekä kytkeytymistä rautatiejärjestelmään ja kattaen koko esiteyn toimintakentän. (ENISA-ERA, 2021)

Kuva 4. prTS 50701 overview - Scope - IT/OT. (Traficom, 2020, s. 5).



EU:n kyberturvallisuuvirasto ENISA hyödyntää toiminnassaan EU:n vuonna 2016 hyväksymää EU:n verkko- ja tietoturvadirektiiviä NIS, joka on ensimmäinen EU:n laajuinen kyberturvallisuutta koskeva lainsäädäntö. Direktiivin tavoitteena on parantaa kyberturvallisuutta kaikkialla EU:ssa, johon pyritään yhdenmukaistamalla kansallisia kyberturvallisuusvalmiuksia, ylläpidetään yhteisiä rajoja ylittävän yhteistyön käytäntöjä EU-maiden välillä sekä yhtenäistetään kriittisten alojen kansallisen valvonnan käytänteitä jokaisessa jäsenmaassa. Kriittisillä aloilla tarkoitetaan muun muassa energia-, liikenne-, vesi-,

terveys- ja rahoitusaloja sekä digitaalista infrastruktuuria. Liikenteen osalta NIS-direktiivi käsittää rautateillä liikennöinnin lisäksi vesiliikenteen, liikenteen maanteillä sekä ilmateitse. Kansallisella tasolla EU-maissa NIS-direktiivin täytäntöönpano tapahtui toukokuun 9. päivä vuonna 2018. (ENISA, n.d.)

ENISA on toiminut aktiivisesti esimerkiksi kansallisten kyberturvallisuusstrategioiden ylläpidossa, EU:n jäsenmaiden CSIRT-verkoston jäsenmaiden tukemisessa sekä kyberharjoituksien toteuttamisessa. CSIRT-lyhenne tulee sanoista Computer Security Incident Response Teams ja suomeksi lyhenteellä tarkoitetaan tietoturvaloukkauksia käsittelevää ryhmää. (ENISA, n.d.)

4.4.2 Lainsäädäntö, sääntely, määräykset ja suositukset

Traficomin suositus kyberturvallisuuden edistämisestä tuo esille, että nykyisellään raideliikenteen osalta kyberturvallisuuden sääntely on vielä kehittymisvaiheessa. Nykyisellään Raideliikennelain 1302/2018 169 § sisältää säännökset velvollisuuksista huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta sekä ilmoittamisvelvollisuudesta tietoturvallisuuteen liittyvien häiriöiden yhteydessä. Säännös nykyisellään kohdistuu vain rataverkon haltijaan sekä liikenteenohjauspalvelua tuottavaan tahoon. Taustalla on EU:n verkko- ja tietoturvadirektiivi eli NIS-direktiivi. Raideliikenteen kyberturvallisuuteen liittyen EU-sääntelyä ei varsinaisesti ole NIS-direktiiviä lukuunottamatta. (Traficom, 2020, s. 5)

Raideliikennelain 172 § kohdistuu rautatieliikenteen harjoittajiin, rataverkon haltijoihin, liikenteenohjauspalvelua tarjoavaan yhtiöön sekä kaupunkiraideliikenteen rataverkon liikenneohjauksesta vastaavaan toimijaan. Näiden tulee ilmoittaa Traficomille tietoon tulleet tapahtumat, jotka voivat vaikuttaa tilannekuvan muodostamiseen. Pykälän tulkitsemisessa voidaan todeta sen sisältävän ilmoittamisvelvollisuuden liittyvän myös kyberturvallisuusuhkiin ja -häiriöihin. (Raideliikennelaki 1302/2018)

Traficom on laatinut myös määräyksen valmiussuunnitelman järjestämisestä, jossa huomioidaan myös kyberturvallisuuden kokonaisuutta. Esimerkiksi määräystä koskevien

määritelmien kohdassa 5 kuvataan kybertoimintaympäristö, joka muodostuu yhdestä tai useammasta sähköisessä muodossa olevan datan tai informaation käsittelyyn tarkoitetusta tietojärjestelmästä. Lisäksi määritelmien kohdassa 6 kuvataan kyberuhkaksi uhka, joka toteutuessaan vaarantaa yhteiskunnan elintärkeän toiminnon tai muun kybertoimintaympäristöstä riippuvaisen toiminnon. (Traficom, 2020, s. 2) Raideliikenteen erityismääräyksissä velvoitetaan, että rataverkon haltijan on kuvattava valmiussuunnitelmassa rautatieliikenteen varmistamiseksi tarvittava rataverkko, kybertoimintaympäristö ja menettelyt sekä miten varmistetaan henkilöstön kyky ja osaaminen normaaliolojen häiriötilanteissa ja poikkeusoloissa kriittisten palvelujen edellyttämässä laajuudessa. Henkilöstöön luetaan kuuluvaksi myös palveluntuottajien ja alihankkijoiden henkilöstö. Traficomin määräys on tullut voimaan 1.6.2021. (Traficom, 2020, s. 6)

Organisaation toimintaa ohjaavaa tietosuojalainsäädäntöä ovat EU:n yleinen tietosuoja-asetus (Yleinen tietosuoja-asetus 2016/679), Tietosuojalaki (Tietosuojalaki 1050/2018), EU:n rikosasioiden tietosuojadirektiivi (Rikosasioiden tietosuojadirektiivi 680/2016) sekä Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (Laki henkilötietojen käsittelystä 1054/2018). Henkilötietojen käsittellyä koskevaa erityislainsäädäntöä ovat Laki sähköisen viestinnän palveluista (Laki sähköisen viestinnän palveluista 917/2014), Laki yksityisyyden suojasta työelämässä (Laki yksityisyyden suojasta työelämässä 759/2004) sekä Luottotietolaki (Luottotietolaki 527/2007).

Keväällä 2018 tuli voimaan EU-maissa henkilötietojen käsittelyä sääntelevä GDPR-laki, jonka lyhenne muodostuu englannin kielen sanoista General Data Protection Regulation. Tämä suomeksi yleistä tietosuoja-asetusta tarkoittavan lain myötä yksityishenkilöllä on oikeus saada tietoa omien henkilötietojen käsittelystä sekä tutustua niihin. Tietoja on mahdollisuus oikaista ja niihin pääsyä voidaan rajoittaa. Henkilön pyynnöstä tiedot voidaan poistaa, jolloin henkilö voi tulla unohdetuksi. Yleisesti ottaen EU:n tietosuoja-asetuksessa kerrotaan oikeuksista, jotka henkilöllä on silloin kun jokin yritys tai organisaatio käsittelee hänen henkilötietojaan. Kun oraganisaatio tunnistetaan henkilötietoja käsitteleväksi rekisterinpitäjäksi, on sen toteutettava asetettuja toimenpiteitä tietosuojaoikeuksien toteuttamiseksi. Lisäksi organisaation on helpotettava rekisteröidyn henkilön oikeuksien

käyttämistä. (Tietosuojavaltuutetun toimisto, n.d.) Euroopan parlamentin ja neuvoston asetuksella 2016/679 vahvistetaan säännöt luonnollisten henkilöiden suojelulle henkilötietojen käsittelyssä sekä henkilötietojen vapaaseen liikkuvuuteen. (EU:n asetus 2016/679)

Rikoslain 39:n luvuissa 28, 34, 35, 38 on kohdat kyberrikollisuuteen liittyville pykälille. Pykälät koskevat tekoja, joita ovat esimerkiksi luvaton läyttö, vaaran aiheuttaminen, vahingonteko, häirintä, loukkaus, murto ja varkaus. Yleisimpien vakavuusasteiden tasot ovat lievä, perustaso sekä törkeä. Lievällä tasolla on tuomittava lievästä tietoliikenteen häirinnästä sakkoon. Perustasolla on tuomittava tietojärjestelmän häirinnästä sakkoon tai vankeuteen enintään kahdeksi vuodeksi. Törkeällä tasolla on tuomittava törkeästä tietojärjestelmän häirinnästä vankeuteen vähintään neljäksi kuukaudeksi ja enintään viideksi vuodeksi. Mikäli rikos kohdistuu tietojärjestelmään, jonka vahingoittaminen vaarantaisi energiahuollon, yleisen terveydenhuollon, maanpuolustuksen, oikeudenhoidon taikka muun näihin rinnastettavan yhteiskunnan tärkeän toiminnon, täyttää se aina törkeän tietojärjestelmän häirinnän kriteerit. Huomioitaava on, että jo pelkkä yritys on myös aina rangaistava teko. (Rikoslaki 39/1889)

4.4.3 Riskienhallinnan prosessi

Kyberturvallisuudesta huolehtiminen on osa organisation riskienhallintaa. Riskit voivat olla strategisia ja operatiivisia tai taloudellisia ja vahinkoriskejä, jotka kaikki omalta osaltaan uhkaavat toiminnan jatkuvuutta toteutuessaan. Organisaatiolla pitäisi olla kyky tunnistaa riskejä, jotta se tietäisi ylipäätään miltä on suojautumassa ja miten suojautuminen voitaisiin parhaiten toteuttaa. Riskienhallinta ei ole pelkästään varsinaisten riskien etsintää, vaan sitä voisi luonnehtia jatkuvaksi prosessiksi, jossa tehdään jatkuvaa analysointia tarvittavista toimenpiteistä. Lisäksi täytyy olla mahdollisuus mitata toimenpiteiden vaikutuksia ja niiden myötä toteutuneiden ongelmien poistoja. (Suomen Riskienhallintayhdistys ry, n.d.)

Riskit tunnistamisen ja yksilöinnin myötä on kuvattava varsinainen riski ja minkälaista vahinkoa se voi tuottaa tapahtuessaan. Lisäksi riskin todennäköisyys tulee arvioida sekä minkälaisia toimenpiteitä riskin toteutuessa tarvitaan ja minkälaiselle vakavuusasteelle riski

määritellään. Riskin seuranta ja seurannan säännöllisten toimenpiteiden kartoittaminen ja varsinainen jalkauttaminen käytäntöön, jotta suunnitelmat eivät jää vain teoreettisiksi pohdinnoiksi.

Riskien hallinnan toiminnan raameja kutsutaan englanninkielisellä termillä Risk Management Framework, jonka lyhenne on RMF. RMF:n toteuttamisesta ja kuvaamisesta on useita eri versioita, mutta pääpiirteittäin niissä on samankaltaiset sisällöt. Kuvassa 5 prosessin eteneminen on esitelty kellon etenemistä mukailevalla kuvaamistavalla. Esitystavassa havainnollistuu prosessin eteneminen kuudessa sen vaiheessa. (Impactmakers, n.d.)

Kuva 5. Risk Management Framework. (Impactmakers, n.d.).

Ensimmäisessä vaiheessa (Categorize Information Systems) luokitellaan riskit sekä analysoidaan minkälaisia ne ovat ja mihin kaikkeen niillä on vaikutusta. Riskienhallintaa ei kannata lähteä toteuttamaan isona organisaatiotason kokonaisuutena, vaan ennemmin lähestyy sitä kyberturvallisuuden näkökulmasta ja luokittelee järjestelmät toimintaperiaatteen mukaisesti. Toisessa vaiheessa (Select Security Controls) määritellään turvakontrollit, jolloin on päätettävä jonkin tietyn standardin mukaisten kontrollien noudattamista vai käytetäänkö jotain omaa mallia. (Impactmakers, n.d.)

Kolmannessa riskienhallinnan kehitysvaiheessa (Implement Security Controls) otetaan käyttöön ne turvakontrollit, jotka on edellisessä vaiheessa määritelty noudatettavaksi. Kontrollista ja käytännöistä tulee tuottaa myös dokumentaatio, jota voidaan käyttää jatkossa kontrollin toteuttamisen tukena. Tämän jälkeen neljännessä vaiheessa (Assess Security

Controls) arvioidaan, että toteutuuko laadittu kontrolli vai ei. Esimerkiksi dokumentaatiolla on kuvattu turvakontrolliksi se, että työasemat tulee olla aina lukittuina, kun työntekijä ei ole samassa tilassa. Neljännessa vaiheessa arvioidaan, että toteutuuko tämä kontrolli käytännön työskentelyn yhteydessä vai ei. (Impactmakers, n.d.)

RMF:n viidennessä vaiheessa (Authorize Information Systems) tarkastetaan riskien määrittely ja tarkistetaan että kaikki kunnossa. Tämän lisäksi toimitetaan tarvittavat tiedot vastuuhenkilölle, jonka vastuualueella kyseinen toiminta on. Lopuksi kuudennessa vaiheessa seurataan, että täyttyykö asetetut kontrollit vai ei. Mikäli kontrollt eivät toteudu, niin prosessin läpikäynti aloitetaan alusta ja selvitetään asiat, mitä on mahdollisesti unohdettu ja muokataan kontrollin sisältöä tarvittaessa. (Impactmakers, n.d.)

5 Rautatieliikenteen operaattoreiden näkökulma

5.1 Haastatteluun valmistautuminen

Opinnäytetyön toteuttamisen yhteydessä olin yhteydessä ensisijaisen kohderyhmän organisaatioihin, joita ovat Suomessa toimivat uudet rautatieliikenteen operaattorit. Yrityksiin oltiin ennakkoon yhteydessä kiinnostuksesta osallistua opinnäytetyöhön ja tutkimukseen haastattelun muodossa. Yhteydenotossa painotettiin, että haastattelujen tarkoituksena selvittää operaattoreiden tuntemusta kyberturvallisuuteen varautumiseen tarkoitettujen välineiden osalta, sekä kyvykkyyden tasoa niiden hyödyntämistä yrityksen toiminnassa kyberturvallisuuteen liittyen. Haastattelut toteutettiin Teams-kokouksina, jotka myös tallennettiin sekä litteroitiin aineiston myöhempää käsittelyä selkeyttämään.

Haastateltaville lähetettiin ennakkoon haastattelukysymykset (Liite 1) tutustumista varten ja kysymysten oli tarkoitus toimia myös ohjaavana runkona haastattelutilaisuuksissa. Kysymykset olivat luokiteltuja koskemaan yleisiä tietoja, kyberturvallisuuden tehtävien järjestämistä yrityksessä, tietoturvan ja kyberturvallisuuden hallinnoinnin nykytilaa sekä valikoitujen kyberturvallisuuden työvälineiden tuntemusta ja hyödyntämistä yrityksen toiminnassa. Yritystä koskevien kysymyksien perusteella oli tarkoitus saada kuva toiminnan laajuudesta ja kehittymisestä toimialalla. Kyberturvallisuuden tehtävien osalta kysymyksillä tarkennettiin yrityksessä toteutettua työnjakoa tietoturvallisuuden ja kyberturvallisuuden osalta sekä muutoinkin kartoitettiin resurssien ja koulutustarpeiden tilannetta. Tietoturvan sekä kyberturvallisuuden nykytilaa koskevilla kysymyksillä oli tarkoitus kartoittaa yrityksessä toteutettuja toimenpiteitä sekä varautumisen astetta kyberturvallisuusuhkiin. Lisäksi kohdeyrityksiltä pyrittiin selvittämään mahdollisia toteutuneita kyberturvallisuuden uhkia ja minkälaista vahinkoa ne olivat saaneet aikaan sekä minkälaisilla toimenpiteillä niistä toivuttiin jatkamaan normaalia toimintaa.

Kyberturvallisuuden työvälineistä tutkimukseen otettiin mukaan EU:n Cybersecurity Toolkit eli kyberturvallisuuden välineistö, Traficomin suositus kyberturvallisuuden edistämisestä raideliikenteessä sekä Traficomin Kyberturvallisuuskeskuksen julkaisema Kybermittari. Haastattelussa oli tarkoituksena selvittää, miten hyvin yrityksessä tunnetaan nämä

kyberturvallisuuden työvälineet ja onko niitä hyödynnetty jollain asteella organisaation toiminnassa myös käytännössä. EU:n Cybersecurity Toolkitiin liittyvillä kysymyksillä selvitettiin yrityksen tietämystä kyberuhkista sekä niihin suojautumisesta ja mahdollisesti toteutuneista uhkista toipumisen käytäntöjä. Lisäksi Toolkitin avulla selvitettiin kyberuhkista raportoimisen käytäntöjä sekä yrityksessä olevaa rooli- ja vastuualueiden jakoa. Traficomin suosituksiin liittyen haastattelukysymykset koskivat suosituksessa esilletuotuja kehittämiskohtia, kuten turvallisuusjohtamista ja turvallisuuskulttuuria sekä kyberturvallisuuteen liittyvän osaamisen, pätevyyden sekä yhteistyön lisäämistä ja hyödyntämistä. Kybermittarin osalta haastattelulla pyrittiin selvittämään työvälineen mahdollinen hyödyntäminen toiminnan arvioimiseen sekä kehitystarpeiden kartoittamiseen. Kybermittari on työvälineenä erittäin laaja, joten yritys on jo aiemmin mahdollisesti hyödyntänyt siihen tarjolla olevaa tukea sekä koulutuksia.

5.2 Fenniarail Oy

Fenniarail Oy:ltä haastateltiin marraskuussa 2021 yrityksen turvallisuuspäällikköä Juha Vuorista Teams-kokouksessa. Haastateltava luonnehti yrityksen olevan Suomen toiseksi tai kolmanneksi suurin rautatieliikenteen harjoittaja katsantakannasta riippuen. Fenniarail on alun perin perustettu vuonna 2009, mutta toiminnan käynnistäminen ja markkinoille tulemisen vaihe kesti huomattavan kauan, joten varsinainen liikenne alkoi vuonna 2015. Fenniarail työllistää tällä hetkellä 25 henkilöä ja sillä on useampia junia ajossa päivittäin. Yrityksellä oli haastattelun ajankohtana käytössään kuusi diesel-veturia. Yrityksen pääkonttori sijaitsee Helsingissä, jonka lisäksi Kouvolassa sekä Imatralla sijaitsevat operatiivisen henkilöstön työpisteet. Kotkassa sijaitsevissa huoltotiloissa ei ole varsinaista henkilökuntaa ja tiloja käytetään vain kaluston huoltoon. (J. Vuorinen, henkilöhaastattelu, 18.11.2021)

Fenniarail pyrkii omalta osaltaan kasvattamaan rautatieliikenteen käytön houkuttelevuutta ja markkinaosuutta Suomessa. Yritys on keskittynyt puhtaasti tavaraliikenteeseen ja kulkumuodon käytön kasvattamisen tarkoituksena on myös vaikuttaa tavarakuljetuksien ympäristöystävällisyyteen sekä liikenneturvallisuuteen. Yritys aloitti sahatavaran säännöllisen kuljettamisen junaliikenteen vuonna 2016 ja vuonna 2018 toiminta laajeni

yhteistyökumppani UPM:n Venäjän tuontipuun kuljetussopimuksen myötä. Fenniarail kuljettaa Suomen puolella kokonaisuudessaan UPM:n tuotantolaitoksille Venäjältä tulevan puutavaran. (J. Vuorinen, henkilöhaastattelu, 18.11.2021)

Vaikka Suomi kuuluu EU:hun ja EU-tasoiset vaatimukset koskevat kaikkia jäsenmaita, niin vertailu Suomen ja muiden EU-maiden rautatieliikenteen toimijoiden kesken on haasteellista keskeisten erojen takia. Keski-Euroopassa rautatieyritksen perustaminen on hyvin suoraviivaista. Yrityksen perustamisen jälkeen hankitaan asiakas tai useampia ja sen jälkeen vuokrataan kalusto, sillä alueella on toimivat vuokramarkkinat. Markkinoille tulon kynnys on hyvin alhainen ja kohtuullisen pienellä pääomalla sekä selkeillä rahoitusmalleilla yrityksen saa toimintaan. Suomessa on käytössä oma kansallinen raideleveys, jonka myötä esimerkiksi vuokrakaluston hankkiminen on erittäin haasteellista ja täten täytyy investoida myös omaan kalustoon. Suomessa on kolme isompaa toimijaa ja heidän välillään kilpailu on todella kovaa. (J. Vuorinen, henkilöhaastattelu, 18.11.2021)

5.2.1 Toimintaympäristö

Rautatieliikenteen operatiivisen toiminnan puolelta Fenniarail käyttää liikenteenohjausyhtiö Fintrafficin tietojärjestelmiä sekä muita työvälineitä. Toimistohenkilökunnalla on käytössään kannettavat tietokoneet ja älypuhelimet, joiden lisäksi operatiivisella puolella toimivilla kuljettajilla on käytössä päätelaitteet junayksiköiden kuljettamisen KUPLA-sovelluksen käyttöä varten. Ulkoinen palveluntarjoaja huolehtii yrityksen laitehallinnasta sekä siihen liittyvistä tietoturvaratkaisuista. Toimintatapa on määritely hyvälle normaalitasolle siten, että palveluntarjoaja huolehtii esimerkiksi automaattisista päivityksistä laitteille. (J. Vuorinen, henkilöhaastattelu, 18.11.2021)

Fenniarail Oy:n toimihenkilöiden määrä on alhainen ja turvallisuuspäällikkökin toimii tehtävässään ilman alaisia. Työroolissa on lähtökohtaisesti keskitytty rautatie- ja työturvallisuuden puolelle, mutta erityisesti muutaman viime vuoden aikana tietoturva- ja kyberturvallisuusasioihin liittyvien työtehtävien määrä on lisääntynyt selvästi. Fenniarail huolehtii asianmukaisesti myös tietosuoja-asetuksisen toteutumisesta osaltaan. Yritys toimii

myös rautatiealan oppilaitoksena, jonka myötä yritys ylläpitää henkilörekisteriä koulutuksista. (J. Vuorinen, henkilöhaastattelu, 18.11.2021)

Vuorinen toi haastattelun aikana esille, että operaattorit saavat nykyään paljon hyödyllistä tietoa, suosituksia sekä työvälineitä kyberturvallisuuteen liittyen Traficomin puolella toimivan kyberturvallisuuden erityisasiantuntijan toimesta. Kansallisella ja EU-tasolla annettujen määräysten ja velvotteiden Vuorinen toivoisi kuitenkin olevan sellaisessa suhtessa, että pienimmätkin toimijat kykenevät noudattamaan niitä ilman, että tekeminen muuttuu liian raskaaksi tai hintavaksi. Vuorinen muistutti, että riskienhallintaan kuuluu myös arvioida riskien hyväksyttävä taso. (J. Vuorinen, henkilöhaastattelu, 18.11.2021)

Vaikka EU-tasolta tuotetaan jäsenvaltioissa toimiville rautatiealan yrityksien toimintaan liittyviä suosituksia sekä vaatimuksia, Vuorinen arvioi, että tietojärjestelmien sekä toimintatapojen suoraan vertaaminen EU-tasolla ei ole järkevää vaan yhteistyön painotus tulisi olla ennemminkin kansallisesti suomalaisten yritysten kesken. Traficom on sopivassa roolissa toimiessaan tahona, joka koordinoi turvallisuustyötä ja yleensäkin yhteistyötä kansallisesti. Samanaikaisesti Traficom toimii myös suomalaisena edunvalvojana ja linkkinä ulospäin EU-tasolle ja sieltä takaisinpäin. Fenniarailin puolelta on koettu hyväksi toimintamalliksi se, että aktiivinen tiedottaminen ja viestintä tapahtuu Traficomin suunnalta ja yritys voi sitten arvioida oman osallistumisensa tilaisuuksiin tarpeen ja resurssitilanteen mukaan. (J. Vuorinen, henkilöhaastattelu, 18.11.2021)

5.2.2 Tietoturvan ja kyberturvallisuuden nykytila

Palveluntarjoajan kautta hallinnoidaan työntekijöiden kannettavia tietokoneita sekä työtehtävien suorittamiseen liittyviä mobiililaitteita sekä niiden päivityksiä. Yrityksessä on käytössä myös kolmannen osapuolen ohjelmistoja, jotka eivät ole palveluntarjoajan sopimuksen piirissä. Kolmannen osapuolen ohjelmistotuotteiden osalta päivityksien ajantasaisuus ja niiden myötä haavoittuvuuksien korjaamisen toteuttamisessa on tunnistettu haasteita. Yrityksessä käytössä oleva tietoliikennettä turvaava VPN-ohjelmiston tietyssä versiossa oli ilmennyt haavoittuvuus. Tämä haavoittuvuus ja sen vaatimasta korjauspäivityksestä ei tullut ohjelmistotoimittajalta suoraan selkeää tietoa

päivitystarpeesta, vaan tilanne selvisi vasta paljon myöhemmin Traficomin kyberturvallisuuden yhteistyöryhmän asiantuntijoiden kesken käydyn keskustelun yhteydessä. Jälkeenpäin asian tutkinnan yhteydessä selvisi, että ohjelmistotoimittaja oli kuitenkin jossain vaiheessa julkaissut verkkosivuillaan tiedon haavoittuvuudesta ja sen korjaavasta päivityksestä. Nämä tiedot löytyivät kuitenkin vasta tarkemman tutkimisen yhteydessä useamman linkin takaa. Suurempien toimittajien ohjelmistojen haavoittuvuuksista ja niitä korjaavista päivityksistä ilmoitetaan pääsääntöisesti avoimesti ja näyttävästi sekä mahdollisimman pian havainnon jälkeen. (J. Vuorinen, henkilöhaastattelu, 18.11.2021)

Fenniarail Oy:llä on käytössä itse kehitetty toiminnanohjausjärjestelmä. Tällä toiminnanohjausjärjestelmällä ohjataan kuljettajien toimintaa ja kalustoa, seurataan junien sijainteja ja niiden etenemistä reiteillään. Järjestelmällä voidaan myös muodostaa junakokoonpanoja ja tarkistaa niiden jarrutuskyvyn riittäminen laskennallisesti. Järjestelmää käytetään verkon yli ja se sijaitsee kaupallisella vuokrapalvelimella. Pavleluntarjoajan palvelimiin on toiminnanohjausjärjestelmän käytössäolon aikana kohdistunut kahdesti palvelunestohyökkäys. Molemmat näistä hyökkäyksistä on tunnistettu kohdistumaan palveluntarjoajan hallinnoimiin palvelimiin, joissa myös Fenniarailin järjestelmä sijaitsee. Havaittujen palveluestohyökkäyksien arvioitiin kestäneen korkeintaan muutamia tunteja. Hyökkäyksillä ei ollut näillä kerroilla vaikutusta yrityksen päivittäiseen toimintaan ja junien kulkuun. (J. Vuorinen, henkilöhaastattelu, 18.11.2021)

Vastaavien tilanteiden varalta toiminnanohjausjärjestelmän jatkuvan toiminnan varmistamiseksi on suunniteltu ohjelmiston kahdentamista palvelinkokonaisuuden arkkitehtuurissa. Tämä ratkaisu ei ole kuitenkaan vielä edennyt toteutukseen saakka. Kahdentamisen yhteydessä on mahdollinen riski varsinaisen järjestelmän sekä varajärjestelmän tietojen ajantasaisuuden sekä yhteneväisyyden varmistamisen osalta. Teknisesti ja kustannuksiltaan kahdentaminen olisi mahdollista, mutta tietojen ajantasaisuuden osalta on vielä asioita ratkaisematta ja kahdentamisen myötä saattaisi ilmetä lisäriskejä toimintaan ja käytettävyyteen liittyen. Tämän vuoksi yrityksessä on toistaiseksi koettu, että muilla aiemmin määritellyillä varajärjestelyillä on mahdollista pitää toiminta käynnissä myös häiriön aikana. Poikkeustilanteessa voidaan toiminta varmistaa

manuaalisella työllä, mutta mikäli kyseessä olisi laaja koko yhteiskuntaa koskeva poikkeustilanne, niin varajärjestelmä toimii käytännössä, vaikka pelkästään lyijykynää ja ruutupaperia käyttäen. (J. Vuorinen, henkilöhaastattelu, 18.11.2021)

Toiminnanohjausjärjestelmän suunnittelemattoman tai suunnitellun käyttökatkon jälkeen esimerkiksi junien kulkutiedot syötetään järjestelmään manuaalisesti tilastollisten sekä kirjanpidollisten syiden takia. Toiminnanohjauksen kautta on mahdollista seurata muun muassa maksettujen ratamaksujen määrää ja oikeellisuutta sekä kaluston kilometripohjaista huolto-ja komponenttien vaihtoväliä. Häiriötilanteiden varalta yrityksessä on käytössä vaihtoehtoinen seurantaratkaisu, jonka avulla voidaan varmistaa tietojen oikeellisuus sekä ajantasaistaa ne myös toiminnanohjausjärjestelmän puolella. Komponentit tarvitsevat huoltoa tai vaihtoa tietynlaisen kilometrimäärän jälkeen ja tietojen täytyy olla luotettavia, jotta tarvittavat toimenpiteet toteutetaan ajallaan. Esimerkiksi jo 1000 kilometrin puuttuminen tilastoista on merkittävä, mikäli komponentin huoltoväli on 30000 kilometriä. Palvelunestohyökkäys hankaloittaa tai pahimmillaan estää toiminnanohjausjärjestelmän käytön, mutta järjestelmään tunkeutuminen todennäköisesti aiheuttaisi vain sekaannuksia ja ylimääräistä selvittelytyötä. Järjestelmässä ei ole sen tason yrityssalaisuuksia, että niiden takia tunkeutumista kannattaisi yrittää. Vastaavat tiedot voi tarvittaessa selvittää esimerkiksi ratapihalla tehdyn kävelykierroksen yhteydessä. Vuorinen arvioi, jotta toiminnanohjausjärjestelmään tunkeutuja pystyisi lähettämään oikeanlaisia tietoja oikealla sisällöllä sekä elementeillä, niin tunkeutujan täytyisi tuntea kohtalaisen hyvin suomalainen rautatiejärjestelmä ja sen ominaispiirteet. (J. Vuorinen, henkilöhaastattelu, 18.11.2021)

Yrityksen nykyisen toiminnan laajuuden sekä toiminnanohjausjärjestelmän käyttöön peilaten vaikutukset määräytyvät sen mukaan, mihin vuorokauden aikana hyökkäys tapahtuu. Mikäli hyökkäys tulee ajallisesti kriittisellä hetkellä ja tämän vuoksi ei saada junaa kulkuun ajallaan, taloudelliset vahingot saattavat muutaman tunnin palvelunestohyökkäyksen ja toiminnan pysähdyksen myötä jäädä vähäisiksi. Mikäli pahin skenaario tapahtuisi ja juna kulkeminen estyy ja jää ajamatta samalla vaikuttaen asiakkaan kuljetuskokonaisuuteen, niin rahallisen vahingon määrä voisi nousta hyvin merkityksellisiksi. Suuremman vahingon yhteydessä luvut voivat ovat realisoituessaan todella huomattavia etenkin pienelle yritykselle. (J. Vuorinen, henkilöhaastattelu, 18.11.2021)

Näiden suurempien poikkeamien lisäksi Vuorinen kertoi, että tunnistavat jatkuvasti todennäköisiä tietojen kalasteluyrityksiä sekä yksittäisiin päätelaitteisiin tunkeutumisen yrityksiä. Näiden osalta Fenniarail on teknisen varautumisen lisäksi huolehtinut henkilöstönsä koulutuksesta ja varautumisesta vastaavien tilanteiden osalta. Henkilöstölle tiedotetaan säännöllisesti muistutuksia ja tietoja esimerkiksi parhaillaan liikkeellä olevista huijauspuheluista tai muista tietojen kalasteluyrityksistä. Henkilöstön kanssa on käyty perussäännöt sekä käytännöt läpi, miten yritysessä käsiteltävää tietoa ja heidän laitteitaan suojataan vastaavilta uhkilta. Turvallisuuspäällikkö arvioi, että nämä käytännöt soveltuvat pienyritykselle ja niiden huomiointi ja käytännön toteuttaminen ovat yrityksessä tällä hetkellä hyvällä perustasolla. (J. Vuorinen, henkilöhaastattelu, 18.11.2021)

5.2.3 Kyberturvallisuuden työvälineiden hyödyntäminen

EU Cybersecurity Toolkit Poster:ia esiteltässä Vuorinen heti totesi, että näki kyseisen dokumentin ensimmäistä kertaa. Tietoiskun tapaisessa julisteessa tuodaan esille kyberturvallisuuden huolehtimisesta ylätason kategoriat sekä niihin luokiteltuja tehtäviä. Nämä ovat kuitenkin Fenniaraililla toteutettuja. Ylemmällä tasolla julisteessa kehoitetaan suojautumaan haittaohjelmilta, tunnistamaan mahdolliset palvelunestohyökkäykset, suojaamaan tiedot ulkopuolisilta pääsyiltä sekä tunnistamaan mahdolliset ohjelmistojen manipulaatiot. Vuorinen luetteli näihin kategorioihin liittyviä tehtäviä, jotka ovat vähintään huomioitu yritytyksen toiminnassa ottamalla toimenpiteet käyttöön tai käytännöt ovat muuten järjesteltyinä. Tutkimuksessa mukana ollut varsinainen EU Cybersecurity Toolkit -ohjeistus ei myöskään ollut haastateltavalle entuudestaan tuttu. Tässä dokumentissa on tarkemmalla tasolla selvitetty Poster:in huomioitavia turvallisuuskäytänteitä ja haastattelun teon hetkellä siitä oli julkaistu vasta 47 sivuinen englanninkielinen versio. (J. Vuorinen, henkilöhaastattelu, 18.11.2021)

Traficomin Suositus kyberturvallisuuden edistämisestä raidelikenteestä -julkaisuun haastateltava oli jo tutustunut aiemmin. Tämän suosituksen dokumentti on kaikkinensa yhteensä 17 sivua pitkä, joten se on saatu koottua tiiviiseen pakettiin ja sen sisältämät varsinaiset kehittämiskohdat on selkeästi luokiteltu ja esitelty dokumentissa. Otsikoiden aihepiirit ovat huomioituja Fenniarailin toiminnassa ja ovat kunnossa. Vuorinen pohti

kuitenkin, että olisiko näihin kuitenkin tarve pystyä panostamaan vieläkin enemmän. Aihepiiriä voisi tarkastella vielä lisää lähetymällä nostettuja aiheita iteraatioilla, jolloin kerros kerrokselta syvennyttäisiin asiaan ja samalla parannettaisiin sitä. (J. Vuorinen, henkilöhaastattelu, 18.11.2021)

Kyberturvallisuuskeskuksen tuottama Kybermittari ja sen arviointityökalu ovat Vuoriselle myös tuttuja entuudestaan. Hän toteaa työkalun olevan varmasti toimiva ja sen käytöllä päästään analysoimaan osa-alueita syvällisemmälle tasolle, jolle suuremman organisaation tulee päästäkin. Pienempien toimijoiden osalta Kybermittarin laajuus sekä osittain myös erikoissanastoon ja -lyhenteisiin painottuva sisällön sopivuus pienempien organisaatioiden osalta ei puolestaan tunnu niin suoraviivaiselta ja tarkoituksenmukaiselta. Mikäli organisaatiosta ei löydy sopivaa asiantuntijaa, jolla on täysin hallussa termistö ja koko kyberturvallisuuden aihealue, niin pelkästään sisällön ja kysymyksien selvittämiseen saa kulumaan erittäin paljon aikaa. Pienemmillä organisaatioilla ei ole välttämättä henkilöresursseja, joilla olisi mahdollista ottaa Kybermittari kokonaisvaltaisesti käsittelyyn. Tällaiset organisaatiot tarvitsisivat ja varmasti ottaisivat mielellään vastaan esimerkiksi Traficomilta valmiiksi tuotteistetun mallin, jossa asian käsittely olisi erittäin selkeää ja käytännönläheistä. (J. Vuorinen, henkilöhaastattelu, 18.11.2021)

Fenniarail on viime vuonna tuottanut ja ottanut käyttöön inhimillisten ja organisatooristen tekijöiden HOF-strategian liittyen heidän turvallisuusjohtamisjärjestelmäänsä. Lisäksi hiljattain he ovat myös laatineet turvallisuuskulttuurin edistämisstrategian. Traficomin suosituksen kappaleessa 4.1 käydään läpi kyberturvallisuuden toimiminen osana turvallisuusjohtamista ja turvallisuuskulttuuria, ja kappaleeseen viitaten yrityksessä olisi tarpeen määrittää ensi tilassa kyberturvallisuusstrategia. Vuorinen toteaa, että pienen organisaation kannalta olisi erittäin tervetullutta, mikäli esimerkiksi juuri kyberturvallisuusstrategian osalta aineistot olisivat hyvin pitkälle valmisteltu ennakkoon. Tällöin toimija voisi hyödyntää resurssiensa käyttöä konkreettisiin parannustoimenpiteisiin. Lukuisten strategioiden laatiminen voi muodostua työlääksi, jolloin henkilöstöstä enää löydykään tarpeeksi resursseja niiden varsinaisen toteuttamisen edistämiseksi. Lisäksi skaalautuvuutta ja sen mahdollisuutta tulisi huomioida selkeämmin. Strategiatasolla liikkuminen ja niiden hyödyntäminen voi soveltua hyvin tuhansien työntekijöiden konserniin,

mutta pienemmän organisaation kohdalla muutaman kymmenen työntekijän tavoittaminen tapahtuu tehokkaasti erilaisen ja pienemmän organisaatiorakenteen myötä. (J. Vuorinen, henkilöhaastattelu, 18.11.2021)

5.2.4 Yhteenveto Fenniarail Oy:n tilanteesta

Fenniarail Oy:n turvallisuuspäällikön kanssa käydyn haastattelun perusteella organisaation varautumisen nykytilanteen kyberturvallisuuteen liittyen arvioisin olevan hyvällä tasolla. Organisaatiossa kyberturvallisuusasiat ovat tulleet mukaan muuhun turvallisuustoimintaan ja sen vaatima hallinnoimisen taso on saatu toteutettua kuitenkin jossain määrin käytössä olevien rajallisten resurssien ansiosta. Opinnäytetyössä keskiössä olevat kyberturvallisuuden työvälineistä eivät kaikki olleet aiemmin tuttuja, mutta niiden sisältämät asiat ovat kuitenkin huomioituja. Turvallisuuspäällikkö Vuorisella on selkeä kokonaiskuva nykytilanteesta sekä siitä, mitä toimia ollaan kehittämässä ja mihin suuntaan kehittämistä tulisi viedä heidän kannaltaan. Erityisen hyvänä huomiona pidän sitä, että yhteistyö Traficomin kyberturvallisuuden asiantuntijoiden kanssa on tuonut selkeyttä myös viestintään, tiedonkulkuun sekä yhteistyöhön.

Vuorinen toi esille huolensa siitä, miten paljon organisaatiolle osoitetaan suositeltavia työtehtäviä kyberturvallisuuteen liittyen, jotka voivat jatkossa olla velvottavia toimia. Fenniarail on pieni organisaatio, jossa resurssien ohjaaminen nopealla aikataululla uusiin tehtäviin on haasteellista. He toteuttavat ehdottomasti välttämättömät tarpeet, joihin voi vaikuttaa konkreettisilla toimilla, mutta erilaisten strategioiden laatimista ja toimintatapojen kehittämistä ei koeta pienessä organisaatiossa kaikkein kriittisimmäksi toimeksi. Näihin ymmärrettävästi Vuorinen toivoo Traficomin ja muiden viranomaistahojen kehittävän ratkaisun, joka palvelee suoraan käytännön toimia.

5.3 Operail Finland Oy

Suomessa toimivan Operail Finland Oy:n osalta haastateltiin organisaation IT-osaston asiantuntijaa tammikuun 2022 alussa. Haastattelu toteutettiin Teams-kokouksena ja se käytiin lähes kokonaan suomeksi, joskin joissain tilanteissa käytettiin tueksi englanninkielistä

termistöä. Operail-konserni toimii Virossa sekä Suomessa ja heidän Tallinnan toimistolla sijaitseva IT-osasto huolehtii kyberturvallisuusasioista koko organisaation osalta. Haastattelin Operailin IT-osaston Product Ownerina Tõnis Muugaa. IT osasto toimii fyysisesti kokonaisuudessaan Tallinnassa, mutta he palvelevat myös Suomen tytäryhtiötä ja Suomessa toimivaa henkilöstöä. AS Operail on Viron valtion omistama yritys, jolla on yhteensä noin 600 työntekijää, josta Suomen henkilöstöä on noin 40 työntekijää. Suomessa veturinkuljettajia on 25 henkilöä ja muiden työpiste sijaitsee yrityksen toimistolla Helsingin Vallilassa. (T. Muuga, henkilöhaastattelu, 5.1.2022)

Viron valtion omistama Eesti Raudtee perustettiin 1. tammikuuta vuonna 1992 josta lohkottiin vuonna 2009 tavaraliikenteen hallinnasta vastava AS EVR Cargo. Yhtiö muutti 2010 rakennettaan ja sen toiminta alkoi painottua rahdin kuljettamisesta enemmän vaununvuokraukseen sekä liikkuvan kaluston korjaus- ja huoltopalveluiden liikentoimintaan. Vuonna 2018 yrityksen nimi vaihdettiin muotoon AS Operail ja vuonna 2020 yrityksen toiminta laajeni Suomen rautateille. (Operail, n.d.) Operail Finland Oy:llä oli haastattelun tekohetkellä kaksi Suomessa sijaitsevaa ja toimivaa asiakasta. Asiakkaista toinen toimii Hangon Koverharin alueella ja toinen Kotkan satamasta käsin. Sen sijaan koko konsernin asiakkaiden kokonaismääräksi Muuga arvioi noin 200 ja erityisesti Venäjän puolelelta tulevia vaunuja hallinnoivia asiakasyrityksiä on paljon. (T. Muuga, henkilöhaastattelu, 5.1.2022)

5.3.1 Toimintaympäristö

Operail AS on Viron valtion omistama yritys, siihen kohdistuu kyberturvallisuuden hallinnoimisen osalta ensisijaisesti kansallinen lainsäädäntö ja asetukset. Yrityksessä kyberturvallisuuden vastuut sekä tehtävien jako on tehty IT-päällikön sekä IT-palvelutiimissä toimivien asiantuntijoiden kesken, joihin myös Muuga lukeutuu. Laajemmat kokonaisuudet hallinnoidaan IT-päällikön kautta ja palvelutiimin vastuulla päivittäisessä työssä ovat kyberturvallisuustilanteen seurannan lisäksi asiaan liittyvä tuki sekä neuvonta loppukäyttäjille. Muuga mainitsee, että hän sekä IT-päällikkö ovat aloittaneet töissä muutama vuosi sitten. Operailissa oltiin tällöin toteuttamassa toiminnan kokonaisvaltaista digitalisointia. Tätä ennen paperiset dokumentit olivat yrityksen toiminnassa keskeisessä

roolissa ja esimerkiksi rahtikirjojen, palkkalaskelmien ja vuosilomien käsittelyt tapahtuivat kaikki paperisella dokumentaatiolla. (T. Muuga, henkilöhaastattelu, 5.1.2022)

Tärkeänä osana toiminnan digitalisoinnissa toimi yrityksessä samanaikaisesti käyttöönotettu toiminnanohjausjärjestelmä, jolla esimerkiksi suunnitellaan rautatiekuljetuksille soveltuva henkilökunta sekä kuljetuksien myynti asiakkaille. Järjestelmä oli uusi kaikille työntekijöille ja se otettiin käyttöön myös Suomen toimintojen puolella. IT-osaston toiminta on ollut keskeisessä roolissa toiminnan digitalisoimisessa sekä toiminnanmuutoksen toteuttamisessa. Uuden järjestelmän kautta esimerkiksi veturinkuljettaja saa tarvittavat tiedot junan ajamista varten. Järjestelmän kautta saa tiedot päivän ohjelmasta ja kuljetuksen tiedoista, aikataulusta ja työn lähtöpaikasta, minkälainen juna ja vaunujen kokoonpano on kyseessä, sekä milloin työvuoron on tarkoitus päättyä. Työtä tukee myös säätietojen seurantamahdollisuus, jotta lumitilanteen tai lämpötilojen myötä voi ennakoida tulevaa työpäivää. (T. Muuga, henkilöhaastattelu, 5.1.2022)

Yrityksen henkilökuntaa koulutetaan kyberturvallisuuteen liittyen Cybexer-sivuston ja siihen liittyvän testiympäristön avulla. Kyberturvallisuudesta vastaavat henkilöt osallistuvat lisäksi asiantuntijoille suunnattuihin koulutuksiin sekä alan kokoontumisiin, joita on järjestetty ulkopuolisten tahojen toimesta. Esimerkiksi lokakuussa 2021 Operailin kyberturvallisuudesta vastaavat osallistuivat suomalaisen Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry:n järjestämään Huoltovarmuusorganisaation koulutukseen kyberturvallisuuden hallinnan työkaluihin ja hyviin käytäntöihin liittyen. (T. Muuga, henkilöhaastattelu, 5.1.2022) Lisäksi Muuga toi esille, että IT-osaston henkilöitä on osallistunut aktiivisesti Euroopan unionin kyberturvallisuusviraston ENISA:n järjestämiin webinaareihin raideliikenteen kyberturvallisuudesta, joista uusin järjestettiin vuoden 2021 marraskuun lopulla. (ERA-ENISA, 2021). Toiminnan digitalisoituessa on Operail on panostanut voimakkaasti myös työntekijöidensä koulutuksiin. Yrityksessä työskentelevistä suurimmalla osalla ei ollut entuudestaan tarvittavia taitoja tai kokemusta älypuhelimien, tietokoneiden tai erilaisten tietojärjestelmien käyttöön. (T. Muuga, henkilöhaastattelu, 5.1.2022)

Toimistotyöntekijöillä sekä veturinkuljettajilla on pääsääntöisesti käytössä työnantajan puolesta tietokone sekä älypuhelin. Microsoftin tuotteita käytetään paljon, mutta myös

muiden toimittajien ratkaisuja ja järjestelmiä on käytössä. Järjestelmien ylläpito ja päivitykset hoidetaan keskitetyn hallinnan kautta. Uudet päivitykset ja järjestelmäversiot tarkistetaan ennen niiden asentamista tuotantoympäristöön. Päivytykset asetetaan aluksi karanteeniin, jossa niiden sisältö ja toiminnallisuus tutkitaan ja käydään läpi. Tarkastuksissa varmistetaan, ettei päivitys sisällä esimerkiksi viruksia tai haittaohjelmia. Mikäli päivityksessä ei ole mitään epäselvää, sopii IT-osasto ajankohdan päivityksen teolle tuotantoympäristöön esimerkiksi toimistoaikojen ulkopuolelle, jotta useimpien työnteko ei häiriintyisi tai keskeytyisi. (T. Muuga, henkilöhaastattelu, 5.1.2022)

5.3.2 Tietoturvan ja kyberturvallisuuden nykytila

Yrityksessä on käytössä työvälineet, joiden avulla voi seurata kyberturvallisuuden tilannekuvaa IT-ympäristössä. Muuga toteaa, että heihin kohdistuu jatkuvasti ulkopuolisia hyökkäyksiä, joista osan he ovat tunnistaneet olevan kiristyshaittaohjelmia tai muutoin rahan kiristämiseen liittyviä hyökkäyksiä. Näiden tunkeutuminen Operailin verkkoon ei ole onnistunut. Hyökkäykset jäävät palomuurissa kiinni ja niiden eteneminen verkossa estetään. Taustalla toimiva järjestelmän ilmoitetaan suodattavan sähköposteista 99,9% varmuudella roskapostit ja muuten vahingolliset sähköpostit. Mikäli kuitenkin jokin epäilyttävä sähköposti pääsee suodattimen läpi, niin loppukäyttäjät on ohjeistettu ottamaan välittömästi yhteyttä IT-palvelutiimiin viestin vaarallisuuden tarkistamiseksi. (T. Muuga, henkilöhaastattelu, 5.1.2022)

Työntekijät tarvitsevat henkilökohtaisen salasanan päästäkseen kirjautumaan yrityksen tietokoneelle. Operail käyttää salasanan asettamisessa käytäntöä, jonka myötä käytettävän salasanan tulee olla vahva. Salasanan pitää olla tarpeeksi pitkä sekä sisältää isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä. Mikäli tietokoneen käyttäjä haluaa päästä Operailin sisäisen verkon palvelimien tiedostoihin kiinni, hänellä täytyy lisäksi olla aktivoituna VPN-yhteys, jossa käytetään erillistä salasanaa. (T. Muuga, henkilöhaastattelu, 5.1.2022) VPN tulee englanninkielisistä sanoista Virtual, Private ja Network ja se tarkoittaa virtuaalista erillisverkkoa, jonka avulla salataan käytettävä verkkoyhteys. (F-Secure, n.d. -b)

Yrityksessä on käytössä kaksivaiheinen tunnistautuminen, jolloin kirjauminen vahvistetaan salasanan lisäksi myös jollain toisella tavalla (T. Muuga, henkilöhaastattelu, 5.1.2022). Kaksivaiheisella tunnistautumisella on tarkoituksena estää luvaton käyttö, vaikka varsinainen salasana olisikin kaapattu. Salasanan lisäksi tunnistamiseen käytetään joko kertaluonteista koodia tekstiviestin tai erillisen sovelluksen kautta toimitettuna tai jotain yksilöivää fyysistä ominaisuutta. (Hernández, 2020) Esimerkiksi yrityksen älypuhelimiin kirjautumisessa käytetään henkilön sormenjälkeä tai kasvojen tunnistusta laitteen tarjoamien ominaisuuksien mukaan. Työkäyttöön tarkoitettujen älypuhelimien osalta sovelluksien asentaminen Applen AppStoren ja Googlen PlayStoren kautta on rajoitettu vain tarpeellisiin sekä työhön liittyviin sovelluksiin. Muita sovelluksia laitteille ei voi ladata ja asentaa. Lisäksi laitteiden tausta-asetuksiin on määritelty estoja haitallisiksi tunnistetuille internet-sivuille. Yrityksessä yleisenä käytäntönä on, että henkilöstöllä on erilliset älypuhelimet työkäyttöä sekä omaa henkilökohtaista käyttöä varten. (T. Muuga, henkilöhaastattelu, 5.1.2022)

5.3.3 Kyberturvallisuuden työvälineiden hyödyntäminen

Tutkimuksen kohteena olevien työvälineiden tuntemuksen ja hyödyntämisen tasot ovat haastattelun perusteella vaihtelevalla tasolla. EU Cybersecurity Toolkit Poster sekä varsinainen Toolkit-dokumentti olivat Muugalle entuudestaan tuttuja. Operailin IT-osaston kyberturvallisuudesta vastaavat ovat hyödyntäneet aiemminkin Euroopan unionin kyberturvallisuusviraston ENISA:n palveluja esimerkiksi järjestettyjen kyberturvallisuuteen liittyviin webinaareihin osallistumisen myötä, joten myös materiaalien ja dokumentaation lähteenä taho on entuudestaan tuttu. Toolkit Poster:issa otsikkotasolla esilletuodut asiat ovat Operailin puolella järjestetty kuntoon. Esimerkiksi organisaatiossa käytäntöihin kuuluvat jo toimintatavat vahvan salasanan käytölle, varmuuskopioiden käytännöille, järjestelmäpäivityksien hallinnoimiselle ja jakelulle sekä pääsynhallinnan osalta. (T. Muuga, henkilöhaastattelu, 5.1.2022)

Haastateltava toteaa, että ovat sisäisesti aiemmin käyneet läpi sisällön Traficomin suosituksen kyberturvallisuuden edistämisestä raidelikenteestä. Haastattelun aikana kävimme sisällön ylätasolla läpi ja totesimme, että suosituksen kehittämistoimenpiteet ovat tunnistettavasti käynnissä. Kyberturvallisuus on Operailissa otettu osaksi

turvallisuusjohtamista ja turvallisuuskulttuuria sekä osaamista kehitetään sekä henkilöstöä koulutetaan edelleen. Kyberturvallisuusuhkia seurataan jatkuvasti ja niihin on varauduttu niin teknisillä toimenpiteillä kuin seuraamusten jälkihoidollisten prosessien osalta. Yhteistyö muiden toimijoiden kanssa kehittyy ja laajenee luonnollisesti esimerkiksi suomalaisten ja virolaisten toimijoiden osalta yrityksen toimiessa aktiivisesti näissä maissa. (T. Muuga, henkilöhaastattelu, 5.1.2022)

Kyberturvallisuuskeskuksen tuottama Kybermittari ja sen arviointityökalu eivät olleet tuttuja entuudestaan haastateltavalle. Haastateltavalle toimitettiin ennen haastattelua materiaalin mukana Kybermittarin arviointityökalun versio 1.0. Muuga ei ainakaan oman työroolinsa kautta ole päässyt hyödyntämään arviointityökalua kyberturvallisuuden tilannekuvan muodostamiseksi Operailin toiminnasta. Kuitenkin ennen haastattelua hän ehti tutustua materiaaliin sekä tutkia Kybermittarin dokumentaation sisältöä. Hän arvioi, että suurin osa arvioitavista kohdista on jo huomioitu sekä toteutettu organisaatiossa. Ylipäätään sisältö oli vaikuttanut varsin selkeältä, mutta muutamat kuvaukset käytännöistä olivat tuntuneet vaikeaselkoisilta tai niiden varsinainen tarkoitus oli jäänyt hieman epäselväksi. Kybermittarin käyttöä Operailin toiminnan arvioinnissa Muuga ei voi todentaa, mutta asiat on kuitenkin hoidettu kuntoon todennäköisesti muita työvälineitä ja käytäntöjä hyödyntäen. (T. Muuga, henkilöhaastattelu, 5.1.2022)

Kyberturvallisuuskeskus tuottaa palveluna myös kyberharjoituksia, joiden avulla voidaan selvittää kyberhäiriöiden vaikutuksia organisaation toimintaan. Harjoituksessa kyberhäiriötä mallinnetaan luoden kuitenkin todellista tilannetta vastaavat olosuhteet. Tavoitteena on selvittää organisaatioiden toimitavalmiuksia ja reagointikyky vastaavissa tilanteissa ja löytää toiminnassa mahdollisia puutteita, joihin voidaan löytää soveltuva ratkaisu (lähde: kyberturvallisuuskeskus). Operail on toteuttanut organisaation sisäisen kyberturvallisuusharjoituksen keväällä 2021, jossa käytiin läpi kaikki yrityksessä käytössä olevat järjestelmät sekä palvelimet. Yhtenä harjoituksen tehtävänä oli toimittaa sähköpostiviestiksi naamioituja kyberturvallisuusuhkia, mutta tavoitteena oli yleensäkin löytää kaikkia mahdollisia virheitä tai ongelmakohtia, jotka voisivat vaarantaa yrityksen toimintaa. Koko harjoituksen läpivienti kesti kuukauden verran ja sen myötä löytyi korjaus- sekä parannuskohteita, joiden korjaamisen suunnitelma syksyllä sai yrityksen johdolta

hyväksynnän. Operail yrityksenä pitää toiminnan turvallisuutta tärkeimpänä asiana, ja siihen kuuluvat niin turvallisuus rautateillä kuin turvallisuus IT-asioiden osalta. (T. Muuga, henkilöhaastattelu, 5.1.2022)

Yrityksen toiminnan painopiste on Virossa, joten tutkimuksen piirissä olevien työvälineiden sijaan Operail hyödyntää kyberturvallisuusasioissa ensisijaisesti Viron valtion kansallisen tietojärjestelmäviranomaisen RIA:n tukea, suosituksia sekä ohjeistuksia. Kuitenkin Operail tekee jatkuvasti yhteistyötä myös Traficomin kanssa. Välillä ajankohtaiset asiat painottuvat selkeästi maantieteellisesti jompaankumpaan maahan, jolloin ehdotettujen toimenpiteiden kiireellisyys ja tarve voivat poiketa huomattavasti maiden välillä. Esimerkiksi akuutisti esille tulleen uhkan osalta käytettyä teknologiaa ei Viron puolella ole koskaan käytetty, mutta Suomessa vastaavan teknologian käytöllä voi olla pitkät perinteet ja teknologialla on vuosien saatossa muodostuneet laaja-alaiset integroutumiset muihin järjestelmiin ja kriittisyys sen myötä. Tällöin reagointi ja jatkotoimenpiteiden vaatimukset ovat erilaisia maasta riippuen. (T. Muuga, henkilöhaastattelu, 5.1.2022)

5.3.4 Yhteenveto Operail Finland Oy:n tilanteesta

Operail Finland Oy kuuluu osana Viron suurimpaan tavaraliikennöitsijään Operailin organisaatioon ja yrityksen kyberturvallisuusasioista vastaa Viron puolella toimiva IT-osasto. Operailin IT-puolen Product Ownerin kanssa käydyn haastattelun perusteella organisaatio on panostanut viimeaikoina erityisen paljon kyberturvallisuuden hallintaan, johon on vaikuttanut voimaakkaasti myös hiljattain toteutettu toimintatapojen digitalisointi. Organisaatiossa on huomioitu tutkimuksen kohteena olevien työkalujen asiasisällöt ja EU:n tuottama Toolkit sekä siihen liittyvä tietoisku-poster ja niiden sisällöt olivat sellaisenaan tunnettuja. Koska yrityksen toiminnan pääpaino on Viron puolella sekä kyberturvallisuudesta vastaavat tahot toimivat myös Virosta käsin, niin heille luonnollisesti ensisijainen tiedonlähde sekä kyberturvallisuuden toimintaa ohjaava taho on virolainen Riigi Infosüsteemi Amet eli RIA, jonka roolia ja toimintaa voisi verrata Suomessa toimivan Traficomin Kyberturvallisuuskeskukseen. Operail tekee yhteistyötä myös Traficomin kanssa sekä on mukana EU-tasoisissa rautatieliikenteeseen keskittyvissä yhteistyörymissä.

Haastattelun kysymyksien pohjalta Muugan toi etenkin teknisen näkökulman kautta esille organisaation kyvykkyyden vastata kyberturvallisuuden haasteisiin ja päivittäisiin uhkiin. IT-puolella on mahdollista saada tekninen tilannekuva kyberhyökkäyksistä, joita kohdistuu organisaatioon jatkuvasti, mutta niiden torjunnassa onnistutaan myös. Henkilöstöllä on suuri rooli sekä vastuu huomioida mahdollisia uhkien toteutumisia, joita varten heidät on koulutettu sekä ohjeistettu toimimaan tarvittaessa. Kyberturvallisuuden hallinnoinin osalta Muuga tunnisti Kybermittarin arviointityökalun vastuita ja tehtäviä, jotka on huolehdittu organisaatiossa kuntoon jo aiemmin. Operailin toiminnan digitalisoimisen yhteydessä organisaatiolla on ollut hyvä tilaisuus vastata samanaikaisesti kyberturvallisuuden haasteisiin, sillä vanhempia historian myötä periytyviä tietojärjestelmiä eikä niihin liittyviä käytäntöjä ole ollut käytössä.

6 Yhteenveto

Raideliikenteen toimiala digitalisoituu voimakkaasti. Suomessa nykyinen junankulunvalvontajärjestelmä on elinkaarensa päässä kuluvan vuosikymmenen loppuun mennessä ja korvaava järjestelmä tulevaisuudessa toimii radioverkkopohjaisesti. Modernilla digitaalisilla ratkaisuilla tavoitellaan niin kapasiteetin nostoa raiteilla kuin parempaa toimintavarmuutta ja turvallisuutta. Rautatieliikenteen hallintajärjestelmän ja junien kulunvalvonnan modernisoinnin ja digitalisoinnin yhteydessä on mahdollista kehittää myös muita raideliikenteeseen liittyviä järjestelmiä ja niiden integroitumista keskenään. Uusien digitaalisten järjestelmien myötä kyberturvallisuus sekä uhkien lisääntyvä määrä täytyy huomioida voimakkaammin kehitystyössä. Kyberturvallisuuden hallintaan ja tietämykseen liittyviä työvälineitä on tuotettu organisaatioille, jotta ne pystyvät vastaamaan kehittyvään tilanteeseen.

Opinnäytetyön tavoitteena oli tuottaa raideliikenteen operaattoreiden organisaatioissa tietämyksen kyberturvallisuuteen varautumiselle ja sen hallinnoinnille parhaita toimintatapoja, jotka voi myös yhteensovittaa päivittäiseen liiketoimintaan sekä säännölliseen kehitystyöhön. Opinnäytetyön tarkoituksena oli selvittää raideliikenteen operaattoreiden tämänhetkinen tietämys tarjolla olevista kyberturvallisuuden työvälineistä sekä niiden mahdollisesta hyödyntämisestä organisaation toiminnassa sekä kyberturvallisuuden kypsyystason arvioinnissa sekä kehityskohteiden tunnistamisessa.

Opinnäytetyön toimeksiantajalla Liikenne ja viestintävirasto Traficomilla on oma roolinsa tuotta raideliikenteen organisaatioille suomessa tukea kyberturvallisuusasioissa ja työn tekeminen lähti liikkeelle Traficomin kyberturvallisuuden erityisasiantuntijan yhteyhdenotosta HAMKiin. Viraston näkökulmasta mielenkiinnon kohteena olivat työvälineet, joita organisaatiot voivat hyödyntää oman kypsyystasonsa, ymmärryksensä sekä kehitystarpeidensa kartoittamisessa kyberturvallisuuteen liittyen. Toimeksiantajan ja HAMKin ohjaajan kanssa käytyjen keskustelujen myötä kohderyhmäksi valikoitui Suomessa toimivat uudet rautatieliikenteen operaattorit. Kyberturvallisuuden työvälineistä ensisijaisiksi tutkimuskohteiksi valikoituivat EU:n kyberturvallisuuden välineistö, Traficomin

suositus kyberturvallisuuden edistämiseksi raideliikenteessä sekä Kyberturvallisuuskeskuksen Kybermittari.

Kyberturvallisuusasioiden hallinnoinnin nykytilan kartoittamiseksi raideliikenteen operaattoreihin oltiin yhteydessä. Operaattoreilta tiedusteltiin halukkuutta osallistua opinnäytetyön tutkimukseen. Puolet tavoitelluista henkilöistä vastasi myöntävästi kutsuun ja henkilöhaastattelut pidettiin aiemmin laaditun haastattelukysymysten rungon pohjalta. Tutkimukseen osallistuneet raideliikenten operaattorit tunnistivat osan tutkimukseen mukaan otetuista kyberturvallisuuden työvälineistä, mutta osa oli heille vieraita. Kuitenkin heidän organisaatioissaan oli työvälineiden kattava osa-alue kyberturvallisuuteen liittyen käyty läpi ja hallinnon osalta järjestetty. Molempien haastateltavien organisaatioiden osalta vastuuhenkilöt tekevät yhteistyötä kansallisten kyberturvallisuuden virastojen kanssa. Kyberturvallisuuden hallinnassa pitää huomioida niin tekniset valmiudet ja osaaminen kuin varsinaisen toiminnan ohjaaminen sekä prosessit.

Pienemmällä organisaatiolla ei ole välttämättä tarpeeksi resursseja ohjattavaksi kyberturvallisuustyöhön, jolloin tarvitaan mahdollisimman valmiita ratkaisuja ja konsepteja viranomaisen suunnasta tarvittavan kyberturvallisuuden kypsyystason ylläpitämiseksi ja kehittämiseksi. Vaikka luotettavat kyberturvallisuuden hallinnoinnin työvälineet ovat helposti saatavilla, niin niiden käsittelyyn ja toiminnan arviointiin tarvitaan aikaa. Mikäli henkilöresursseja ei suoraan voida organisaatiossa nimetä kyberturvallisuusasioista vastaaviksi, niin asiasta kiinnostuneille henkilöille voisi yrittää alkuun osoittaa pienempiä osa-alueita aiheeseen liittyen ja antaa tätä myöten kasvaa kyberturvallisuuden asiantuntijaksi varsinaisen päätoimen ohella. Tilanne ei ole kestävä, mikäli kaikki kyberturvallisuudenkin asiat ovat vain henkilön vastuulla.

Luotettavat tekniset ratkaisut suojaavat oikein käytettyinä sekä ylläpidettyinä orgaisaatioita kyberturvallisuusuhkilta. Teknisillä apuvälineillä voidaan seurata hyökkäyksien määrää ja tapaa sekä tunnistaa uhkia, joita on kohdistettu organisaatioon esimerkiksi ulkoisen verkon kautta. Henkilöstön koulutus sekä ohjeistus kyberturvallisuusuhkien osalta on välttämätöntä, jotta organisaation varsinaisen toiminnan jatkuminen pystytään takaamaan. Vahinkoja kuitenkin sattuu ja teknologiakin voi joskus pettää. Toteutunut kyberuhka saattaa vaikuttaa

organisaation tai järjestelmän toimintaan lamaannuttavasti. Tämän vuoksi uhkat on hyvä tiedostaa sekä myös tunnistaa. Tekniset ratkaisut vaativat kuitenkin rinnalleen ennakkoon suunnitellut prosessit, mikäli jossain kohtaa kyberturvallisuusuhka tai -häiriö toteutuu. Valmiiksi suunniteltu ja mahdollisesti ennakkoon harjoiteltu toiminta kyberturvallisuuden poikkeustilanteessa vähentää riskiä lisävahingon aiheuttamiselle, kun jokaisella osapuolella on tiedossa tilanteen korjaavat toimenpiteet. Kyberturvallisuus on kaikkien organisaatiossa toimivien yhteinen asia ja jokaisella on oma vastuunsa turvallisuudesta huolehtimisessa sekä tietojensa ylläpidossa.

Kyberturvallisuuden hallinnoimiseseen voi soveltaa jatkuvan kehittämisen prosessia, jossa säännöllisesti käydään aihepiirin asiat toistuvien työvaiheiden kautta. Tällä voi varmistaa, että organisaatiolla säilyy jatkuvasti vireystila vastata kyberturvallisuuden muuttuviin haasteisiin. Toimintamallia tulee olla mahdollisuus parannella ja työvaiheiden sisältöjä päivittää. Kun toimintamalli on kaikille avoin, niin siihen voi myös jokainen vaikuttaa. Kyvykkyyden ylläpitoon liittyy myös organisaation jäsenten tietämyksen tasosta huolehtiminen. Kyberturvallisuudesta huolehtimisen avoimuudella voidaan edesauttaa sen hallinnoinnin liittymistä päivittäiseen toimintaan. Mahdollisen riskitason noustessa tai uuden uhkan tunnistamisen yhteydessä tiedottamisella on suuri rooli ajantasaisten tietojen jakelussa. Organisaatiolle kyberturvallisuuden menestyksekäs hallinnointi ja kyvykkyyden ylläpitämisestä huolehtiminen tuovat todennäköisesti myös kilpailuetua toimijoiden välillä.

7 Pohdinta

Tämän opinnäytetyön teko käynnistyi keväällä 2021 ja työhön liittyvä loppuseminaari pidettiin toukokuun lopulla vuonna 2022. Vuodenvaihteen molemmin puolin käytyjen henkilöhaastattelujen jälkeen maailmanpoliittinen tilanne muuttui merkittävästi helmikuussa 2022. Molempien haastateltavien yritysten osalta tilanne on varmasti muuttunut, sillä niiden toiminta ulottui myös Suomen ja Viron itärajojen toiselle puolelle. Kyberturvallisuuden osalta muutoksia tilanteesen tuo todennäköisesti Suomen ja Ruotsin yhtäaikainen hakemus puolustusliittoon. Mahdollisten kyberhyökkäysten ja -häirintätapausten määrä tulee todennäköisesti nousemaan ajan kuluessa. Huomioitavaa on, että raideliikenne on luettavissa yhteiskunnan kannalta kriittiseksi toiminnoksi, joten poikkeustilanteessa se voidaan nähdä hyvänä kohteena esimerkiksi juuri kyberhyökkäykselle.

Turvallisuustilanteen voimakkaasti muututtua on organisaatioissa erityisen tärkeää tarkistaa oma varautumisensa taso ja ryhtyä tarvittaessa kriittisiin toimiin. On erittäin tärkeää, että organisaatioilla on mahdollisuus hyödyntää viranomaisten tarjoamaaa tukea ja palvelua myös kyberturvallisuuden osalta. Tässä opinnäytetyössä on tuotu esille viranomaistahojen roolia raideliikenteen operaattoreiden kyberturvallisuuden hallinnoimiseen liittyen. Suomen Traficomin sekä Viron Riigi Infosüsteemi Ametin työ on erittäin arvokasta ja niiden asiantuntijuuteen voi luottaa. Tärkeää on, että kyberturvallisuusasioissa tukea tarvitseva taho löytää itselleen asiantuntevaa apua sekä ohjausta.

Kyberturvallisuusuhkiin varautuminen sekä varautumistaitojen ja osaamisen ylläpitämisen lisäksi organisaation on tärkeää oman toimintansa kehittämisen lisäksi huolehtia yhteistyöstä muiden alan toimijoiden kanssa. Liikenne ja viestintävirasto Traficom toimii kyberturvallisuusasioissa viestinviejänä ja koordinaattorina Euroopan Unionin suuntaan, mutta se toimii kansallisesti raideliikenteen toimijoita yhdistävänä tekjänä. Yhteistyönverkoston kautta pienenkin organisaation on mahdollista vaihtaa muiden samalla alalla toimivien kesken kokemuksia ja tietämystä sekä hyviä käytäntöjä ja menettelytapoja kyberturvallisuuteen liittyen.

Lähteet

Aurorarail. (n.d.). *Historiamme*. Haettu 21.10.2021 osoitteesta https://www.aurorarail.fi/historia/

CENELEC. (n.d.). *About CENELEC*. https://www.cencenelec.eu/about-cenelec/

CENELEC. 10.6.2021. *A major step for railways cybersecurity: the new CLC/TS 50701*. https://www.cencenelec.eu/news-and-events/news/2021/eninthespotlight/2021-06-10-new-clc-ts-50701-railways-cybersecurity/

Cimpanu, C. (9.7.2021). *Cyber-attack disrupts Iran's national railway system*. The Record. https://therecord.media/cyber-attack-disrupts-irans-national-railway-system/

Cluley, G. (28.4.2021). *Was the email account of Merseyrail's MD hacked to spread word of ransomware attack?*. https://grahamcluley.com/merseyrail-ransomware/

Cyble. (3.7.2020). *Netfilim ransomware operators.* https://blog.cyble.com/2020/06/30/stadler-rail-data-leak-part-2-being-published-by-the-netfilim-ransomware-operators/

Digirata. (n.d.). *Yhdessä kohti rautatieliikenteen Euroopan kärkeä!*. Haettu 4.5.2022 osoitteesta https://digirata.fi/

Digirata. (2.11.2021). *Digiradan pilottivaihe toteutetaan Tampere-Pori/Rauma-rataosuudella*. https://digirata.fi/digiradan-pilottivaihe-toteutetaan-tampere-pori-rauma-rataosuudella/

ENISA. (n.d.) *NIS Directive.* European Union Agency for Cybersecurity. Haettu 13.1.2022 osoitteesta https://www.enisa.europa.eu/topics/nis-directive

ENISA. (n.d.). *About ENISA.* European Union Agency for Cybersecurity. Haettu 28.9.2021 osoitteesta https://www.enisa.europa.eu/about-enisa

ENISA-ERA. (16.3.2021). *prTS 50701 overview - Scope - IT/OT* [kuva] https://www.enisa.europa.eu/events/ENISA-ERA_Conference/enisa-era-conference-slides/4-status-update-on-cenelec-wg-26-benoliel-schlehuber.pdf

ENISA-ERA. (16.3.2021). *Cybersecurity in Railways*. https://www.enisa.europa.eu/events/ENISA-ERA_Conference/enisa-era-conference-slides/4-status-update-on-cenelec-wg-26-benoliel-schlehuber.pdf

ERA. (n.d.). *ERA Knowledge Hub.* Haettu 28.9.2021 osoitteesta https://www.era.europa.eu/content/era-knowledge-hub_en

ERA-ENISA. (25.11.2021). *Managing Cybersecurity Risks in Railways* [webinaari] https://www.era.europa.eu/content/era-enisa-free-webinar-managing-cybersecurity-risks-railways_en

Euroopan komissio. (13.1.2021). Euroopan parlamentin ja neuvoston direktiivin 2012/34/EU 15 artiklan 4 kohdan mukainen seitsemäs kertomus rautatiemarkkinoiden kehityksen seurannasta. Euroopan komissio. https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52021DC0005&qid=1611835047038&from=FI

Euroopan komissio. (20.7.2021). *Liikenteen kyberturvallisuutta koskeva välineistö.* https://transport.ec.europa.eu/system/files/2021-10/cybersecurity-toolkit_fi.pdf

Euroopan parlamentin ja neuvoston asetus (EU) 216/679. (27.4.2016). https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=FI

Euroopan parlamentin ja neuvoston asetus 2016/679. https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=FI

Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680. (27.4.2016). EU https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016L0680&from=FI

Euroopan unioni. (n.d.). *Infografiikka – Suurimmat kyberuhat EU:ssa.* Haettu 15.9.2021 https://www.consilium.europa.eu/fi/infographics/cybersecurity-in-the-eu/

Fenniarail (n.d.). *Fenniarail Oy on tehokas tavaraliikenteen rautatieoperaattori*. Haettu 20.10.2021 osoitteesta https://www.fenniarail.fi/yhtio/

Fintraffic. (n.d.). *Fintraffic - Turvallista ja sujuvaa liikennettä.* Haettu 4.10.2021 osoitteesta https://www.fintraffic.fi/fi/fintraffic-0

Fintraffic Raide. (n.d.). *Fintraffic Raide - Turvallista ja ympäristöystävällistä rautatieliikennettä.* Haettu 4.10.2021 osoitteesta https://www.fintraffic.fi/fi/raide

F-Secure. (13.5.2017). *WannaCry – historian levinnein kiristyshaittaohjelma*. https://blog.f-secure.com/fi/wannacry-historian-levinnein-kiristyshaittaohjelma/

F-Secure. (n.d. -a). *Madot*. Haettu 19.12.2021 osoitteesta https://help.f-secure.com/product.html?home/anti-virus/latest/fi/concept_CF47E32B1E9E49ABAF8BBC156CD122B5-anti-virus-latest-fi

F-Secure. (n.d. -b). *Mikä on VPN?*. Haettu 3.4.2022 osoitteesta https://www.f-secure.com/fi/home/articles/what-is-a-vpn

F-Secure. (n.d. -c). *Rootkit*. Haettu 3.4.2022 osoitteesta https://www.f-secure.com/v-descs/rootkit.shtml

F-Secure. (n.d. -d). *Mitä ovat vakoiluohjelmat?*. Haettu 5.4.2022 osoitteesta https://www.f-secure.com/fi/home/articles/what-is-spyware

F-Secure. (n.d. -e). *Troijalaiset*. Haettu 3.4.2022 osoitteesta https://help.f-secure.com/product.html?home/anti-virus/latest/fi/concept_AD66CB676C2749B8A235B6D7E63BB4C2-anti-virus-latest-fi

Haworth, J. (24.7.2020). *Spanish state railway company Adif hit by REvil ransomware attack*. The Daily Swig - Cybersecurity news and views. https://portswigger.net/daily-swig/spanish-state-railway-company-adif-hit-by-revil-ransomware-attack

Hernández, L. (29.10.2020). *Two-factor authentication: what it is and how to enable it*. F-secure. https://blog.f-secure.com/two-factor-authentication-what-it-is-and-how-to-enable-it/

Huoltovarmuusorganisaatio. (n.d.). *Kyberympäristö ja kyberturvallisuus EI-kyberihmisille*. Haettu 15.11.2021 osoitteesta https://www.varmuudenvuoksi.fi/filebank/a/1416224994/ebe6ce40e87e4d1972490571a63ad0de/439-Kyber_esite_WEB.pdf

Impactmakers. (n.d.). *Analyze risks, define security requirements, ensure compliance*. Haettu 12.2.2022 osoitteesta https://www.impactmakers.com/security-risk/

Impactmakers. (n.d.). *Risk Management Framework* [kuva]. https://www.impactmakers.com/security-risk/

International Electrotechnical Commission. (26.2.2021). *Understanding IEC 62443*. https://www.iec.ch/blog/understanding-iec-62443

IRJ. (19.10.2020). *Keolis Commuter Services takes Boston systems offline following ransomware attack*. IRJ International Railway Journal. https://www.railjournal.com/technology/keolis-commuter-services-takes-boston-systems-offline-following-ransomware-attack/

ISO 27000 *Directory*. (n.d.) An Introduction To ISO 27001. Haettu 13.1.2022 osoitteesta http://www.27000.org/iso-27001.htm

J. Puro. 27.4.2017. *IT on kustannus, mutta digitalisaatio tarjoaa kilpailuetua!*. https://www.itewiki.fi/blog/2017/04/it-on-kustannus-mutta-digitalisaatio-tarjoaa-kilpailuetua/

Kaspersky. (n.d.). *Miten haittaohjelmista pääsee eroon?* Haettu 10.1.2022 osoitteesta https://www.kaspersky.fi/resource-center/threats/malware-protection

L.S. Vailshery. (17.3.2022). *Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030*. Statista. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

L.S. Vailshery. (17.3.2022). *Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030* [kuva]. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä 1054/2018. https://www.finlex.fi/fi/laki/alkup/2018/20181054

Laki sähköisen viestinnän palveluista 917/2014. https://www.finlex.fi/fi/laki/ajantasa/2014/20140917

Laki yksityisyyden suojasta työelämässä 759/2004. https://www.finlex.fi/fi/laki/ajantasa/2004/20040759

Liikenne ja viestintäministeriö. (2020). *CENELEC prTS 50701:2019 Railway Applications – Cybersecurity* [kuva]. LVM Kohti digitaalista ja älykästä rautatieliikennettä. http://urn.fi/URN:ISBN:978-952-243-589-7

Luottotietolaki 527/2007. https://www.finlex.fi/fi/laki/ajantasa/2007/20070527

LVM. (16.5.2012). *Ratarahti Oy:lle toimilupa rautateiden tavarakuljetuksiin*. Liikenne- ja viestintäministeriö. https://www.lvm.fi/-/ratarahti-oy-lle-toimilupa-rautateiden-tavarakuljetuksiin-732387

lähde 58.1 Partanen, A., Orkola, J. (2019). *Esineiden internet valtaa sinunkin kotis*i. https://www.traficom.fi/fi/tilastot-ja-julkaisut/blogit/iot-blogisarja

Lönnqvist, I. & Moilanen, P. (n.d.). *Kyberin taskutieto - Keskeisin kybermaailmasta jokaiselle*. Haettu 7.11.2021 osoitteesta https://jyx.jyu.fi/bitstream/handle/123456789/53510/978-951-39-7009-3.pdf

Microsoft. (8.3.2014). *Support for Windows XP ends in one month on April 8, 2014*. https://www.microsoft.com/security/blog/2014/03/08/support-for-windows-xp-ends-in-one-month-on-april-8-2014/

Microsoft. (n.d. -a). *Mitä kyberturvallisuus on?* Haettu 14.12.2021 osoitteesta https://support.microsoft.com/fi-fi/topic/mit%C3%A4-kyberturvallisuus-on-8b6efd59-41ff-4743-87c8-0850a352a390

Microsoft. (n.d. -b). *Virusten ja muiden haittaohjelmien estäminen ja poistaminen*. Haettu 3.4.2022 osoitteesta https://support.microsoft.com/fi-fi/topic/virusten-ja-muiden-

haittaohjelmien-est%C3%A4minen-ja-poistaminen-53dc9904-0baf-5150-6e9a-e6a8d6fa0cb5

Operail (n.d.). *About*. Haettu 21.10.2021 osoitteesta https://operail.com/en/about/

Palkeet. (11.2.2022). *Väylävirasto*. Valtion talous- ja henkilöstöhallinnon palvelukeskus. https://www.valtiolle.fi/fi-FI/Tyonantajat_ja_tyontekijat/Liikenne_ja_viestintaministerio/Vaylavirasto

Palkeet. (16.2.2022). *Liikenne- ja viestintäministeriö*. Valtion talous- ja henkilöstöhallinnon palvelukeskus. https://www.valtiolle.fi/fi-FI/Tyonantajat_ja_tyontekijat/Liikenne_ja_viestintaministerio

Pylvänäinen, J., Lehtola, J., Nieminen, T., Brotherus, M., Sandelin, E., Wallin, J. & Artukka, J. (2020). *Kohti digitaalista ja älykästä rautatieliikennettä – Digirata-selvityksen loppuraportti*. Liikenne- ja viestintäministeriö. http://urn.fi/URN:ISBN:978-952-243-589-7

Raideliikennelaki 1302/2018. https://www.finlex.fi/fi/laki/ajantasa/2018/20181302

Railway Technology. (8.5.2020*). Stadler IT systems attacked by malware*. https://www.railway-technology.com/news/stadler-it-systems-malware/

Railway Technology. (n.d.). *About Us*. Haettu 13.2.2022 osoitteesta https://www.railway-technology.com/about-us-online/

Rautatiealan Sääntelyelin. (15.5.2020). *Rautatiealan sääntelyelimen toiminta*. Haettu 10.10.2021 osoitteesta https://www.saantelyelin.fi/fi/rautatiealan-saantelyelimen-toiminta

Rikoslaki 39/1889. https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

Sainio, K. (18.3.2020). *Traficomin tavoitteet raideliikenteen kyberturvallisuudelle*. Liikenne- ja viestintävirasto Traficom. https://www.traficom.fi/sites/default/files/media/file/Trtaaficomin%20tavoitteet%20raideliikenteen%20kyberturvallisuudelle%20Kaisa%20Sainio.pdf

Sanastokeskus TSK ry. (2018). *Kyberturvallisuuden Sanasto*. Turvallisuuskomitea. https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

SESKO. (n.d.). *Sesko Ry.* Haettu 9.1.2022 osoitteesta https://sesko.fi/sesko_ry/

Sisäministeriö. (n.d.). *Maalittaminen rapauttaa yhteiskunnan luottamusta*. Haettu 14.12.2021 osoitteesta https://intermin.fi/poliisiasiat/viharikollisuus/maalittaminen

Suomen Riskienhallintayhdistys ry. (n.d.). *PK-RH-riskienhallinta*. Haettu 12.3. osoitteesta https://pk-rh.fi/riskien-luokittelu/vahinkoriskit.html

TEM. (n.d.). *Ydinvoimalaitoksilta tulee kolmannes Suomen sähköntuotannosta*. Työ- ja elinkeinoministeriö. Haettu 12.10.2021 osoitteesta https://tem.fi/ydinenergia

Tervonen, J. (2011). *Yksityisraiteet ja ratamaksusääntely*. Liikenne- ja viestintäministeriön julkaisuja 34/2011, s. 6. Liikenne- ja viestintäministeriö. http://urn.fi/URN:ISBN:978-952-243-273-5

Tietosuojalaki 1050/2018. https://www.finlex.fi/fi/laki/ajantasa/2018/20181050

Tietosuojavaltuutetun toimisto. (n.d.). *Usein kysyttyä EU:n tietosuoja-asetuksesta.* Haettu 27.10.2021 osoitteesta https://tietosuoja.fi/gdpr

TNW. (25.10.2019). *Apple and Google remove 50+ apps that served malicious ads.* The Next Web. Haettu 18.12.2021 osoitteesta https://thenextweb.com/news/apple-and-google-remove-50-malicious-apps-that-stole-your-data

Traficom. (13.6.2019). *Rautatiesektorin toimijat*. Haettu 3.10.2021 osoitteesta https://www.traficom.fi/fi/liikenne/raideliikenne/rautatiesektorin-toimijat

Traficom. (13.7.2021). *Raideliikenteen turvallisuusohjelma*. Haettu 29.9.2021 osoitteesta https://www.traficom.fi/fi/liikenne/raideliikenne/raideliikenteen-turvallisuusohjelma

Traficom. (17.10.2020). *Kybermittari Kansallinen kyberturvallisuuden arviointimalli - Käyttöohje.*

https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybermittari_K%C3%A4ytt%C3%B6ohje_V1.pdf

Traficom. (17.10.2020). *Kyberturvallisuuden arvioinnin viisivaiheinen prosessi* [kuva] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybermittari_K%C3%A4ytt%C3%B6ohje_V1.pdf

Traficom. (17.6.2019). *Rautatietoimijoiden turvallisuusjohtamisjärjestelmä*. Haettu 3.11.2021 osoitteesta https://www.traficom.fi/fi/liikenne/raideliikenne/rautatietoimijoiden-turvallisuusjohtamisjarjestelma

Traficom. (2/2020). *Kyberturvallisuus ja yrityksen hallituksen vastuu*. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

Traficom. (21.7.2021). *CERT-FI 20 vuotta: Oi, muistathan Heartbleedin ja NotPetyan!* https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/cert-fi-20-vuotta-oi-muistathan-heartbleedin-ja-notpetyan

Traficom. (29.6.2020). *Suositus kyberturvallisuuden edistämisestä raideliikenteessä.* Liikenne- ja viestintävirasto Traficom. https://www.traficom.fi/sites/default/files/media/regulation/Suositus%20kyberturvallisuuden%20edist%C3%A4misest%C3%A4%20raideliikenteess%C3%A4.pdf

Traficom. (7.6.2021). *Raideliikenteen kyberturvallisuuden työpaja 4.6.2021*. https://www.traficom.fi/fi/raideliikenteen-kyberturvallisuuden-tyopaja-462021

Traficom. (n.d.). *Toimintamme*. Haettu 11.10.2021 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/toimintamme

Traficom. 04.01.2021. *Rautatieliikenne*. Haettu 11.10.2021 osoitteesta https://liikennefakta.fi/fi/markkinat/henkilot-ja-tavarat/rautatieliikenne

Traficom. 11.2.2022. *Kybermittari*. Liikenne- ja viestintävirasto Traficom. https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/kybermittari

Traficom. 15.5.2020. *Valmiussuunnittelun järjestäminen iikennejärjestelmässä*. https://www.finlex.fi/data/normit/46012/TRAFICOM_308489_03_04_04_00_2019_FI_Valmiussuunnittelun_jarjestaminen_liikennejarjestelmassa.pdf

Turvallisuuskomitea. (3.10.2019). *Suomen kyberturvallisuusstrategia 2019*. Turvallisuuskomitea. https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia-2019/

Valtioneuvosto. (2.4.2020). *Kohti digitaalista ja älykästä rautatieliikennettä*. Valtioneuvosto ja ministeriöt. https://valtioneuvosto.fi/-/kohti-digitaalista-ja-alykasta-rautatieliikennetta

Väylävirasto. (n.d. -a). *Digirata*. Haettu 30.10.2021 osoitteesta https://vayla.fi/digirata

Väylävirasto. (n.d. -b). *Yksityisraiteet*. Haettu 30.10.2021 osoitteesta https://vayla.fi/vaylista/rataverkko/yksityisraiteet

Väylävirasto. (8.11.2021) *Rataverkko*. https://vayla.fi/vaylista/rataverkko

Liite 1: Haastattelukysymykset

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

HAASTATTELUKYSYMYKSET 1 (4)

3.11.2021

Raideliikenteen kyberturvallisuus

Nämä haastattelukysymykset toimivat aineistona opinnäytetyölle, jonka aiheena on raideliikenteen kyberturvallisuus. Tarkoituksena on selvittää kyberturvallisuuteen varautumiseen tarkoitettujen välineiden välineiden tuntemusta ja hyödyntämistä yrityksen toiminnassa.

Haastateltavan tiedot

- Esittely
- Tehtävät yrityksessä

Yrityksen tiedot

- Nimi
- Paikkakunta
- Henkilömäärä
- Historia lyhyesti
- Keskeisin toiminta
- Asiakkaiden toimiala
- Toimialue, sijainti

Kyberturvallisuuden tehtävät

- Onko nimettyä tietoturva- ja/tai tietosuojavastaavaa?
- Onko kyberturvallisuudelle nimetty vastaavaa?
- Kuuluuko kyberturvallisuus yrityksen riskienhallintaan?
- Koulutetaanko yrityksen työntekijöitä kyberturvallisuuden osalta?
- Onko yrityksellänne tarve tai aikomus palkata kyberturvallisuuden asiantuntija/ -joita?
- Oletteko kartoittaneet tarvetta kyberturvallisuuteen liittyvään koulutukseen?

Tietoturvan ja kyberturvallisuuden nykytila

- Onko yritykseenne kohdistunut tai kyberhyökkäystä tai havaittu tietoturvaongelmia?
- Onko yrityksenne kärsinyt kyberhyökkäyksestä sivullisena osapuolena?
- Ovatko yrityksenne johto sekä työntekijät tietoisia mahdollisista kyberuhkista?
- Onko yrityksenne osallistunut poikkeusttilanteiden tai kyberhyökkäyksen osalta harjoituksiin?
- Onko yrityksessänne määritelty toimintatavat ilmenneen kyberhyökkäyksen yhteydessä ja tilanteesta toipumiseen?

Kyberturvallisuuden työvälineet

EU Cybersecurity toolkit

- Oletteko tietoisia EU:n j ulkaisemasta Cybersecurity toolkit -arvioinnin työvälineestä?
- Pystyttekö osoittamaan, että yrityksessänne on huolehdittu palautumissuunnitelmasta, mikäli seuraavista kyberuhkista toteutuu tai toteutuu osittain (suojaudu haittaohjelmilta, auta tunnistamaan palvelunestohyökkäykset, suojaa data/tiedot luvattomilta pääsyiltä ja varkauksilta, tiedosta mahdollisuus ohjelmistojen manipulointiin)
- Oletteko tarvinneet tukea EU Cybersecurity toolkit:in sisällön läpikäyntiin ja soveltamisessa yrityksen toimintaan?
- Onko yrityksessänne ennalta varmistettu käytännöt ylimmän johdon kyberturvallisuuden raportoimisesta johtajille ja hallituksen jäsenille?
- Onko yrityksessänne huolehdittu, että kyberturvallisuudesta sekä fyysisestä turvallisuudesta vastaavan henkilön johtamisvastuut ovat selvät?
- Ovatko kyberturvallisuuteen liittyvät roolivastuut määritelty selkeästi ja osoitettu vastuuhenkilöille?
- Ovatko kyberturvallisuusriskien ja uhkien hallinnan toimien ja ohjaamisen vastuut jaettu ja varmistettu, että ne ovat voimassa koko sopimuksen elinkaaren ajan?

- Ovatko tarvittavat riskienhallinnan toimenpiteet tunnistettu ja niiden myötä suunnitelmat toteutettu kyberturvallisuusriskien vähentämiseksi?
- Tekeekö yritys säännöllisesti kyberturvallisuusriskien arviointeja, joissa huomioidaan uusimmat uhat sekä tunnetut haavoittuvuudet. Lisäksi arvioinneissa huomioidaan toimintaa tukevien järjestelmien (maksujärjestelmät, kirjanpito, verkko, turvajärjestelmät) lisäksi myös yrityksen varsinaisen toiminnan järjestelmät, jotka liittyvät kalustoon, liikenteen hallintaan ja ohjaukseen yms.

Traficomin suositus

- Tunnetteko Traficomin julkaiseman julkaisun ”Suositus kyberturvallisuuden edistämisestä raideliikenteessä”?
- Onko yrityksessänne osoitettu suosituksen toimien edistäminen jonkun henkilön vastuualueelle?
- Onko yrityksessänne suosituksen voimaantulon 1.7.2020 jälkeen käynnistetty ja ylläpidetty edistämisen toimenpiteitä?
- Oletteko tarvinneet tukea sisällön läpikäyntiin ja suosituksen sovittamiseen yrityksenne toimintaan?

Kybermittari

- Onko Traficomin Kyberturvallisuuskeskuksen julkaisema Kybermittari teille tuttu kyberturvallisuuden arvioinnin työkalu?
- Onko yrityksestänne tunnistettavissa henkilö, jonka vastuualueella tai muuten tarvittava osaaminen Kybermittarin eri osa-alueista (Kriittisten palveluiden suojaaminen, Riskienhallinta, Toimitusketjun ja ulkoisten riippuvuuksien hallinta, Omaisuuden muutoksen ja konfiguraation hallinta, Identiteetin- ja pääsynhallinta, Uhkien ja haavoittuvuuksien hallinta, Tilannekuva, Tapahtumien ja häiriötilanteiden hallinta, Henkilöstön hallinta, Kyberturvallisuusarkkitehtuuri, Kyberturvallisuusohjelma)?

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

3.11.2021

- Oletteko käyttäneet Traficomin Kybermittaria oman toimintanne arvioimiseen ja kehitystarpeiden kartoittamiseen?
- Oletteko tarvinneet Kybermittarin käyttöön tukea? Ja onko käytössä avustanut Traficomin Kyberturvallisuuskeskus vai jokin muu ulkopuolinen taho?
- Oletteko hyödyntäneet mittaustulosten jakamista vertailutietojen kartuttamiseksi?
- Onko yrityksenne osallistunut tai kiinnostunut osallistumaan Traficomin Kyberturvallisuuskeskuksen järjestämiin Kybermittari-tilaisuuksiin organisaation, palveluntarjoajan tai teknisen käytön rooleissa?