Antopäivä:	Voimaantulopäivä:	Voimassa:
30.1.2023	30.1.2023	toistaiseksi

Lainsäädäntö, johon ohje perustuu:

Muutostiedot:
Versio 1.0, antopäivä 29.6.2020, voimaantulopäivä 1.7.2020
Versio 1.1, antopäivä 1.2.2023

- Kappale 1-2: Vähäisiä ymmärrettävyyttä edistäviä muutoksia
- Kappale 3: Päivitetty vastaamaan 2022 tilannekuvaa
- Kappale 3.1: Lisätty mm. viittaukset SVPL 244 a §, TS50701, Traficomin ohjeeseen raideliikenteen häiriöiden ilmoittamisesta ja Kybermittari. Päivitetty kuvausta tulevasta sääntelystä ja raideliikenteen kyberturvallisuuden kansainvälisistä verkostoista.
- Kappale 3.2-3.3: Vähäisiä muutoksia, ei oleellisia vaikutuksia sisältöön
- Kappale 4: Suositetaan hyödyntämään uusissa OT-järjestelmissä TS50701 ja olemassa olevien järjestelmien osalta IEC 62443 sarjaa. IT-järjestelmien osalta ensisijaisesti suositetaan ISO/IEC 27001 hyödyntämistä, vaihtoehtoinen viitekehys esimerkiksi Kybermittari. ISO/IEC 27001 hallintajärjestelmään voidaan sisällyttää myös OT-ympäristö hyödyntäen lisäksi OT-järjestelmien standardeja. Em. viitekehyksillä voisi korvata päällekkäisiltä osin tämän suosituksen kappaleiden 4.1-4.11 kohdat.
- Suosituksen kappaleet 4.1-4.11 uudistettu vastaamaan vähintään Kybermittarin tavoitetasoa 1. Aikaisemmat suositukset säilytetty siltä osin, kun ne vastaavat kybermittaria. Useita uusia suosituksia lisätty.
- Suosituksessa esitetyt hallintakeinot ja kybermittari -työkalu liitteinä

SUOSITUS KYBERTURVALLISUUDEN EDISTÄMISESTÄ RAIDELIIKENTEESSÄ

Sisällys

Taulukot

Liitteet

1. Suosituksen tarkoitus ja soveltamisala

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

- raideliikennealan 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. Suosituksen liitteet sisältävät luvun 4 kohdat taulukkomuodossa ja liitteillä on tarkoitus edistää suosituksen hyödynnettävyyttä.

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.

Suosituksen 2020 versio laadittiin virkatyönä Liikenne- ja turvallisuusvirastossa ja sen valmistelussa kuultiin raideliikenteen toimijoita. Suosituksen 2022 päivitys on laadittu myös Liikenne- ja viestintäviraston virkatyönä. Vuoden 2022 suosituksen päivitys on ollut valittujen toimijoiden kommentoitavana syksyllä 2022 ja kaikkien raideliikennetoimijoiden kommentoitavana marraskuussa 2022.

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]

[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)

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.
Kyberuhka	Kyberuhka tarkoittaa mahdollisen ei-toivotun haitallisen tapahtuman tai kehityskulun aiheuttajaa, 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.
Kyberriski	Kyberriski ilmaistaan haavoittuvuutta hyödyntävän uhkan, mahdollisten tapahtumien, seurausten ja niiden todennäköisyyksien yhdistelmänä. Riskejä voidaan hallita riskienhallintamenetelmin.
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 maantieteellinen hajautuneisuus, operatiivisten järjestelmien avulla tapahtuva laitteiden ohjaus sekä tiedon eheyden ja saatavuuden korostuminen. 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.
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.
OT, operatiivinen teknologia	Operatiivisella teknologialla (OT, operational technology) tarkoitetaan ohjelmoitavia digitaalisia järjestelmiä ja laitteita, jotka vuorovaikuttavat fyysisen ympäristön kanssa tai hallitsevat laitteita, jotka vuorovaikuttavat fyysisen ympäristön kanssa. OT-järjestelmillä esimerkiksi hallitaan liikenneverkkoinfrastruktuuria ja liikkuvaa kalustoa, kuten liikennöintiä, merkinantoa, voimanlähteitä, viestintää ja asemien hallintaa.
IT, informaatioteknologia	Informaatioteknologialla (IT, information technology) tarkoitetaan liiketoimintaa tukevia IT-järjestelmiä sekä IT-järjestelmiä, jotka tukevat operatiivisia järjestelmiä ja tarjoavat liittymän operatiivisiin järjestelmiin. Esimerkkejä: Matkustajainformaatio, kuljettajan päätelaitesovellukset, kuljetusten seurantajärjestelmät, liikenteenohjauksen hallintajärjestelmät, yleisesti käytössä olevat tiedonsiirtotavat (esim. WLAN-verkko) sekä tieto- ja viestintäjärjestelmät

Taulukko 1 Keskeiset suosituksessa käytettävät määritelmät

3. Kyberturvallisuus raideliikenteessä

Eurooppalaisen rautatiejärjestelmän yhtenäistymisen ja digitalisoitumisen myötä järjestelmästä on tullut harmonisoidumpi ja avoimempi, mutta mahdollisesti myös haavoittuvampi. Venäjän hyökkäyssota Ukrainassa on vahvistanut rautatiejärjestelmän olevan tärkeä osa yhteiskunnan kriittistä infrastruktuuria. Vuoden 2022 aikana Ukrainassa, Valko-Venäjällä ja EU:n alueella on havaittu useita rautatiejärjestelmään kohdistuneita kyberhäiriöitä. Nämä tekijät ovat johtaneet kyberturvallisuusriskien kasvuun raideliikenteessä. Raideliikenteen tehokkuuden parantaminen nojaa vahvasti digitalisaatioon ja tulevaisuuden digitalisaatiotavoitteiden mahdollistamien hyötyjen saavuttaminen edellyttää vahvaa kyberturvallisuuden perustasoa.

Kaupunkiraideliikennejärjestelmät ovat rautatieliikenteeseen verrattuna maantieteellisesti selvästi rajoittuneemmat. Kuitenkin matkustajien ja matkojen määrästä johtuen häiriöiden vaikutukset voivat olla yhteiskunnallisesti merkittäviä. Myös kaupunkiraideliikennejärjestelmät ovat maailmalla joutuneet kyberturvallisuushyökkäysten kohteeksi, joilla on ollut vaikutuksia järjestelmien toimintaan toimintavarmuuteen. Häiriöillä voi olla myös vaikutus liikenneturvallisuuteen.

Raideliikenteessä kyberriskit voivat realisoitua monin eri tavoin. Kyberturvallisuusriski voi realisoitua tahattomasti, mutta myös tarkoituksellisesti, jolloin sen toteuttajina voivat olla yksittäiset ihmiset, verkostot, organisaatiot tai valtiolliset tahot. Uhkien tunnistaminen edellyttää kaikkien uhkatekijöiden huomioimista, olivat ne sitten luonnon tai ihmisen aiheuttamia, onnettomuuksia tai tahallaan aiheutettuja. 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, terroristien tai hakkerienkin joukosta. Traficomin raideliikenteen palvelukokonaisuus pitää yllä tilannekuvaa julkisuuteen raportoiduista raideliikenteen kyberhäiriöistä.

Toteutuneilla kyberturvallisuushäiriöillä voi olla merkittäviä negatiivisia vaikutuksia raideliikenteeseen. Todennäköistä on, että kyberturvallisuushäiriöt johtavat palveluiden saatavuuden heikentymiseen, lisätyöhön ja mainekolauksiin, mutta ne voivat johtaa myös vaaratilanteisiin ja jopa onnettomuuksiin. Tässä suosituksessa kyberturvallisuutta käsitelläänkin erityisesti turvallisuuden kannalta kriittisten järjestelmien osalta.

Koska rautatiejärjestelmä on kasvavassa määrin yksi yhteinen järjestelmä, toteutunut kyberturvallisuushäiriö voi johtaa jopa koko järjestelmän ja valtion rataverkon kattaviin häiriöihin. Vastaavasti on mahdollista, että kyberturvallisuushäiriö 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. Merkittävillä raideliikenteen häiriöillä voi olla myös välillisiä vaikutuksia muiden liikennemuotojen ja muun yhteiskunnan kriittisen infrastruktuurin toimintaan.

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

Kyberturvallisuutta raideliikennejärjestelmässä säädellään EU:n verkko- ja tietojärjestelmien turvallisuutta koskevassa NIS-direktiivissä[2] (EU:n verkko- ja tietoturvadirektiivi, (EU) 2016/1148). Sitä ei kuitenkaan sää-

[2] https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016L1148&from=FI

dellä kattavasti rautatieliikenteen omassa EU-sääntelyssä tai huomioida esimerkiksi rautatieliikenteen turvallisuusjohtamisjärjestelmän sisältöä ohjaavissa arviointikriteereissä. Vaikka rautatietoimijoiden turvallisuusjohtamisjärjestelmä perustuu rautateitä koskevaan EU-sääntelyyn, kyberturvallisuus suositetaan sisällytettävän osaksi toimijan turvallisuusjohtamisjärjestelmää tai turvallisuuden hallintajärjestelmää.

3.1. Raideliikenteen kyberturvallisuussääntely

3.1.1. Nykytila

Raideliikenteen kyberturvallisuussääntelyn kehityksen odotetaan jatkuvan. Raideliikennelain 169 § on jo yli neljän vuoden ajan sisältänyt 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 NIS-direktiivi. Laki sähköisen viestinnän palveluista 244 a § velvoittaa tiettyjen edellytysten täyttyessä raideliikennejärjestelmän keskeisimpien toimijoiden, kuten valtion rataverkon haltijan ja liikenteenohjauspalveluiden tarjoajan, yleiseen viestintäverkkoon liitetyn erillisverkon osalta tunnistamaan ja dokumentoimaan verkon kriittiset osat ja niissä käytetyt verkkolaitteet sekä arvioimaan, miten varmistutaan siitä, että verkkolaitteiden käytöstä ei aiheudu uhkaa kansalliselle turvallisuudelle tai maanpuolustukselle. Velvoitteen taustalla on EU:n 5G toolbox[3] ja huoli 5G-verkkojen tietoturvasta.

Raideliikennelaki sisältää myös yleisemmän velvoitteen ilmoittaa tilannekuvan muodostamiseksi tarvittavista tiedoista. Lain 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. Traficom on ohjeistanut pykälän mukaista toimintaa vuonna 2022 (Ohje raideliikenteen häiriöiden ilmoittamisesta). Pykälän voidaan katsoa sisältävän myös kyberturvallisuusuhkista ja -häiriöistä ilmoittamisvelvollisuuden. Kaikkia raideliikennetoimijoita suositetaan ilmoittamaan kyberturvallisuuteen liittyvistä häiriöistä matalalla kynnyksellä Traficomin Kyberturvallisuuskeskukselle ja Raideliikenne palvelukokonaisuudelle. Yksinkertaisinta ilmoittaminen on sähköisellä lomakkeella: https://eservices.traficom.fi/dataservices/forms/NISlomake.aspx

Raideliikennelain lisäksi kyberturvallisuus huomioidaan Traficomin määräyksessä valmiussuunnitelman järjestämisestä (TRAFICOM/308489/03.04.04.00/2019). Määräys muun muassa edellyttää, että rataverkon haltija kuvaa valmiussuunnitelmassaan kybertoimintaympäristönsä. Määräys koskee sekä valtion rataverkon haltijaa, että yksityisraiteen haltijoita. Lisäksi valtion rataverkon haltijan ja sen liikenteenohjauspalvelun tarjoajan tulee huomioida kybertoimintaympäristöä uhkaavat tapahtumat ja uhkat kuvatessaan menettelyitä, joilla se varmistaa rautatieliikenteen hoidon varautumisen eri tavoitetasoilla. Määräys tuli sovellettavaksi siirtymäajan jälkeen 1.6.2021. Traficom on antanut myös määräystä koskevan ohjeen valmiussuunnitelman laatimisesta.[4]

3.1.2. Tuleva

Raideliikenteen kyberturvallisuuden sääntelyä, standardointia ja ohjeistusta kehitetään useilla eri tahoilla. Tulevasta EU-sääntelystä keskeisin on 27.12.2022 julkaistu yhteiskunnan kriittisten palveluiden kyberturvallisuutta koskeva ns. NIS2 direktiivi (EU) 2022/2555, joka tarkentaa yhteiskunnan kriittisten palveluiden kyberturvallisuuden riskien hallinnan vaatimuksia. NIS2 direktiiviuudistus koskee myös raideliikennealan valmistavaa sektoria. Standardisointiorganisaatio CENELEC on julkaissut rautateiden kyberturvallisuuden teknisen eritelmän TS50701 vuonna 2022. Standardisointiorganisaatio IEC kehittää teknisen eritelmän pohjalta

[3] https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security
[4] https://www.traficom.fi/fi/saadokset/ohje-valmiussuunnitelman-laatimiseksi-raideliikenteessa

kansainvälistä rautateiden kyberturvallisuusstandardia (IEC projektiryhmä). IEC:n on tarkoitus julkaista rautatiejärjestelmän kyberturvallisuusstandardi 31.7.2025. Traficomin Kyberturvallisuuskeskus osallistuu Euroopan rautateiden kyberturvallisuuden tiedonvaihtoryhmä ER-ISAC:in toimintaan. ER-ISAC on julkaissut yhdessä EU:n kyberturvallisuusvirasto ENISA:n kanssa ohjeen TS50701 soveltamisesta. Traficom on mukana ENISA:n Transport Resilience and Security Expert Group (TRANSSEC) raideliikenneryhmässä. ENISA on vuosittain julkaissut raideliikennejärjestelmän kyberturvallisuutta koskevia tutkimuksia. Lisäksi Traficom ja Poliisihallitus ovat mukana EU-komission alaisissa maaliikenteen ja rautateiden turvallisuusryhmissä Expert Group on Land Transport Security (Landsec) ja Rail Passanger Security Platform (Railsec), joissa jaetaan tietoa raideliikenteen kyberturvallisuudesta ja laaditaan suosituksia. Kaikilla raideliikenteen toimijoilla on mahdollisuus vaikuttaa toimialan kyberturvallisuuden kehitykseen. Väylävirasto on kansainvälisen rautatieliitto UIC:n jäsen ja UIC:n kyberturvallisuusryhmän on tarkoitus aktivoitua vuoden 2022 loppupuolella. UIC oli mukana CYRAIL-projektissa, joka 2018 julkaisi kyberturvallisuussuosituksen ohjauksesta ja merkinannosta. Väylävirasto on myös mukana European Rail Infrastructure Managers (EIM) kyberturvallisuusryhmässä ja eurooppalaisen raideliikenteen hallintajärjestelmän (ERMTS) käyttäjäryhmän (EUG) kyberturvallisuuden työryhmässä. EUG esimerkiksi selvittää sertifikaattien hallintaa ERTMS online avaintenhallintajärjestelmässä. Lisäksi tulee huomioida Valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla, jonka toimenpiteet toteutuessaan velvoittaisi muun muassa määrittämään kriittiset tieto- ja tietoliikennetekniset toiminnot sekä käyttämään ISO 27001 -sertifiointia.[5]

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 muun muassa CENELEC:in TS 50701 railway applications - cybersecurity.

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 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. Uhka tarkoittaa mahdollisen ei-toivotun vahingollisen tapahtuman aiheuttajaa, ja uhkia voidaan hallita arvioimalla niiden aiheuttamat riskit. Riskejä sen sijaan voidaan käsitellä riskienhallinnan menetelmin.

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

[5] https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f80732d82

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 operationaalisia toimia. Kyberriskien kokonaisuuden kannalta on tärkeää huomioida, että kyberriskit korreloivat usein keskenään ja yksi riski voi toteutuessaan aiheuttaa tapahtumasarjan, joka laukaisee useampia riskejä.[6]

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 Taidot Tiedot Ohjaus Saatavuus	2.3. Järjestelmät Suunnittelu Tekniset vaatimukset Integraatio Monimutkaisuus	3.3. Tukitoiminnot Henkilöstöhallinta Rahoitus Kehitys- ja koulutustoiminta Hankinta	4.3. Liiketoiminnan ongelmat 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 katsotaan-

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

kin 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. Myös OT-järjestelmien tekniset ratkaisut alkavat nykypäivänä lähestyä IT-järjestelmien teknisiä ratkaisuja.

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.

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 järjestelmissä 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, kyberturvallisuusvaatimuksista on tärkeää sopia myös vanhoja sopimuksia päivitettäessä tai uusittaessa.

3.3. Esimerkkejä kyberturvallisuusuhkista ja niiden hallinnan keinoista

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

Kyberriski	Esimerkkejä (uhka)	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 järjestelmässä esimerkiksi sen päivityksen yhteydessä.	Liikenteenohjaus, rataverkon haltija, rautatieliikenteen harjoittajat
Liikenteen ohjausjärjestelmien yleiseen verkkoon liittymisen riskit	Yleisen verkon kautta tehdään tahallisesti eitoivottuja päivityksiä tai konfiguraatiomuutoksia järjestelmiin tai yhteys yleiseen verkkoon katkeaa.	Liikenteenohjaus, rataverkon haltija, rautatieliikenteen harjoittajat
IT- ja OT -järjestelmien yhteenliittämisen ja yleiseen verkkoon liittämisen rajapintariskit	IT- ja OT-järjestelmiä liitetään yhteen sekä yleiseen verkkoon, jolloin OT-järjestelmien eheys voi vaarantua.	Liikenteenohjaus, rataverkon haltija ja rautatieliikenteen harjoittajat
Sähkönsaannin turvaamiseen liittyvät riskit	Kantaverkkoon tulee häiriö, joka estää sähkön siirtymisen syöttöasemille 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	Kaappauksen seurauksena 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. Erityisesti vaaralliset työyhdistelmät.	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 3. Esimerkkejä raideliikenteen kyberuhista

Kyberturvallisuusskenaarioiden yksityiskohtaisessa tarkastelussa ja analysoinnissa voidaan käyttää esimerkiksi ns. Bowtie-mallia.[7] 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.

JUNAN KULKU					
Toiminto	**Käynnistävä tekijä**	**Tapahtuma/vaaratilanne**	**Estävä tai ennaltaehkäisevä 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				

Taulukko 4. Esimerkkejä junan kulkuun liittyvien kyberturvallisuustapahtumien tarkastelusta

KUNNOSSAPITO					
Toiminto	**Käynnistävä tekijä**	**Tapahtuma/vaaratilanne**	**Estävä tai ennaltaehkäisevä 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, salassapitosopimukset		
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

Taulukko 5. Esimerkkejä kunnossapitoon liittyvien kyberturvallisuustapahtumien tarkastelusta

4. Suositukset raideliikenteen kyberturvallisuuden kehittämiseksi

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

[7] Esimerkiksi IEC 31010:2019 Riskienhallinta. Riskien arviointimenetelmät. B.4.2 Rusettianalyysi (Bow tie analysis) ja s. 22
https://www.traficom.fi/sites/default/files/media/file/Guidance%20for%20FSTD%20operators.pdf

Liikenne- ja viestintävirasto suosittelee, että uusissa raideliikennejärjestelmän operatiivisen teknologian (OT) osissa sovellettaisiin TS50701 Railway Applications - Cybersecurity teknistä eritelmää ja myöhemmin eritelmän pohjalta kehitettävää standardia. Olemassa olevien OT-järjestelmien suositetaan jatkettavan teollisuusautomaation turvallisuuteen tarkoitettua IEC 62443 sarjan noudattamista, mikäli järjestelmät on kehitetty niiden pohjalta.

Kaikkien raideliikennejärjestelmän toimijoiden suositellaan arvioivan ja mittaavan organisaationsa kyberturvallisuuden tasoa. Olemassa olevien hallinnollisten IT-järjestelmien osalta ensisijaisesti suositellaan käytettävän ISO/IEC 27001:2022[8] kyberturvallisuuden hallintajärjestelmästandardia. ISO/IEC 27001 tietoturvallisuuden hallintajärjestelmällä on mahdollista hallinnoida myös OT-ympäristöä, jossa lisäksi sovelletaan edellä mainittuja OT-ympäristöön soveltuvia standardeja.[9] Muu vaihtoehtoinen viitekehys voi olla esimerkiksi Kyberturvallisuuskeskuksen ylläpitämä, ilmainen ja suomenkielinen Kybermittari[10]. Kybermittaria viitekehyksenä käytettäessä kaikkien raideliikennetoimijoiden suositetaan ylittävän tavoitetason 1. Raideliikennejärjestelmän kriittisten palveluiden tarjoajien (NIS-toimijoiden) suositetaan ylittävän tavoitetason 2. Tämän suosituksen liitteenä on Kybermittari_V2 arviointityökalu, johon on merkitty ristiin viittaukset kappaleiden 4.1-4.11 suosituksista.

Edellä mainittuja viitekehyksiä soveltamalla voi korvata jäljempänä olevat kappaleiden 4.1-4.11 suositukset siltä osin, kun valitun viitekehyksen mukaiset vaatimukset ovat vähintään yhtä vaativia. Tämän suosituksen kappale 4.12 koskee yhteistyön lisäämistä raideliikennejärjestelmässä. Suosituksen kappaleiden 4.1-4.11 koostamisessa on sovellettu Kybermittarin tavoitetasoa 1, mutta muutamat suosituksen kohdat asettuvat tavoitetasoa 1 korkeammalle. Kybermittari perustuu NIST Cybersecurity Framework ja Cybersecurity Capability Maturity Model (C2M2) -kyberturvallisuuden viitekehykseen, johon myös aikaisempi, tällä suosituksella päivitetty, suositus kyberturvallisuuden edistämisestä raideliikenteessä perustui. Myös Digi- ja väestötietoviraston (DVV) julkaiseman digitaalisen turvallisuuden arkkitehtuurikehys (DTARK) perustuu NIST Cybersecurity Framework -kehykseen. DTARK soveltuu hyvin kyberturvallisuuden suunnitteluun, mutta sitä ei ole ensisijaisesti tarkoitettu kyberturvallisuuden tason arviointiin ja mittaamiseen.

4.1. Kyberturvallisuus osana turvallisuusjohtamista ja turvallisuuskulttuuria

Liikenne- ja viestintävirasto suosittelee, että raideliikenteen toimijat sisällyttävät kyberturvallisuuden johtamisen osaksi turvallisuusjohtamisjärjestelmäänsä tai turvallisuuden hallintajärjestelmäänsä tai jos heillä ei kumpaakaan niistä ole, osaksi yleistä johtamisjärjestelmäänsä. Kyberturvallisuutta edistetään mahdollisimman pitkälti hyödyntäen muun toiminnan kehittämiseen olennaisena osana kuuluvia toimintamalleja (riskienarviointi, omavalvonta jne.) 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.
    - Dokumentoida kyberturvallisuusstrategia ja tavoitteet. Strategian ja tavoitteiden tulee olla linjassa organisaation yleisten tavoitteiden ja kriittiseen infrastruktuuriin kohdistuvien riskien kanssa.

[8] https://sales.sfs.fi/fi/index/tuotteet/SFS/ISO/ID5/2/1155761.html.stx
[9] Traficomilla ei ole toimivaltaa vaatia toimijoilta ISO/IEC 27001 sertifiointia, vaikka esimerkiksi Tanskassa sertifiointivaatimus on olemassa. Traficom kohdistaa toimijoihin valvontaa riskiperustaisesti ja sertifikaatin hankkimisella olisi Traficomin valvonnan tarvetta vähentävä vaikutus.
[10] https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostot/kybermittari

- Huomioida kyberturvallisuus toiminnan jatkuvuuteen liittyvissä suunnitelmissa ja huolehtia, että kyberturvallisuusstrategia ja toiminnan jatkuvuuteen liittyvät suunnitelmat on sovitettu keskenään yhteen.
- Osoittaa resurssit (henkilöt, rahoitus ja työkalut) kyberturvallisuuden hallinnan perustamiseen.
- Määrittää ja dokumentoida 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.

4.2. Kriittisten palveluiden suojaaminen

Liikenne- ja viestintävirasto suosittelee, että raideliikenteen toimijat tunnistavat roolinsa logistiikkaketjun osana, joka on yhteiskunnan kriittinen palvelu ja hallitsevat riskejä sen mukaisesti. Kriittiset palvelut ja niiden riippuvuudet tulee tunnistaa ja hallita sekä minimoida kyberhäiriöiden vaikutukset. Tätä varten toimijoiden tulisi:

- Määrittää ja dokumentoida raideliikenteen jatkuvuuden ja turvallisuuden kannalta kriittiset palvelut.
- Määrittää ja dokumentoida raideliikenteen jatkuvuuden ja turvallisuuden kannalta kriittisten palveluiden tuottamiseen tarvittava data.
- Määrittää ja dokumentoida raideliikenteen jatkuvuuden ja turvallisuuden kannalta kriittiset prosessit.
- Määrittää ja dokumentoida suojattavat kohteet eli raideliikenteen jatkuvuuden ja turvallisuuden kannalta kriittiset informaatiojärjestelmät, operatiiviset järjestelmät ja tiedot, kuten liikenteenhallintajärjestelmät eri toimintoineen.
- Määrittää ja dokumentoida tilannekuvan ja kriittisten järjestelmien, -palveluiden ja -laitteiden valvonnan kannalta oleelliset järjestelmät ja toiminteet.
- Saattaa organisaation turvallisuuden hallinnan ja politiikkojen piiriin kaikki raideliikenteen jatkuvuuden ja turvallisuuden kannalta kriittisten palveluiden tuottamiseen tarvittavat resurssit (data, prosessit, tilat, laitteet, toimitusketjut).
- Saattaa organisaation riskienhallinnan politiikkojen piiriin kaikki raideliikenteen jatkuvuuden ja turvallisuuden kannalta kriittisten palveluiden tuottamiseen tarvittavat resurssit (data, prosessit, tilat, laitteet, toimitusketjut).
- Laatia kybertapahtumien ja -häiriöiden hallintasuunnitelma, joka kattaa kaikki raideliikenteen jatkuvuuden ja turvallisuuden kannalta kriittiset palvelut.
    - Hallintasuunnitelma kattaa perusteellisesti tunnettujen hyökkäysten todennäköiset vaikutukset.
    - Kybertapahtumien ja -häiriöiden hallintaan osallistuva henkilöstö sisäistää ja ymmärtää hallintasuunnitelman.
    - Hallintasuunnitelma on dokumentoitu ja jaettu relevanteille sidosryhmille.

4.3. Omaisuuden, muutosten ja konfiguraatioiden hallinta

Liikenne- ja viestintävirasto suosittelee, että raideliikenteen toimijat hallitsevat IT- ja OT-omaisuutta. Omaisuudella tarkoitetaan toimintojen kannalta olennaisia laitteita, ohjelmistoja ja tietoja. Tätä varten toimijoiden tulisi:

- Luoda rekisteri raideliikenteen jatkuvuuden ja turvallisuuden kannalta tärkeistä laitteista ja ohjelmistoista.
- Luoda rekisteri raideliikenteen jatkuvuuden ja turvallisuuden kannalta tärkeistä tietovarannoista kuten toimijan toimialaan kuuluvista kapasiteetinhallinnasta ja asiakastiedoista sekä laitteiden ja ohjelmistojen perusasetuksista.
- Luoda vakioidut perusasetukset laitteiden, ohjelmistojen ja tietovarantojen konfiguraatioista.

- Arvioida ja hyväksyttää rekisteriin kirjattuihin laitteisiin, ohjelmistoihin ja tietovarantoihin tehtävät muutokset ennen niiden toteuttamista.
    - Pitää lokia rekisteriin kirjattuihin laitteisiin, ohjelmistoihin ja tietovarantoihin tehtävistä muutoksista.
- Luoda menetelmät laiteohjelmistojen pitämisestä ajan tasalla (esim. ohjelmistopäivitykset)
- Luoda menetelmät kriittisten laitteiden etävalvonnasta, -hallinnasta ja -päivittämisestä.

4.4. Uhkien ja haavoittuvuuksien hallinta

Liikenne- ja viestintävirasto suosittelee, että raideliikenteen toimijat määrittävät toimintatavat kyberturvauhkien ja haavoittuvuuksien havaitsemiseen, tunnistamiseen, analysointiin, hallitsemiseen ja niihin vastaamiseen ottaen huomioon raideliikenteen jatkuvuuteen ja turvallisuuteen kohdistuvat uhat. Tätä varten toimijoiden tulisi:

- Tunnistaa soveltuvia tietolähteitä haavoittuvuuksien tunnistamiseksi.
    - Kerätä ja tulkita haavoittuvuustietoa toimintaansa varten.
    - Tehdä haavoittuvuusarviointeja.
    - Puuttua toimintansa kannalta olennaisiin haavoittuvuuksiin esimerkiksi lisäämällä valvontaa tai asentamalla korjauspäivityksiä.
    - Haavoittuvuusarviointeja hyödyntäen selvittää käyttämiensä järjestelmien kyberturvallisuushyökkäyksille alttiit kohdat ottaen huomioon mm. järjestelmien rajapinnat ja riippuvuudet.
- Tunnistaa soveltuvia tietolähteitä uhkien tunnistamiseksi.
    - Kerätä ja tulkita uhkatietoa toimintaansa varten.
    - Puuttua toimintansa kannalta olennaisiin uhkiin esimerkiksi lisäämällä valvontaa tai seuraamalla uhkien kehitystä.
        - Seurata ja valvoa kyberturvallisuusuhkia ja niiden hallintaa riskiperustaisella oikea-aikaisuudella 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.

4.5. Riskienhallinta

Liikenne- ja viestintävirasto suosittelee, että raideliikenteen toimijat määrittävät organisaation laajuisen riskienhallintajärjestelmän kyberturvallisuusriskien tunnistamisen, analysoinnin ja vähentämisen mahdollistamiseksi sekä riskien seuraamiseksi huomioiden liiketoimintayksiköt, tytäryhtiöt, yhteen liitetyt infrastruktuurit ja muut sidosryhmät suhteessa raideliikenteen jatkuvuuteen ja turvallisuuteen kohdistuviin riskeihin. Tätä varten toimijoiden tulisi:

- Suunnitelmallisesti ohjata kyberturvallisuuden riskienhallintaa.
- Tunnistaa kyberriskejä kartoittamalla toimintatapoihinsa, järjestelmiinsä ja ihmisiinsä kohdistuvia riskejä ja hyödyntää jatkuvaa riskienarviointia
- Priorisoida kyberriskit niiden arvioitujen vaikutusten perusteella.
- Reagoida kyberriskeihin ja kyberriskikategorioihin esimerkiksi pienentämällä, hyväksymällä, välttämällä tai siirtämällä niitä.
- Sopia hyväksyttävistä riskitasoista ja määrittää, millä toimenpiteillä organisaatiota suojataan ja mihin toimenpiteisiin mahdollisessa hyökkäystilanteessa ryhdytään hyökkäyksen havaitsemiseksi, analysoimiseksi, niihin vastaamiseksi ja niistä palautumiseksi.

- Huomioida kyberturvallisuusriskit päätöksiä tehdessä.
    - 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.

4.6. Identiteetin ja pääsynhallinta

Liikenne- ja viestintävirasto suosittelee, että raideliikenteen toimijat määrittävät 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. Tätä varten toimijoiden tulisi:

- Osoittaa erilliset identiteetit työntekijöille ja muille yksiköille (kuten prosessit ja laitteet, jotka tarvitsevat pääsyn toimintoihin kuuluviin laitteisiin, ohjelmistoihin ja tietovarantoihin), sekä arvioida jaettujen identiteettien tarpeellisuutta.
    - Jakaa työntekijöille ja muille yksiköille pääsyvaltuustiedot kuten salasanat, älykortit tai avaimet.
    - Poistaa identiteetit käytöstä, kun niitä ei enää tarvita.
- Käyttää loogisten käyttöoikeuksien (tietojärjestelmien) hallinnan valvonnan keinoja.
    - Poistaa käyttöoikeudet, kun niitä ei enää tarvita.
- Käyttää fyysisen pääsynhallinnan valvontakeinoja (esimerkiksi aitoja, lukkoja tai kylttejä).
    - Poistaa pääsyoikeudet, kun niitä ei enää tarvita.
    - Pitää lokia pääsyoikeuksista.
- Vahvempaa tai monivaiheista tunnistautumista vaaditaan käyttö- ja pääsyoikeuksille, joihin liittyy korkeampi riski (esim. hallinta- ja ylläpitotunnukset, jaetut tunnukset, etäyhteydet).

4.7. Tilannekuva

Liikenne- ja viestintävirasto suosittelee, että raideliikenteen toimijat määrittävät toiminnot ja käytettävät teknologiat operatiivisen ja kyberturvallisuustiedon keräämiseen, analysointiin, hälytysten nostamiseen, esittämiseen ja hyödyntämiseen tilannekuvan muodostamiseksi organisaation toiminnasta ja kyberturvallisuuden tasosta. Tätä varten toimijan tulisi:

- Kerätä lokitietoja raideliikenteen jatkuvuuden ja turvallisuuden kannalta tärkeistä laitteista, ohjelmistoista ja tietovarannoista.
- Seurata ja analysoida lokien ja muiden lähteiden kautta kerättyä tietoa.
    - Valvoa IT- ja OT-ympäristöjä poikkeavan toiminnan ja mahdollisten kybertapahtumien varalta.
- Määrittää toimintatavat kyberturvallisuuden tilannekuvan luomiseen, ylläpitämiseen ja viestimiseen, joita päivitetään säännöllisesti.
    - Koota yhteen valvontatietoa toimijan operatiivisen tilannekuvan muodostamiseksi.
    - Rikastaa tilannekuvaa organisaation muilla soveltuvilla tiedoilla, kuten visuaalisilla havainnoilla.

4.8. Tapahtumien ja häiriöiden hallinta sekä toiminnan jatkuvuus

Liikenne- ja viestintävirasto suosittelee, että raideliikenteen toimijat määrittävät suunnitelmia, prosesseja ja käytettäviä teknologioita kyberturvallisuuteen liittyvien tapahtumien ja -poikkeamien havaitsemiseksi, analysoimiseksi, niihin vastaamiseksi ja niistä palautumiseksi suhteessa raideliikenteen jatkuvuuteen ja turvallisuuteen kohdistuviin riskeihin. Tätä varten toimijoiden tulisi:

- Määrittää toimintatavat kyberturvallisuustapahtumista ja -poikkeamista ilmoittamiseksi ennalta määritetyille henkilöille tai roolien haltijoille sekä pitää niistä lokia.
- Laatia kriteeristö kyberhäiriöiden määrittämisestä.

    - Analysoida kybertapahtumat siten, että se tukee mahdollisten kyberhäiriöiden määrittämistä.
- Tunnistaa soveltuvat työntekijät ja osoittaa heille roolit kybertapahtumiin ja -häiriöihin reagoimista varten.
    - Reagoida kybertapahtumiin ja -häiriöihin siten, että rajoitetaan toimintoon kohdistuvaa vaikutusta ja palautetaan toiminta normaaliksi.
    - Kyberhäiriöistä raportoidaan Liikenne- ja viestintäviraston Kyberturvallisuuskeskukselle ja raideliikenneyksikölle sekä esimerkiksi L-ISAC ryhmälle.
    - Tietoturvaloukkauksista ja niiden yrityksistä ilmoitetaan poliisille, kun epäillään että kyseessä on rikos.
- 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.
    - Varmuuskopioida tiedot ja testata varmuuskopioita.
    - Tunnistaa varaosia tarvitsevat rautatieliikenteen jatkuvuuden ja turvallisuuden kannalta kriittiset IT- ja OT-laitteet.
- Harjoitella oman organisaation sisällä sekä yhdessä muiden liikennejärjestelmän toimijoiden kanssa jatkuvuussuunnitelmien testaamiseksi, kyberturvallisuustapahtumiin ja -poikkeamiin vastaamiseksi ja haavoittuvuuksien kartoittamiseksi.

4.9. Kumppaniverkoston riskien hallinta

Liikenne- ja viestintävirasto suosittelee, että raideliikenteen toimijat määrittävät toimintatavat toimitusketjun ja ulkoisten riippuvuuksien hallintaan, joilla hallitaan palveluiden ja suojattavien kohteiden ulkopuolisesta tahoista riippuvaisia kyberturvallisuusriskejä suhteessa raideliikenteen jatkuvuuteen ja turvallisuuteen kohdistuviin riskeihin. Tätä varten toimijoiden tulisi:

- Tunnistaa merkittävät kumppaniverkoston IT- ja OT-riippuvuudet, mukaan lukien toimintojen operoinnista vastaavat kumppanit.
    - Tunnistaa kumppaniverkoston toimijat, jotka omistavat, hallinnoivat tai pääsevät muutoin käyttämään toiminnon kannalta tärkeitä laitteita, ohjelmistoja tai tietovarantoja.
- Huomioida osana toimittajien ja muiden kumppaniverkoston toimijoiden valintaa arvio niiden kyberturvallisuuskelpoisuuksista.
- Huomioida tuotteiden ja palveluita valittaessa arvio niiden kyberkyvykkyyksistä.
    - Varmistaa hankittavien järjestelmien turvallisuus asettamalla hankintavaiheessa tarvittavat kyberturvallisuusvaatimukset sekä hankittavalle järjestelmälle että toimittajan kyberturvallisuuden tasolle.
- Huolehtia sopimuksin kumppaniverkoston toimijoiden kyberturvallisuustoimenpiteiden riittävyydestä ja niiden sovittamisesta oman organisaation kyberturvallisuuden toimintamalleihin.
- Osana hyväksyntätestausta kriittisimmät hankittavat laitteet, tietovarannot ja järjestelmät todetaan turvallisuustestauksella turvallisiksi ennen niiden käyttöönottoa.

4.10. Henkilöstön johtaminen ja kehittäminen

Liikenne- ja viestintävirasto suosittelee, että raideliikenteen toimijat määrittävät ja ylläpitävät suunnitelmia, prosesseja, teknologiaa ja kontrolleja toimijan kyberturvallisuuskulttuurin luomiseksi ja sopivan sekä osaavan henkilöstön takaamiseksi suhteessa raideliikenteen toimintavarmuuteen ja turvallisuuteen kohdistuviin riskeihin ja toimijan omiin tavoitteisiin. Tätä varten toimijoiden tulisi:

- Tunnistaa kyberturvallisuuteen liittyvät vastuut ja nimetä organisaation vastuuhenkilön tai -henkilöt.

- Kyberturvallisuuskoulutusta vastuuhenkilöille tarjoamalla varmistaa, että organisaatiossa on sen toiminnan laatuun ja laajuuteen nähden riittävää kyberturvallisuusosaamista, jota ylläpidetään ja kehitetään.
- Varmistaa, että vastuuhenkilöt tuntevat toimijan toiminnalliset ja liikennöintiä koskevat järjestelmät ja ymmärtävät niihin kohdistuvat kyberturvallisuusriskit sekä työskentelevät niiden minimoimiseksi. Vastuuhenkilöt tuntevat kyberturvallisuutta koskevan lainsäädännön ja standardit ja voivat varmistaa niiden riittävän huomioimisen ja noudattamisen organisaatiossa.
- Tunnistaa kyberturvallisuuteen liittyvien tietojen, taitojen ja kykyjen vaatimukset ja niissä mahdollisesti ilmenevät puutteet sekä nykyiset että tulevat tarpeet huomioiden.
- Kouluttaa myös muuta henkilöstöään ja tarvittaessa myös alihankkijoitaan kyberturvallisuuskysymyksistä ja huolehtia organisaation kyberturvallisuustietoisuuden kasvattamisesta.
- Määrittää toimintatavat työntekijöiden ja toimittajien taustatarkastuksiin sekä nimeämiseen sellaisiin tehtäviin, joissa on pääsy raideliikenteen jatkuvuuden ja turvallisuuden kannalta kriittisten palveluiden toimittamiseen liittyviin suojattaviin kohteisiin.
    - Työsuhteen päättymiseen liittyvissä menettelyissä huomioidaan kyberturvallisuus.

4.11. Kyberturvallisuusarkkitehtuuri

Liikenne- ja viestintävirasto suosittelee, että raideliikenteen toimijat luovat ja ylläpitävät rakenteita, joilla ne hallinnoivat ja ohjaavat organisaatioiden kyberturvallisuuskontrolleja, -prosesseja ja muuta kyberturvallisuuden toimintaa suhteessa sekä organisaation omaisuuteen kohdistuviin riskeihin, että organisaation asettamiin tavoitteisiin. Tätä varten toimijoiden tulisi:

- Määrittää kyberturvallisuusarkkitehtuuristrategia kriittisten järjestelmien eheyden ja saatavuuden sekä suojattavan tiedon ympärille kiinnittäen erityistä huomioita turvalaitteiden suunnittelu- ja käyttöperiaatteisiin sekä laitetilojen fyysiseen suojaamiseen ja valvontaan.
- Eriyttää organisaation IT-verkot OT-verkoista esimerkiksi toteuttamalla verkkojen segmentointi sekä arvioida verkkojen kahdentamisen tarve ja toteuttaa tarvittavat verkkojen kahdennukset.
- Käyttää kyberturvallisuuden suojausmekanismeja toiminnan kannalta tärkeille laitteille, yhteyksille, ohjelmistoille ja tietovarannoille.
- Varmistaa korkean prioriteetin laitteissa ja ohjelmistoissa sisäisesti kehitettävien ohjelmistojen ja kolmansien osapuolten ratkaisujen ohjelmistoturvallisuus koko ohjelmistojen elinkaaren ajan ohjelmistojen hankinnasta käytöstä poistoon saakka huolehtien erityisesti, että turvallisen ohjelmistokehityksen periaatteita noudatetaan.
    - Huomioida turvallisen ohjelmistokehityksen periaatteet myös muissa kuin korkean prioriteetin järjestelmissä.
- Toteuttaa arkaluonteisen tiedon suojaaminen käsiteltävän tiedon tunnistamiseen ja luokitteluun perustuen.
    - Huomioida valittujen tietotyyppien osalta myös kaiken muun tiedon suojaaminen.
    - Huomioida valittujen tietotyyppien osalta myös kaiken siirrossa olevan tiedon suojaaminen.

4.12. Yhteistyön lisääminen

Liikenne- ja viestintävirasto suosittelee, että raideliikenteen toimijat tekevät yhteistyötä raideliikennejärjestelmän 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.
- Välittää tietoja kyberturvallisuusuhkista, -riskeistä ja -hyökkäyksistä muille raideliikenteen toimijoille ja yhteistyöverkostoille yhteisen tilannekuvan luomiseksi ja jakamiseksi.
- Levittää hyviä käytäntöjään kyberturvallisuuden kehittämiseksi.
- Vaikuttaa kyberturvallisuussääntelyn hyvään kehittämiseen muun muassa yhteentoimivuuden teknisissä eritelmissä.
- Huolehtia kyberturvallisuuskysymysten esiin nostamisesta organisaatioiden välisissä sopimuksissa ja erilaisilla näköalapaikoilla.

5. Liitteet, lisätietoa ja tiedon lähteitä

Liite 1: Suosituksessa esitetyt kyberturvallisuuden hallintakeinot taulukkomuodossa

Liite 2: Kyberturvallisuuskeskuksen Kybermittari -työkalu, joka sisältää viittauksen tähän suositukseen

Sääntely

- NIS1 direktiivi (https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016L1148&from=FI)
- NIS2 direktiivi (https://eur-lex.europa.eu/legal-content/FI/TXT/?qid=1672915693202&uri=CELEX%3A32022L2555)
- Raideliikennelaki 169 § (https://finlex.fi/fi/laki/ajantasa/2018/20181302#L22P169)
- Laki sähköisen viestinnän palveluista 244 a § (https://finlex.fi/fi/laki/ajantasa/2014/20140917#O9L29P244a)

Kansalliset viranomaiset

- Traficom määräys valmiussuunnittelun järjestämisestä (https://www.traficom.fi/fi/ajankohtaista/uusi-maarays-valmiussuunnittelun-jarjestaminen-liikennejarjestelmassa)
- Traficom ohje raideliikenteen häiriöiden ilmoittamisesta (https://www.traficom.fi/sites/default/files/media/regulation/H%C3%A4iri%C3%B6ilmoitusohje%20valmis.pdf)
- Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen sivut (https://www.kyberturvallisuuskeskus.fi/fi/)
  - Ohjeet ja oppaat (https://www.kyberturvallisuuskeskus.fi/fi/ohjeet)
  - Kybermittari (https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostot/kybermittari)
  - NIS-ilmoituslomake (Ilmoitus tietoturvapoikkeamasta) (https://eservices.traficom.fi/data-services/forms/NISlomake.aspx)
- Valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla (https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f80732d82)
- Digi- ja väestötietoviraston (DVV) Digitaalisen turvallisuuden arkkitehtuurikehys (DTARK) (https://wiki.dvv.fi/display/DTARK/)

Standardointi

- IEC rautatiejärjestelmän kyberturvallisuuden standardointi (https://www.iec.ch/ords/f?p=103:14:319535360914374:::FSP_ORG_ID:28802)
- ISA 62443, Security for Industrial Automation and Control Systems
- CENELEC (https://www.cenelec.eu/)

  - CLC/TS 50701:2021:en Railway applications - Cybersecurity (https://sales.sfs.fi/fi/index/tuotteet/SFSsahko/CENELEC/ID5/5/1012872.html.stx)
- 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 27001:2022:fi Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. (https://online.sfs.fi/fi/index/tuotteet/SFS/ISO/ID5/2/1155761.html.stxISO/IEC 27002)
- SFS-EN ISO/IEC 27002:2022 Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintakeinot. (https://online.sfs.fi/fi/index/tuotteet/SFS/CENISO/ID2/2/1172534.html.stx)
- ISO/IEC 27005, Tietoturvariskien hallinta. (https://sales.sfs.fi/fi/index/tuotteet/SFS/ISO/ID2/2/738504.html.stx)
- Cybersecurity Capability Maturity Model (C2M2) (https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2)

Muita

- Kyberturvallisuussanasto (https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/)
- EU:n Kyberturvallisuusvirasto ENISA:n sivut (https://www.enisa.europa.eu/)
  - Kyberturvallisuuden uhkaympäristö (https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends)
- Euroopan komission julkaisu Liikenteen kyberturvallisuutta koskeva välineistö https://transport.ec.europa.eu/transport-themes/security-safety/cybersecurity_fi
- EU 5G toolbox (https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security)
- Euroopan rautateiden kyberturvallisuutta koskeva tiedonvaihtoryhmä (ER-ISAC) (https://er.isacs.eu/)
- 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)
- Esimerkki bowtie eli rusettianalyysistä (https://www.traficom.fi/sites/default/files/media/file/Guidance for FSTD operators.pdf)
- Cebula, James J. & Young, Lisa R. 2010. A Taxonomy of Operational Cyber Security Risks. Carnegie Mellon University

Hyväksytty 30.1.2023

Kaisa Sainio
Päällikkö

Ville Lahti

Erityisasiantuntija