Antopäivä:	Voimaantulopäivä:	Voimassa:
29.6.2020	1.7.2020	toistaiseksi

Lainsäädäntö, johon ohje perustuu:

Muutostiedot:

SUOSITUS KYBERTURVALLISUUDEN EDISTÄMISESTÄ RAIDELIIKENTEESSÄ

Sisällys

1. Suosituksen tarkoitus ja soveltamisala

Tällä suosituksella on tarkoitus edistää raideliikenteen kyberturvallisuuden kokonaisvaltaista kehittämistä ja toiminnan jatkuvuuden varmistamista. Tarkoituksena on lisätä:

- raideliikenteen toimijoiden tietoisuutta kyberturvallisuudesta,
- raideliikenteen toimijoiden kyberturvallisuusriskien ja kyberturvallisuushyökkäysten ymmärrystä,
- raideliikenteen toimijoiden varautumista ja vastuullista suojautumista omaan toimintaansa kohdistuvia kyberuhkia vastaan riskienhallinnan avulla ja
- raideliikenteen toimijoiden yhteistyötä, jotta raideliikenteen ja sen järjestelmien kokonaissuojauksen tasoa saadaan nostettua

Tarkoituksena on edistää rautatiejärjestelmän ja kaupunkiraideliikenteen järjestelmien toimintaan osallistuvien organisaatioiden ja viranomaisten kykyä havaita ja tunnistaa erilaisia raideliikenteeseen vaikuttavia kyberturvallisuustapahtumia sekä suojautua niitä vastaan ja palautua niistä mahdollisimman nopeasti.

Suositus jakaantuu kahteen eri osaan. Luvut 1-3 toimivat johdanto-osana. Johdanto-osan tarkoituksena on sekä johdattaa lukija kyberturvallisuuden edistämiseen, että havainnollistaa lukijalle raideliikenteen kyberturvallisuusuhkien monimuotoisuutta. Luvussa 4 esitetään Liikenne- ja viestintäviraston suositukset raideliikenteen toimijoille kyberturvallisuusuhkiin varautumisen sekä kyberturvallisuusriskien hallitsemisen toimenpiteistä.

Koska raideliikenteessä toimii lukuisia erilaisia organisaatioita, suositus ei anna yksiselitteisiä vastauksia siitä, minkälaisiin konkreettisiin toimiin raideliikenteen toimijoiden tulisi kyberturvallisuutensa kehittämiseksi ryhtyä. Suosituksen on tarkoitus toimia konkreettisena apuvälineenä kyberturvallisuuden kehittämisessä. Näin ollen se, miten kukin toimija vastaa luvussa 4 annettuihin suosituksiin, riippuu sekä toimijan toiminnan laadusta ja laajuudesta, että toimijan jo tekemistä toimenpiteistä kyberturvallisuuden kehittämiseksi. Ensisijaisen tärkeää onkin, että kukin raideliikenteen toimija työstää annettuja suosituksia pitäen mielessä oman toimintansa ja toimintaympäristönsä.

Suositus on suunnattu sekä rautatiejärjestelmälle että kaupunkiraideliikenteen järjestelmille. Suositus on pääosin kirjoitettu rautatiejärjestelmää ajatellen, mutta suosituksessa läpikäytävät kyberturvallisuuden käsitteet, haasteet ja hallinnan keinot ovat hyvin sovellettavissa myös kaupunkiraideliikenteeseen. Suosituksen erilaiset esimerkit pohjautuvat pitkälti rautatiejärjestelmään, mutta esimerkit auttavat kyberturvallisuuden hahmottamisessa myös kaupunkiraideliikenteen järjestelmissä.

Suositus on laadittu virkatyönä Liikenne- ja viestintävirastossa ja sen valmistelussa on kuultu raideliikenteen toimijoita. Suositusta päivitetään tarvittaessa.

2. Kyberturvallisuuden käsitteet

Tieto- ja kyberturvallisuutta koskevat termit määritellään varsin kattavasti puolustusministeriön yhteydessä toimivan Turvallisuuskomitean kyberturvallisuussanastossa. Tässä suosituksessa käytetään selkeyden vuoksi pääsääntöisesti termiä kyberturvallisuus, vaikka joissakin kohdissa voisi olla tarkoituksenmukaista viitata tietoturvallisuuteen.[1]

Termi	Määritelmä
Haavoittuvuus	Haavoittuvuus voi olla mikä tahansa heikkous, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamisessa. Haavoittuvuuksia voi olla operatiivisissa järjestelmissä, informaatiojärjestelmissä, prosesseissa ja ihmisen toiminnassa. Haavoittuvuudet voivat johtua esimerkiksi prosesseista, arkkitehtuurista tai suunnittelusta, konfiguraatioista ja ylläpidosta, fyysisestä tunkeutumisesta, järjestelmän ohjelmisto- ja tuotekehityksestä, viestinnästä ja tietoverkoista, harjoittelun ja tietoisuuden puutteesta.
Kyberriski	Kyberriski on todennäköisyys sille, että uhka hyödyntää haavoittuvuutta sekä niitä vaikutuksia, joita tämä haitallinen tapahtuma toteutuessaan organisaatiolle aiheuttaa.
Kybertoimintaympäristö	Kybertoimintaympäristö on yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuva toimintaympäristö. Kybertoimintaympäristölle on tunnusomaista datan ja informaation varastointi, muokkaaminen ja siirto viestintäverkkojen avulla. Raideliikenteen kyberturvallisuusympäristölle on lisäksi tunnusomaista operatiivisten järjestelmien avulla tapahtuva laitteiden ohjaus. Ympäristöön kuuluvat myös datan ja informaation käsittelyyn liittyvät fyysiset rakenteet
Kyberturvallisuus	Kyberturvallisuus on tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kyberturvallisuuteen kuuluvat toimenpiteet, joilla voidaan ennakoivasti hallita ja tarvittaessa sietää erilaisia kyberuhkia ja niiden vaikutuksia. Kybertoimintaympäristön toiminnan häiriytyminen aiheutuu usein toteutuneesta tietoturvauhkasta, joten kyberturvallisuuteen pyrittäessä tietoturva on keskeinen tekijä. Tietoturvan lisäksi kyberturvallisuuteen pyritään muun muassa toimenpiteillä, joiden tarkoituksena on turvata häiriytyneestä kybertoimintaympäristöstä riippuvaiset fyysisen maailman toiminnot. Siinä missä tietoturvalla tarkoitetaan tiedon saatavuutta, eheyttä ja luottamuksellisuutta, kyberturvallisuus tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin.
Kyberuhka	Kyberuhka on mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku, joka kohdistuu kybertoimintaympäristöön ja toteutuessaan vaarantaa siitä riippuvaisen toiminnon. Kyberuhkat voivat aiheutua paitsi toteutuneista tietoturvauhkista myös digitaalisessa viestintäympäristössä tai operatiivisissa järjestelmissä toteutettavista, yhteiskunnan turvallisuutta vaarantavista teoista. Kyberuhkat voivat olla peräisin maan rajojen sisältä tai niiden ulkopuolelta.
Tietoturvallisuus	Tietoturvallisuudella tarkoitetaan järjestelyjä, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus. Saatavuus tarkoittaa, että tieto on hyödynnettävissä haluttuna aikana. Eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja luottamuksellisuus sitä, ettei kukaan sivullinen saa tietoa. Tietoturvan järjestelyjä ovat esimerkiksi kulunvalvonta, tilojen lukitus, asiakirjojen turvallinen säilytys ja hävitys, tietojen salaus ja varmuuskopiointi sekä palomuurin, virustorjuntaohjelman ja varmenteiden käyttö. Tietoturvaan kuuluu muun muassa tietoaineistojen, laitteistojen, ohjelmistojen, tietoliikenteen ja toiminnan turvaaminen. Tietoturvalla ja tietoturvallisuudella voidaan tarkoittaa myös oloja, joissa tietoturvariskit ovat hallinnassa.

Taulukko 1 Keskeiset suosituksessa käytettävät määritelmät

[1] Taulukon 1 määritelmät ovat pääosin Turvallisuuskomitean kyberturvallisuussanastosta, mutta osaa niistä on täydennetty UK:n raideliikenteen kyberturvallisuusstrategiassa käytetyillä määritelmillä sekä muokattu raideliikenteeseen soveltuvammaksi (ks. luku 5. Lisätietoja ja tiedon lähteitä)

3. Kyberturvallisuus raideliikenteessä

Eurooppalaisen rautatiejärjestelmän yhtenäistymisen ja digitalisoitumisen myötä järjestelmästä on tullut harmonisoidumpi ja avoimempi sekä näin ollen haavoittuvampi. Tämä on johtanut kyberturvallisuusriskien kasvuun raideliikenteessä. Raideliikenteen tehokkuuden parantaminen nojaa vahvasti digitalisaatioon ja tulevaisuuden digitalisaatiotavoitteiden mahdollistamien hyötyjen saavuttaminen edellyttää vahvaa kyberturvallisuuden peruskiveä.

Myös maantieteellisesti selvästi rajoittuneemmat kaupunkiraideliikennejärjestelmät voivat joutua kyberturvallisuushyökkäysten kohteeksi. Siitä huolimatta, että hyökkäysten seuraamukset ovat kaupunkiraideliikenteessä maantieteellisesti rajatumpia, niillä voi olla silti merkittäviä negatiivisia vaikutuksia järjestelmien toimintaan ja kaupunkiraideliikenteen turvallisuuteen.

Raideliikenteessäkin kyberriskit voivat realisoitua monin eri tavoin. Kyberturvallisuusriski voi realisoitua tahottomasti, mutta myös tarkoituksellisesti, jolloin sen toteuttajina voivat olla yksittäiset ihmiset, organisaatiot tai jopa vieraat valtiot. Organisaatio voi joutua nimenomaisesti sitä kohtaan kohdennetun kyberturvallisuushyökkäyksen kohteeksi. Organisaatio voi joutua myös kohdentamattoman kyberturvallisuushyökkäyksen kohteeksi esimerkiksi siksi, että sen järjestelmässä on helposti havaittavissa ja hyödynnettävissä oleva haavoittuvuus. Kohdentamattomia hyökkäyksiä tiedetään tapahtuvan useammin kuin kohdennettuja hyökkäyksiä ja kohdentamatonkin hyökkäys voi olla organisaation toiminnalle vahingollinen. Kyberturvallisuusuhkan lähteenä, eli vahingoittamista tavoittelevana tahona, voi myös toimia eri taho kuin itse kyberturvallisuushyökkäyksen toteuttajana. Toteuttajia voi löytyä niin organisaatioiden sisältä, kilpailijoiden tai alihankkijoiden joukosta kuin rikollisten, terroristen tai hakkerienkin joukosta.

Toteutuneilla kyberturvallisuushyökkäyksillä voi olla merkittäviä negatiivisia vaikutuksia raideliikenteeseen. Todennäköistä on, että kyberturvallisuushyökkäykset johtavat toiminnan häiriintymiseen, lisätyöhön ja mainekolauksiin, mutta ne voivat johtaa myös vaaratilanteisiin ja jopa onnettomuuksiin. Tässä suosituksessa kyberturvallisuutta käsitelläänkin erityisesti turvallisuuden kannalta ja turvallisuuden kannalta kriittisten järjestelmien osalta.

Koska rautatiejärjestelmä on kasvavassa määrin yksi yhteinen järjestelmä, toteutunut kyberturvallisuushyökkäys voi johtaa jopa koko järjestelmän ja valtion rataverkon kattaviin häiriöihin. Vastaavasti on mahdollista, että kyberturvallisuushyökkäys lamaannuttaa esimerkiksi metroliikennejärjestelmän toimimisen kokonaisuudessaan. Näin ollen kyberturvallisuutta pitää edistää järjestelmälähtöisesti ja yhdessä – vain näin voidaan estää tilanne, jossa koko järjestelmä kärsii sen yhden osa-alueen haavoittuvuudesta.

Kyberturvallisuuden edistämisessä on keskeistä ymmärtää, että kyberturvallisuus on osa raideliikennejärjestelmän turvallisuutta eikä kyberturvallisuutta tule kokea tai käsitellä erillisenä kokonaisuutena.

Siitä huolimatta, että kyberturvallisuutta ei vielä säädellä kattavasti EU-sääntelyssä tai huomioida esimerkiksi turvallisuusjohtamisjärjestelmän sisältöä ohjaavissa arviointikriteereissä, kyberturvallisuuden sisällyttäminen toimijan turvallisuusjohtamisjärjestelmään tai turvallisuuden hallintajärjestelmään on suositeltavaa ja edistää toimijan kokonaisturvallisuuden johtamista ja hallintaa.

3.1. Raideliikenteen kyberturvallisuussääntely

Raideliikenteen kyberturvallisuussääntely on vasta kehittymässä. Raideliikennelain (1302/

2018) 169 § sisältää säännökset velvollisuudesta huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja tietoturvallisuuteen liittyvästä häiriöstä ilmoittamisesta. Säännös kohdistuu toistaiseksi vain valtion rataverkon haltijaan sekä liikenteenohjauspalvelun tarjoajaan. Sen taustalla on ns. NIS-direktiivi (EU:n verkko- ja tietoturvadirektiivi, (EU) 2016/1148).

Raideliikennelaki sisältää myös yleisemmän velvoitteen ilmoittaa tilannekuvan muodostamiseksi tarvittavista tiedoista. 172 § kohdistuu sekä rautatieliikenteen harjoittajiin, rataverkon haltijoihin, liikenteenohjauspalvelua tarjoavaan yhtiöön sekä kaupunkiraideliikenteen rataverkon liikenteenohjauksesta vastaavaan toimijaan, joiden on ilmoitettava Traficomille viipymättä sellaisista niiden tietoon tulleista tapahtumista, jotka voivat vaikuttaa tilannekuvan muodostamiseen. Traficomin on tarkoitus ohjeistaa pykälän mukaista toimintaa vielä kuluvan vuoden aikana. Pykälän voidaan katsoa sisältävän myös kyberturvallisuusuhkista ja -häiriöistä ilmoittamisvelvollisuuden.

Raideliikennelain lisäksi kyberturvallisuus huomioidaan myös Traficomin määräyksessä valmiussuunnitelman järjestämisestä (TRAFICOM/308489/03.04.04.00/2019). Määräys edellyttää, että rataverkon haltija kuvaa valmiussuunnitelmassaan kybertoimintaympäristönsä ja kohdistuu tältä osin sekä valtion rataverkon haltijaan, että yksityisraiteen haltijoihin. Lisäksi valtion rataverkon haltijan ja sen liikenteenohjauspalvelua tarjoavan toimijan tulee huomioida kybertoimintaympäristöä uhkaavat tapahtumat ja uhkat kuvatessaan menettelyitä, joilla se varmistaa rautatieliikenteen hoidon varautumisen eri tavoitetasoilla. Määräys tulee sovellettavaksi siirtymäajan jälkeen 1.6.2021.

EU-sääntelyä raideliikenteen kyberturvallisuudesta ei edellä mainittua NIS-direktiiviä lukuunottamatta vielä juuri ole. Eri toimijat ovat kuitenkin yrittäneet laatia kyberturvallisuudesta ohjeistuksia, menettelytapoja ja työkaluja. Yksi konsortioista on EU:n rahoittama Shift 2 Rail (S2R), jossa kyberturvallisuutta pyritään huomioimaan ja ohjeistamaan mm. CYRAIL-projektissa, joka on osa EUn HORIZON 2020-tutkimus- ja innovaatio-ohjelmaa.

Myös Euroopan rautatievirasto on jo käynnistänyt toimia, joita tarvitaan kyberturvallisuuden sääntelemiseksi rautatiesektorilla. Työ kohdistuu ensimmäiseksi Euroopan rautatieliikenteen ohjausjärjestelmän ERTMS (European Rail Traffic Management System) kolmannen tason (L3) kehittämiseen. Työssä huomioidaan myös Shif 2 Rail -konsortion projekteissa saadut tulokset. Euroopan Rautatieviraston on tarkoitus sisällyttää kyberturvallisuus jatkossa kattavammin eurooppalaisen raideliikennesääntelyn kehykseen ja huomioida työssä mm. CENELECIN WG 26:n työstämä standardi TS 50701, joka on tarkoitus antaa vuoden 2021 aikana.

Kyberturvallisuuden merkityksen korostuminen raideliikenteen EU-sääntelyssä tullee lähivuosina vaikuttamaan rautatiejärjestelmää koskevien kyberturvallisuuskysymyksien käsittelyyn. Kaupunkiraideliikenteen osalta vastaavia muutoksia ei sen sijaan ole odotettavissa, mistä johtuen kaupunkiraideliikennejärjestelmän kyberturvallisuuskysymysten käsittely säilynee jatkossakin kansallisen ohjauksen piirissä.

3.2. Raideliikenteen kyberturvallisuusuhkat ja -riskit

Kyberturvallisuudessa tärkeintä on kyberturvallisuusriskien ja -uhkien hallinta. Haavoittuvuuksia ja niiden vaikutuksia voidaan hallita ja vähentää tunnistamalla ja korjaamalla. Haavoittuvuuden olemassaolo ei kuitenkaan automaattisesti johda vahinkoon vaan vahinkoa syntyy vasta, kun haavoittuvuutta hyväksikäyttävä uhka toteutuu. Jos haavoittuvuuteen ei liity uhkaa hyväksikäytöstä, se ei välttämättä edellytä hallintakeinon toteuttamista, mutta se olisi silti tunnistettava ja sen tilannetta seurattava mahdollisten muutosten varalta. Uhkia puolestaan voidaan torjua ja seurata, mutta ei juuri käsitellä muilla tavoin. Riskejä sen sijaan voidaan käsitellä riskienhallinnan metodein.

Kyberriskien hallinnalla tarkoitetaankin riskien tunnistamista ja arviointia, sekä riskien käsittelyä varten tehtävää vaihtoehtojen valintaa, kehittämistä ja toteuttamista. Riskienhallinta koskee kaikkia organisaatiota koskevia mahdollisia riskejä ja niihin reagointia. Kyberturvallisuusriskit kuuluvat osana riskienhallinnan kokonaisuuteen. Riskienhallinta kokonaisuutena on systemaattinen ja jatkuva ajatteluprosessi, joka heijastaa organisaation arvoja ja koostuu tunnistamisen, käsittelyn ja arvioinnin lisäksi jatkuvasta koordinoinnista, riskien kehittymisen tutkimisesta, riskien uudelleen arvioinnista, korjaavista toimenpiteistä, viestinnästä sekä raportoinnista. Kyberriskeissä korostuu erityisesti riskienhallinnan näkökulmasta ajattomuus, tilattomuus ja vahingonkorvausten laskettavuuden vaikeus.

Kyberriskit voidaan jakaa neljään pääluokkaan, joita ovat ihmisten toiminta, järjestelmähäiriöt ja tekniset viat, epäonnistuneet sisäiset prosessit sekä ulkoiset tapahtumat. Pääluokat puolestaan voidaan jakaa alaluokkiin, jotka havainnollistavat riskejä aiheuttavia operationaalisista toimia. Kyberriskien kokonaisuuden kannalta on tärkeää huomioida, että kyberriskit korreloivat usein keskenään ja yksi riski voit toteutuessaan aiheuttaa tapahtumasarjan, joka laukaisee useampia riskejä.[2]

1. Ihmisten toiminta	**2. Järjestelmähäiriöt ja viat**	**3. Epäonnistuneet sisäiset toiminnot**	**4. Ulkoiset tapahtumat**
1.1. Tahattomuus Vahingot Virheet Laiminlyönnit	**2.1. Laitteistot** Kapasiteetti Suorituskyky Huolto Vanhentuneisuus	**3.1. Toiminnon suunnittelu ja toteutus** Toiminnon kulku Toiminnon dokumentointi Roolit ja vastuut Ilmoitukset ja hälytykset Tiedon kulku Ongelmien kasvaminen Palvelutasosopimukset Tehtäviensiirto	**4.1. Katastrofit** Sääilmiöt Tulipalot Tulvat Maanjäristykset Levottomuudet Onnettomuudet Pandemiat
1.2. Tahallisuus Petokset Sabotoinnit Varkaudet Vandalismi	**2.2. Ohjelmisto** Yhteensopivuus Konfiguroinnin hallinta Muutostenhallinta Turvallisuusasetukset Ohjelmointikäytännöt Testaus	**3.2. Toiminnan valvonta** Toimintaympäristön valvonta Mittarit Säännöllinen omavalvonta Toiminnan omistajuus	**4.2. Lainsäädännölliset ongelmat** Sääntelyn noudattaminen Sääntelyn toimivuus Oikeudenkäynnit
1.3. Toimettomuus	**2.3. Järjestelmät**	**3.3. Tukitoiminnot**	**4.3. Liiketoiminnan ongelmat**

[2] Taulukko pohjautuu Cebula & Youngin (2010) operationaalisten kyberriskien taulukkoon.

Taidot Tiedot Ohjaus Saatavuus	Suunnittelu Tekniset vaatimukset Integraatio Monimutkaisuus	Henkilöstöhallinta Rahoitus Kehitys- ja koulutustoiminta Hankinta	Alihankkijan häiriöt Markkinaolosuhteet Taloudellinen tilanne
			4.4. Riippuvaisuussuhteet Sähkö-, vesi- ja tietoliikenneverkot Pelastustoimi Varavoima Kuljetus

Taulukko 2. Raideliikenteen kyberriskien jakautuminen pääluokkiin. Perustuu Cebula & Youngin 2010 teokseen.

Kyberriskit voidaan nähdä laajemmin informaatiota ja teknologiaa koskevina operationaalisina riskeinä, jotka vaikuttavat tiedon tai järjestelmän luottamuksellisuuteen, saatavuuteen tai eheyteen. Kyberriskin katsotaankin kattavan kaikki ne riskit, jotka johtavat taloudelliseen menetykseen, toiminnan keskeytymiseen tai organisaation maineen vahingoittumiseen tai organisaation konkreettiseen toimintaan. Kyberriskin toteutuessa voivat vahingot olla pahimmassa tapauksessa taloudellisesti ja inhimillisesti mittavat.

Raideliikenteen kybertoimintaympäristö koostuu sekä rautatiejärjestelmän että kaupunkiraideliikennejärjestelmän osalta kahdesta erillisestä kokonaisuudesta: informaatiojärjestelmistä ja operatiivisista järjestelmistä. Informaatiojärjestelmiä ja operatiivisia järjestelmiä liitetään yhä enenevissä määrin toisiinsa ja tämä aiheuttaa uusia vaatimuksia kyberriskien hallintaan. Perinteisesti kyberturvallisuus on otettu kattavammin huomioon informaatiojärjestelmissä ja kyberturvallisuuskysymyksiin on herätty enenevässä määrin operatiivisissa järjestelmissä vasta viime vuosina.

Raideliikenteelle ominaista on käytettävien järjestelmien pitkä ikä ja osin myös järjestelmien ikääntyminen. Osia järjestelmistä on käytetty vuosikymmeniä ja osia paranneltu matkan varrella, mikä tekee järjestelmistä kyberturvallisuuden kannalta sekä haastavia että haavoittuvia. Kyberturvallisuuden huomioinnin hidas lisääntyminen operatiivisella puolella ja maantieteellinen hajaantuneisuus lisäävät raideliikenteen alttiutta kyberuhkille. Kyberriskien hallinnassa keskeistä on kehittää informaatiojärjestelmien ja operatiivisten järjestelmien toimijoiden yhteistyötä. Lisäksi tärkeää on kiinnittää huomioita järjestelmien suojaamiseen, järjestelmiin kuuluvan tiedon ja datan suojaamiseen sekä järjestelmien sisäisen ja niiden välisen tietoliikenteen turvallisuudesta huolehtimiseen.

Toimintaympäristö	Ominaispiirteet	Esimerkit
Operatiiviset järjestelmät (OT, *operational technology*)	Operatiiviset järjestelmät, joilla hallitaan liikenneverkkoinfrastruktuuria ja liikkuvaa kalustoa, kuten liikennöintiä, merkinantoa, voimanlähteitä, viestintää ja asemien hallintaa.	ERTMS, JKV, kauko-ohjaus, asetinlaitteet, sähkörata ja sen ohjausjärjestelmät, operatiivisten järjestelmien virransyöttö, kuumakäynti- ja lovipyöräilmaisinjärjestelmät
Informaatiojärjestelmät (IT, *information technology*)	Liiketoimintaa tukevat IT-järjestelmät sekä IT-järjestelmät, jotka tukevat operatiivisia järjestelmiä ja tarjoavat liittymän operatiivisiin järjestelmiin.	Matkustajainformaatio, kuljettajan päätelaitesovellukset, kuljetusten seurantajärjestelmät, liikenteenohjauksen hallintajärjestelmät, yleisesti käytössä olevat tiedonsiirtotavat (esim. WLAN-verkko) sekä tieto- ja viestintäjärjestelmät

Taulukko 3. Raideliikenteen toimintaympäristön OT:t ja IT:t

Kyberturvallisuusriskien hallinnan tekee haastavaksi se, että raideliikenteen toimintojen ja järjestelmien kehittyessä ja digitalisoituessa kyberturvallisuusriskien määrä kasvaa ja riskit monipuolistuvat. Digitaalisen maailman täydellinen turvaaminen sen sijaan on mahdotonta, mistä johtuen myös esimerkiksi organisaation kypsyyteen havaita kyberturvallisuusuhkia tulee kiinnittää huomiota.

Kyberuhkien tunnistamiseen ja torjumiseen tulee kiinnittää huomiota sekä olemassa olevia järjestelmiä päivitettäessä, että uusissa hankkeissa aina suunnitteluvaiheesta alkaen. Tilaaja- ja toimijaorganisaatioilla on suuri vastuu kyberturvallisuuden toteuttamisessa ja erityisesti ennen muutettujen tai uusien järjestelmien käyttöönottoa on tärkeää todeta, että järjestelmät ovat myös kyberturvallisia ja niiden käyttäjillä on olemassa menettelyt kyberturvallisuudesta huolehtimiseen järjestelmien koko elinkaaren ajan. Koska raideliikenteessä monet hankintasopimukset ovat pitkiä ja niistä monet on laadittu aikana, jolloin kyberturvallisuuskysymykset eivät olleet keskiössä, kyberturvallisuusvaatimukset on tärkeää huomioida myös vanhoja sopimuksia päivitettäessä tai uusittaessa.

3.2. Esimerkkejä kyberturvallisuusuhkista ja niiden hallinnan keinoista

Seuraavassa taulukossa on kuvattu erilaisia kyberuhkia, jotka voivat kohdistua raideliikenteeseen ja jotka tulisi huomioida raideliikenteen toimijoiden riskienhallinnassa. Taulukossa mainitut kyberuhkat ovat kuitenkin vain esimerkkejä ja kunkin raideliikenteen toimijan tulee arvioida itsenäisesti nimenomaan omaan toimintaansa liittyvät kyberuhkat ja ne kriittiset järjestelmät, jotka tulee kyberturvallisuuden kehittämisessä huomioida.

Kyberuhka	Esimerkkejä	Toimijat, joihin kohdistuu
Tietokoneasetinlaitteisiin liittyvät riskit	Tiedonsiirto liikenteenohjauksesta katkeaa eivätkä komennot välity tietokoneasetinlaitteille toivotulla tavalla esimerkiksi ratatöiden aiheuttamasta kaapelin katkeamisesta johtuen.	Liikenteenohjaus, rataverkon haltija, rautatieliikenteen harjoittajat
Liikenteenohjausjärjestelmien ja asetinlaitteiden väliset rajapintariskit	Tiedonsiirtokatkos tai -häiriö tietokoneiden ja niillä ohjattavien releasetinlaitteiden välillä.	Liikenteenohjaus, rataverkon haltija, rautatieliikenteen harjoittajat
Liikenteenohjausjärjestelmien ja tietokoneasetinlaitteiden väliset rajapintariskit	Liikenteenohjaajan käyttämän kauko-ohjausjärjestelmän komennot eivät välity oikein tietokoneasetinlaitteeseen.	Liikenteenohjaus, rataverkon haltija, rautatieliikenteen harjoittajat
Liikenteenohjausjärjestelmien tiedon eheyteen ja luotettavuuteen liittyvät riskit	Käytettävä tietosisältö murenee esimerkiksi hakkerin toimista johtuen siten, että järjestelmien tietoon ei voida luottaa tai sitä ei voida hyödyntää.	Liikenteenohjaus, rataverkon haltija, rautatieliikenteen harjoittajat
Lähdekoodiin perustuvien liikenteenhallintajärjestelmien riskit	Lähdekoodiin laitetaan haitallinen koodi, joka tulee sisään liikenteenhallintajärjestelmään ja aktivoituu	Liikenteenohjaus, rataverkon haltija, rautatieliikenteen harjoittajat

	järjestelmässä esimerkiksi sen päivityksen yhteydessä.	
Liikenteen ohjausjärjestelmien yleiseen verkkoon liittymisen riskit	Yleisen verkon kautta tehdään tahallisesti ei-toivottuja päivityksiä tai konfiguraatiomuutoksia järjestelmiin tai yhteys yleiseen verkkoon katkeaa.	Liikenteenohjaus, rataverkon haltija, rautatieliikenteen harjoittajat
IT- ja OT -järjestelmien yhteenliittämisen rajapintariskit	IT- ja OT-järjestelmiä liitetään yhteen, jolloin OT-järjestelmien eheys voi vaarantua.	Liikenteenohjaus, rataverkon haltija ja rautatieliikenteen harjoittajat
Sähkönsaannin turvaamiseen liittyvät riskit	Kantaverkkoon tulee häiriö, joka estää sähkön siirtymisen syöttöasettamille tai -asemalta rataverkkoon tai joku pääsee oikeudetta sähköratojen valvontajärjestelmiin.	Rataverkon haltijat, liikenteenohjaus.
Telemaattisten järjestelmin riskit	Joku pääsee tahallisesti häiritsemään matkustajakuulutuksia tai informaationäyttöjä.	Rataverkon haltijat, rautatieliikenteen harjoittajat
Komponentteihin liittyvät riskit	Komponenttiin (esim. mikrosirut ja puhelimet) sisällytetään tahallisesti tekijä, joka aiheuttaa häiriöitä myös komponentin ulkopuolelle.	Liikenteenohjaus, rautatieliikenteen harjoittajat (kalusto)
Laitteiden yhteentoimivuusriskit	Kulunvalvontalaitteiden yhteensopivuus häiriintyy esimerkiksi ohjelmistojen päivityksistä tai huonosti suunnitelluista kehityshankkeista johtuen.	Liikenteenohjaus, rataverkon haltija, rautatieliikenteen harjoittajat
Liikkuvan kaluston kyberriskit	Liikkuvan kaluston kulunvalvontaa tai muita toimintoja häiritään siten, että kaluston käyttäminen ei ole turvallista.	Rautatieliikenteen harjoittajat, kaluston kunnossapitäjät
Järjestelmien kaappaus	Järjestelmien toiminta häiriintyy tai on pakko keskeyttää turvallisuuden varmistamiseksi	Kaikki raideliikenteen toimijat
Henkilökunnasta johtuvat riskit	Henkilökunta, tai aiemmin henkilökuntaan kuulunut, aiheuttaa joko tahallisesti tai osaamattomuuttaan häiriöitä järjestelmille.	Kaikki raideliikenteen toimijat
Alihankkijoista johtuvat riskit	Kuten edellä, mutta toimijana alihankkija.	Kaikki alihankintaa hyödyntävät raideliikenteen toimijat
Palveluiden käyttäjistä johtuvat riskit	Kuten edellä, mutta toimijana palvelun käyttäjä.	Kaikki palveluja tarjoavat raideliikenteen toimijat

Taulukko 4. Esimerkkejä raideliikenteen kyberuhista

Kyberturvallisuusskenaarioiden yksityiskohtaisessa tarkastelussa ja analysoinnissa voidaan käyttää esimerkiksi ns. Bowtie-mallia. Seuraavassa taulukossa esitetään esimerkkejä Bowtie-

mallin avulla työstetyistä yksittäisistä kyberturvallisuustapahtumista. Samalla taulukot toimivat esimerkkeinä toiminnoista, jotka voivat aikaansaada kyberturvallisuustapahtuman, miten tapahtumilta voidaan jo etukäteen suojautua ja jos tapahtuma suojauksesta huolimatta tapahtuu, mitkä ovat sen palauttavat suojaukset ja seuraukset.

Esimerkit on laadittu Traficomin 11.3.2020 järjestämässä raideliikenteen kyberturvallisuustyöpajassa sen testaamiseksi, voisiko Bowtie-mallista olla hyötyä kyberturvallisuustapahtumien tarkemmassa tarkastelussa ja sen hahmottamisessa, mitä kaikkia riippuvuuksia yksittäiseen tapahtumaan voi liittyä. On mahdollista, että mallia tullaan jatkossa hyödyntämään kattavammin erilaisten kyberturvallisuustapahtumien hallinnan kehittämisessä. Koska mallin käytöstä ei ole vielä tehty päätöstä, alla mallin rakennetta on hyödynnetty apuna taulukoita tehtäessä ilman, että esimerkkien luomisessa olisi vielä käytetty varsinaista Bowtie-mallien työstämiseen tarkoitettua ohjelmaa.

JUNAN KULKU					
Toiminto	**Käynnistävä tekijä**	**Tapahtuma/vaaratilanne**	**Estävä tai ennalta-ehkäisevä suojaus**	**Palauttava suojaus**	**Tapahtuman seuraus**
Fyysinen suojaus	Turvalaitetilaan murtautuminen	Kauko-ohjauksen lamaantuminen	Harjoitukset, koulutukset, auditoinnit	Varajärjestelmään turvautuminen, liikenteen pysäyttäminen tai rajoittaminen	Junien kulun estyminen
Suojaus	Verkon kautta hakkerointi				
Suojaus	Haittaohjelma				Onnettomuus
Varajärjestelmä	Varajärjestelmän kaatuminen				

KUNNOSSAPITO					
Toiminto	**Käynnistävä tekijä**	**Tapahtuma/vaaratilanne**	**Estävä tai ennalta-ehkäisevä suojaus**	**Palauttava suojaus**	**Tapahtuman seuraus**
Sopimusongelma	Alihankintasopimus puutteellinen	Alihankkija vaikuttaa järjestelmään kunnossapidon yhteydessä	Sopimuksen hyvä valmistelu ja päivittäminen tarvittaessa, osaavat sopimusneuvottelijat	Vahingon aiheuttajan ja syyn poistaminen ja eristäminen, varajärjestelmät kunnossa, vastuut ja työohjeet kunnossa, nopea reagointi virheeseen, viestintätaidot kunnossa	Järjestelmän lamaantuminen
Sopimusongelma	Sopimusrikkomus		Sopimusseuraamukset kunnossa, valvonta		
Pahat aikeet	Työn suorittajan tahallisuus		Palveluntarjoajan taustojen selvittäminen, aiemmat referenssit, sopimusmäärittelyt, palvelunkuvaukset kunnossa, säännölliset katselmukset		Onnettomuus tai vaaratilanne
Valvonnan puutteet	Alihankintaa ei valvonta, valvonta ei toimi		Valvonnan vastuuttaminen		Mainehaitta

4. Suositukset raideliikenteen kyberturvallisuuden kehittämiseksi

Tähän osioon on koottu Liikenne- ja viestintäviraston suositukset kyberturvallisuuden kehittämiseksi. Raideliikenteen toimijan toiminnan laadusta ja laajuudesta riippuu minkälaisilla toimenpiteillä kunkin toimijan tulisi pyrkiä vastaamaan annettuihin suosituksiin.

Osion koostamisessa on sovellettu Cybersecurity Capability Maturity Model (C2M2) -kyberturvallisuuden viitekehystä.

Liikenne- ja viestintävirasto suosittelee, että raideliikenteen toimijat käsittelisivät alla olevat suositukset ja pyrkivät ottamaan niitä mahdollisuuksien mukaan huomioon omassa toiminnassaan 1.6.2021 mennessä.

4.1. Kyberturvallisuus osana turvallisuusjohtamista ja turvallisuuskulttuuria

Liikenne- ja viestintävirasto suosittelee, että raideliikenteen toimijat sisällyttävät kyberturvallisuuden edistämisen osaksi turvallisuusjohtamisjärjestelmäänsä tai turvallisuuden hallintajärjestelmäänsä tai jos heillä ei kumpaakaan niistä ole, osaksi yleistä johtamisjärjestelmäänsä.

Tätä varten toimijoiden tulisi:

- määrittää kyberturvallisuusstrategia esimerkiksi osana turvallisuusjohtamisjärjestelmää sekä varmistaa organisaation johdon ja hallituksen tai johtoryhmän tuki kyberturvallisuusstrategian mukaisten tavoitteiden toteuttamiseksi
    - kyberturvallisuusstrategian tulee pitää sisällään vähintään lista kyberturvallisuustavoitteista ja suunnitelma niiden toteuttamiseksi
- huomioida kyberturvallisuus toiminnan jatkuvuuteen liittyvissä suunnitelmissa ja huolehtia, että kyberturvallisuusstrategia ja toiminnan jatkuvuuteen liittyvät suunnitelmat on sovitettu keskenään yhteen
- määrittää kyberturvallisuutta koskevat vastuut ja yhteistyömallit kattaen organisaation sekä toimintaan liittyvät muut toimijat ottaen huomioon, että raideliikennejärjestelmässä kyberturvallisuus on päästä päähän ulottuva ketju, joka kulkee useiden eri toimijoiden omistaman infrastruktuurin läpi
- määrittää suojattavat kohteet eli raideliikenteen jatkuvuuden ja turvallisuuden kannalta kriittiset informaatiojärjestelmät, operatiiviset järjestelmät ja tiedot, kuten liikenteenhallintajärjestelmät eri toimintoineen
    - määrittää toimintatavat suojattavien kohteiden omaisuusluetteloiden, konfiguraatioiden ja muutosten hallintaan
- määrittää organisaation laajuisen riskienhallintajärjestelmän organisaation kyberturvallisuusriskien tunnistamiseen, analysointiin, mitigoinnin mahdollistamiseksi ja seurantaan huomioiden liiketoimintayksiköt, tytäryhtiöt, yhteen liitetyt infrastruktuurit ja muut sidosryhmät
- määrittää toimintatavat käyttövaltuus- ja pääsynhallintaan fyysisten tilojen, informaatiojärjestelmien ja operatiivisten järjestelmien osalta huomioiden sisäiset ja ulkoiset henkilöt, mutta myös muut tahot (laitteet, järjestelmät, ohjelmistoprosessit) kiinnittäen erityistä huomioita etäyhteyksiin

- määrittää toimintatavat kyberturvauhkien ja haavoittuvuuksien havaitsemiseen, tunnistamiseen, analysointiin, hallitsemiseen ja niihin vastaamiseen ottaen huomioon raideliikenteen jatkuvuuteen ja turvallisuuteen kohdistuvat riskit

- määrittää toiminnot ja käytettävät teknologiat operatiivisen ja kyberturvallisuustiedon keräämiseen, analysointiin, hälytysten nostamiseen, esittämiseen ja hyödyntämiseen tilannekuvan muodostamiseksi organisaation toiminnasta ja kyberturvallisuuden tasosta

    - määrittää toimintatavat lokien keräämiseen sekä lokien ja muiden lähteiden kautta kerätyn tiedon seurantaan ja analysointiin

    - määrittää toimintatavat tilannekuvan luomiseen ja ylläpitämiseen

- määrittää suunnitelmia, prosesseja ja käytettäviä teknologioita kyberturvallisuuteen liittyvien tapahtumien ja -poikkeamien havaitsemiseksi, analysoimiseksi, niihin vastaamiseksi ja niistä palautumiseksi suhteessa raideliikenteen jatkuvuuteen ja turvallisuuteen kohdistuviin riskeihin

    - määrittää toimintatavat kyberturvallisuustapahtumista ja -poikkeamista ilmoittamiseksi

- määrittää toimintatavat toimitusketjun ja ulkoisten riippuvuuksien hallintaan, joilla hallitaan palveluiden ja suojattavien kohteiden ulkopuolisesta tahoista riippuvaisia kyberturvallisuusriskejä suhteessa raideliikenteen jatkuvuuteen ja turvallisuuteen kohdistuviin riskeihin

- määrittää toimintatavat työntekijöiden ja toimittajien taustatarkastuksiin sekä nimeämiseen sellaisiin tehtäviin, joissa on pääsy raideliikenteen jatkuvuuden ja turvallisuuden kannalta kriittisten palveluiden toimittamiseen liittyviin suojattaviin kohteisiin

- määrittää rakenteen ja toimintatavat organisaation kyberturvallisuuden kontrollien, prosessien ja muiden elementtien osalta suhteessa raideliikenteen jatkuvuuteen ja turvallisuuteen kohdistuviin riskeihin

    - määrittää kyberturvallisuusarkkitehtuuristrategia suojattavan tiedon ympärille kiinnittäen erityistä huomioita turvalaitteiden suunnittelu- ja käyttöperiaatteisiin sekä laitetilojen fyysiseen suojaamiseen ja valvontaan

    - toteuttaa verkkojen segmentointi sekä arvioida verkkojen kahdentamisen tarve ja toteuttaa tarvittavat verkkojen kahdennukset

    - varmistaa hankittavien järjestelmien turvallisuus asettamalla hankintavaiheessa tarvittavat kyberturvallisuusvaatimukset sekä hankittavalle järjestelmälle että toimittajan kyberturvallisuuden tasolle

    - varmistaa järjestelmien turvallisuus koko niiden elinkaaren ajan kiinnittäen erityistä huomioita olemassa olevien järjestelmien turvallisuuden varmistamiseen tilanteessa, jossa vanhoihin järjestelmiin tehdään muutoksia tai mahdollisesti digitalisoidaan osia tai kokonaisuuksia

    - varmistaa kehitettävien ohjelmistojen ja kolmansien osapuolten ratkaisujen ohjelmistoturvallisuus koko ohjelmistojen elinkaaren ajan ohjelmistojen hankinnasta käytöstä poistoon saakka huolehtien erityisesti, että turvallisen ohjelmistokehityksen periaatteita noudatetaan ja järjestelmät todetaan turvallisuustestauksella turvallisiksi ennen niiden käyttöönottoa

    - toteuttaa tiedon suojaaminen käsiteltävän tiedon tunnistamiseen ja luokitteluun perustuen

- huomioida kyberturvallisuuden kattava edistäminen käyttämässään johtamisjärjestelmässä
- sisällyttää kyberturvallisuus yhdeksi toimintansa kehittämisalueeksi, jota kehitetään kiinteästi yhteydessä muiden toimintojen kanssa
- kohdistaa kyberturvallisuuden edistämiseen mahdollisimman pitkälti muun toiminnan kehittämiseen olennaisena osana kuuluvia toimintamalleja (riskienarviointi, omavalvonta jne.)
- sopia oman organisaationsa kyberturvallisuuskulttuurista ja sisällyttää se osaksi koko toimintaansa koskevaa turvallisuuskulttuuria

4.2. Osaaminen ja pätevyydenhallinta

Liikenne- ja viestintävirasto suosittelee, että raideliikenteen toimijat kehittävät kyberturvallisuusosaamistaan ja huolehtivat osaamisen hallinnasta.

Tätä varten toimijoiden tulisi:

- varmistaa, että organisaatiossa on sen toiminnan laatuun ja laajuuteen nähden riittävää kyberturvallisuusosaamista, jota ylläpidetään ja kehitetään
- nimetä organisaation vastuuhenkilön tai -henkilöt, jotka tuntevat kyberturvallisuutta koskevan lainsäädännön ja standardit ja voivat varmistaa niiden riittävän huomioimisen ja noudattamisen organisaatiossa
- nimetä organisaation vastuuhenkilön tai -henkilöt, jotka tuntevat toimijan toiminnalliset ja liikennöintiä koskevat järjestelmät ja ymmärtävät niihin kohdistuvat kyberturvallisuusriskit sekä työskentelevät niiden minimoimiseksi
- kouluttaa myös muuta henkilöstöään ja tarvittaessa myös alihankkijoitaan kyberturvallisuuskysymyksistä ja huolehtia organisaation kyberturvallisuustietoisuuden kasvattamisesta

4.3. Kyberturvallisuusuhkien seuranta ja niihin varautuminen

Liikenne- ja viestintävirasto suosittelee, että raideliikenteen toimijat selvittävät organisaationsa osalta toimintatapoihin, järjestelmiin ja ihmisiin liittyvät haavoittuvuudet ja varautuvat kyberturvallisuusuhkiin sekä kyberturvallisuustapahtumista ja -poikkeamista palautumiseen.

Tätä varten toimijoiden tulisi:

- selvittää käyttämiensä toimintatapojen ja ihmisten kyberturvallisuustapahtumille ja järjestelmien kyberturvallisuushyökkäyksille alttiit kohdat ottaen huomioon mm. järjestelmien rajapinnat ja riippuvuudet
- seurata ja valvoa kyberturvallisuusuhkia ja niiden hallintaa reaaliaikaisesti operatiivisissa järjestelmissä ja informaatiojärjestelmissä, jotta niihin voitaisiin reagoida mahdollisimman aikaisessa vaiheessa

- huolehtia toimintatapojen, järjestelmien ja ihmisten kyberturvallisuusuhkille alttiiden kohtien suojaamisesta koko niiden elinkaaren ajan
- huomioida havaitut kyberturvallisuusuhkat järjestelmien hankinnan suunnitteluvaiheen vaatimusten asettamisesta lähtien koko järjestelmien elinkaaren ajan
- tarvittaessa priorisoida suojausjärjestys
- laatia omaa toimintaansa koskeva järjestelmien toipumissuunnitelma sekä toiminnon jatkuvuussuunnitelma, jossa huomioidaan organisaation keinot toiminnan jatkamiseen häiriötilanteissa sekä mahdollisuudet raideliikenteen jatkuvuuden ja turvallisuuden kannalta kriittisten palvelujen tarjoamisen varmistamiseen
- harjoitella jatkuvuussuunnitelmien testaamiseksi, kyberturvallisuustapahtumiin ja -poikkeamiin vastaamiseksi ja haavoittuvuuksien kartoittamiseksi

4.4. Riskienhallinnan hyödyntäminen

Liikenne- ja viestintävirasto suosittelee, että raideliikenteen toimijat hyödyntävät riskienhallintaa.

Tätä varten toimijoiden tulisi:

- kartoittaa toimintatapoihinsa, järjestelmiinsä ja ihmisiinsä kohdistuvat kyberturvallisuusriskit ja hyödyntävät jatkuvaa riskienarviointia
- huomioida kyberturvallisuusriskit päätöksiä tehdessään
- sopia hyväksyttävistä riskitasoista ja määrittää, millä toimenpiteillä organisaatiota suojataan ja mihin toimenpiteisiin mahdollisessa hyökkäystilanteessa ryhdytään hyökkäyksen havaitsemiseksi, analysoimiseksi, niihin vastaamiseksi ja niistä palautumiseksi
- huomioida havaitut kyberturvallisuusriskit järjestelmien hankinnan suunnitteluvaiheen vaatimusten asettamisesta lähtien koko järjestelmien elinkaaren ajan
- suunnitella järjestelmien elinkaarenhallinta kokonaisuutena ja varmistaa, että mahdollisten jäännösriskien hyväksyminen tehdään hallitusti ja tietoisesti

4.5. Yhteistyön lisääminen

Liikenne- ja viestintävirasto suosittelee, että raideliikenteen toimijat tekevät yhteistyötä järjestelmän kokonaissuojaustason nostamiseksi.

Tätä varten toimijoiden tulisi:

- määrittää oman organisaationsa osalta toimintatavat yhteistyöhön kyberturvallisuuden kehittämiseksi ja kyberturvallisuusriskien hallinnan edistämiseksi muiden alan toimijoiden sekä viranomaisten kanssa.
- huolehtia kyberturvallisuudesta yhteistyössä muiden alan toimijoiden kanssa ja pyrkiä yhtenäistämään toimintatapoja ja suojan tasoa esimerkiksi samaa järjestelmää tai yhteistä rajapintaa käyttävien kesken

- huolehtia alihankkijoiden kyberturvallisuustoimenpiteiden riittävyydestä ja niiden sovittamisesta oman organisaation kyberturvallisuuden toimintamalleihin

- välittää tietoja kyberturvallisuusuhkista, -riskeistä ja -hyökkäyksistä muille raideliikenteen toimijoille ja yhteistyöverkostoille yhteisen tilannekuvan luomiseksi ja jakamiseksi

4.6. Kyberturvallisuuden ohjauksen kehittäminen

Liikenne- ja viestintävirasto suosittelee, että raideliikenteen toimijat osallistuvat kyberturvallisuuden ohjauksen kehittämiseen.

Tätä varten toimijoiden tulisi:

- levittää hyviä käytäntöjään kyberturvallisuuden kehittämiseksi

- vaikuttaa kyberturvallisuussääntelyn hyvään kehittämiseen mm. yhteentoimivuuden teknisissä eritelmissä

- huolehtia kyberturvallisuuskysymysten esiin nostamisesta organisaatioiden välisissä sopimuksissa ja erilaisilla näköalapaikoilla

5. Lisätietoja ja tiedon lähteitä

- Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen sivut (https://www.kyberturvallisuuskeskus.fi/fi/), ks. esimerkiksi Ohjeet ja oppaat (https://www.kyberturvallisuuskeskus.fi/fi/ohjeet) ja suomenkielinen kyberturvallisuuden riskienhallinnan arviointikehys ja työkalu (https://www.kyberturvallisuuskeskus.fi/fi/kybermittari)

- ENISA:n sivut (https://www.enisa.europa.eu/) ks. esimerkiksi ENISA Threat Landscape report 2018 (https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018) ja ENISA threat landscape for 5G Networks (https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks)

- Cyber Europe (https://www.cyber-europe.eu/)

- ISA 62443, Security for Industrial Automation and Control Systems

- CENELEC (https://www.cenelec.eu/): Cybersecurity standard for EU Railways TS 50701 (standardi työn alla, tarkoitus saada valmiiksi helmikuuhun 2021 mennessä

- NIST Cyber Security Framework , kyberturvallisuusviitekehys (https://www.nist.gov/cyberframework)

- NIST 800-82r2, teollisuuden ohjausjärjestelmien kyberturvallisuusohje (https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final)

- ISO/IEC 27001, Tietoturvan hallintajärjestelmän vaatimukset

- ISO/IEC 27002, Tietoturvan hallintakeinojen menettelyohjeet

- ISO/IEC 27005, Tietoturvariskien hallinta

- Cybersecurity Capability Maturity Model (C2M2) v. 2.0 draft, kyberturvallisuusviitekehys (https://www.energy.gov/sites/prod/files/2019/10/f67/C2M2%20v2.0%2006202019%20DOE%20for%20Comment%20%28Draft%29.pdf)

- CYRail (https://cyrail.eu/) Ks. myös CYRail Recommendations on cybersecurity of rail signalling and communication systems (https://cyrail.eu/IMG/pdf/final_recommendations_cyrail.pdf)

- UK:n Rail Cyber Security Strategy (https://www.raildeliverygroup.com/component/arkhive/?task=file.download&id=469772253)

- Cebula, James J. & Young, Lisa R. 2010. A Taxonomy of Operational Cyber Security Risks. Carnegie Mellon University

Hyväksytty 29.6.2020

Pietari Pentinsaari
Johtaja

Heidi Niemimuukko
Päällikkö

Tämä asiakirja on allekirjoittamisen sijasta varmennettu siten, että siitä näkyy asian esittelijän ja ratkaisijan nimi. Päätöksen esittely asian ratkaisijalle on tehty sähköpostitse. Tämä poikkeuksellinen varmentamistapa on tilapäisesti käytössä koronaviruksen leviämisen rajoittamistoimien johdosta, joiden seurauksena asiaa käsittelevä virkamies tekee etätöitä eikä tavanomainen asiakirjan allekirjoittaminen ole mahdollista.