



Liikenne- ja viestintävirasto

Vuoden 2018 työpajan tulosten kertaus ja työpajatehtävien anto

Jouko Pirttimäki



Liikenne- ja viestintävirasto

Teknisiin järjestelmiin vaikuttaminen

TRL ohjaus

- Kaukosäädin
- Etävalvonta
- Häiriöt

Rautatieyrityksen vaihtotyön ohjaus

Tekniikka

- Akselinlaskijat
- Virtapiirit
- Ajolangat

Liikenteenohjausjärjestelmä lamaantuu ja junaliikenne pysähtyy laajalla alueella

Automaatiologiikoiden näkyminen ulkoverkkoon ja sitä kautta hyökkäys

Joku ottaa veturin haltuun etänä esim. huoltoyhteys

Junan ohjausjärjestelmään pääseminen WiFi:n kautta

18.3.2020



Liikenne- ja viestintävirasto

Ilkivalta

Ilkivalta eri osa-alueilla

Palvelunestohyökkäys lamaannuttaa yhteydet

Viestintäyhteyksien häirintä

Järjestelmien päivitys



Liikenne- ja viestintävirasto

Osapuolten riskit

Teleoperaattorit

- Puhelinyhteydet
- Ulkoisten järjestelmiin vaikuttaminen ja sitä kautta raitainfraan vaikutus
- Palvelutuottajan tietojärjestelmään kohdistetaan tietoturvahyökkäys
- Asetinlaitteelle asennetaan "purkki" ja otetaan se ulkopuolisen ohjaukseen
- Alihankintapalveluntuottaja
- Hyökkäysvektorina ylläpitäjät ja kehittäjät

18.3.2020



Maineriski

Avoimen verkon käyttö

VR-junaverkon käyttäminen ihmisten hakkerointiin



Ylläpitoon liittyvät riskit

Palvelimen tietojen salaaminen johtaa jonkin järjestelmän pysähtymiseen
Kriittisiä tietoja vuotaa tietomurron tai väärän konfiguroidun palvelimen seurauksena



Liikenne- ja viestintävirasto

Inhimilliset uhat

Juna ajautuu väärään paikkaan/väärille raiteille ja aiheutuu vaaratilanne/törmäys

(Kriittisten järjestelmien) käyttäjätunnusten vuotaminen organisaation ulkopuolelle

Ihmisten tietoisuus ja ymmärrys



Liikenne- ja viestintävirasto

Tilojen ja laitteiden riskit

Fyysinen valvonta – valvonnan puute

Valvomattomat laitetilat -> vieraslaitteiden kytkentä

Laitetilan palo yms. Jos pysäyttää tai suuresti häiritsee toimintaa

Saako rikkoutuneiden laitteiden tilalle korvaavaa laitetta kohtuullisessa ajassa? Yhteensopivuus

Järjestelmätekniset riskit

Järjestelmien haavoittuvuudet (sisältä/ulkoa)

Järjestelmien keskinäisriippuvuudet

Verkon segmentointi



Järjestelmiä ei voi noin vain päivittää 24/7 käytön takia
Verkon valvonta löytää poikkeamat verkon käytöstä
Virustorjunnan ajanmukaisuuden puute/päivitys
Toimintakulttuuri ja osaaminen (3)
Organisaation toimintatavat
Puutteellinen tietoturvaohjeistus ja/tai valvonta
Henkilöstön toiminta/osaaminen (kyber)



Sähköinfran haavoittuvuus

Hyökkäyksen seurauksena sähköverkko kaatuu, koko Helsingin/Pasilan alueen liikenne pysähtyy(?)

Sähköverkon lamautuminen ohjauskeskuksessa



Liikenne- ja viestintävirasto

Liikenteenohjausjärjestelmien haavoittuvuudet

Liikenteenhallinnanjärjestelmä jaettu julkiseen verkkoon

Liikenteenohjausjärjestelmä kaatuu palvelunestohyökkäyksen seurauksena.
Liikenne keskeytyy

Tietoliikenneverkon lamauttaminen ohjauskeskuksessa (tietoliikennelaitteet)



Liikenne- ja viestintävirasto

Ohjauslaitteiden hakkerointi

Vaihteiden etäohjaus (sen hakkerointi)

Ohjauslaitteiden hallinta ei-toivotulta taholta

Langattomat ohjauslaitteet

- Onko niitä? (opastimien, vaihteiden)

Baliiseja sorkitaan ja ne lakkaavat toimimasta tietyllä rataosuudella. Liikenne keskeytyy

Huoltoyhteydet asetinlaite- ja kauko-ohjausjärjestelmiin, pääsynhallinta ja yhteyksien suojaus saattavat aiheuttaa riskin(?)

Opastimien, baliisien ja veturilaitteiden yhteydet vikaantuvat (kulunvalvontajärjestelmä), liikenne keskeytyy (?)

Kommunikaatiojärjestelmien lamauttaminen (avisoinnit jne.)

Asetinlaitteiden fyysinen suojaaminen

Asetinlaitteiden sijoittelu ja valvonta puutteellista

Asetinlaitteiden tekniikka vanhaa, saattaa aiheuttaa toiminnallisen riskin (esim. varaosien saatavuus, turvallisuuspuutteet)

18.3.2020



Liikenne- ja viestintävirasto

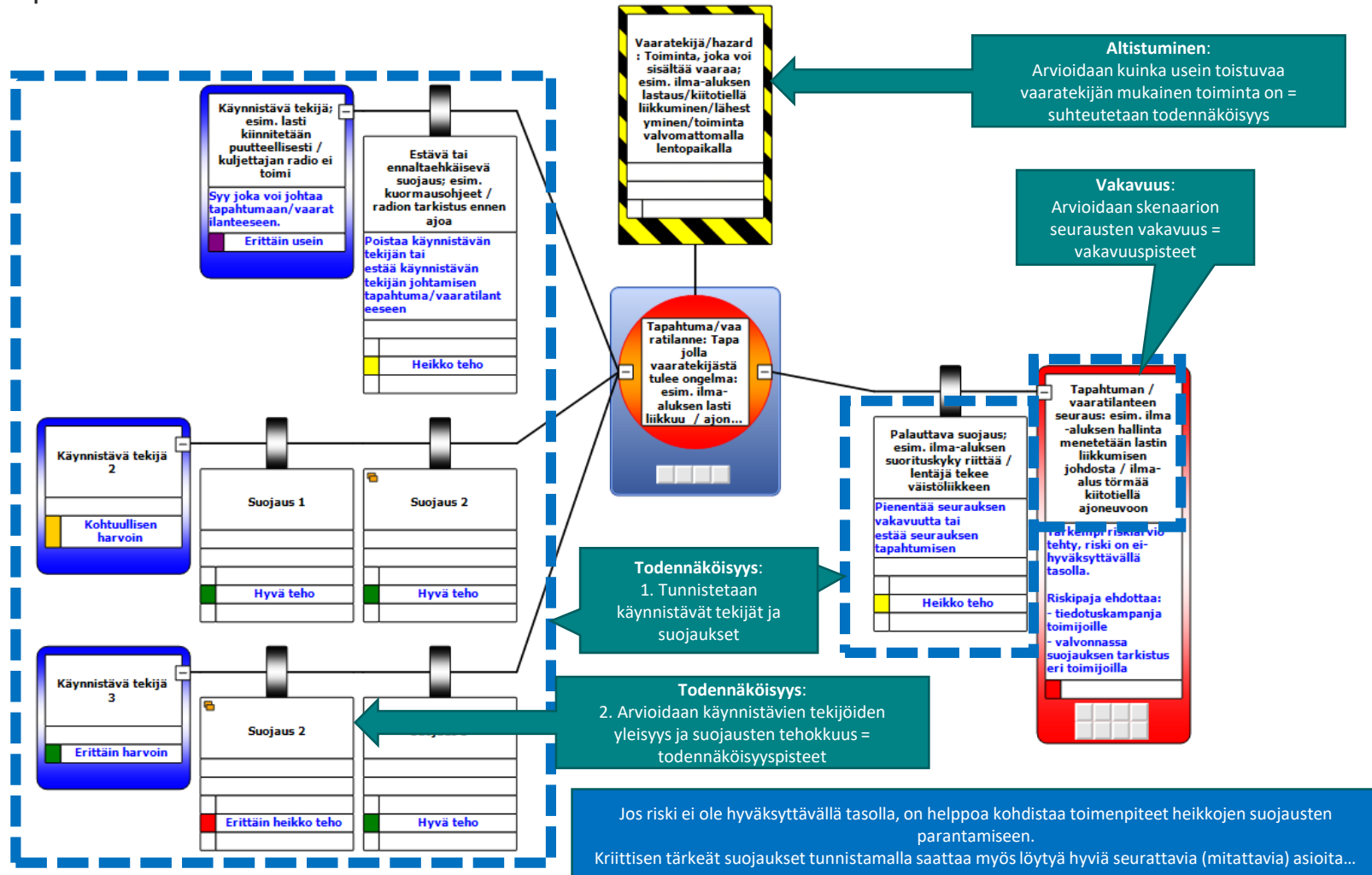
Tietosuoja ja – murrot

Matkustajatietojen haltuunotto (vrt case Frankfurt)

Työpajatehtävät ryhmille

- Miettikää 2 kyberturvallisuushkaa ryhmille jaettavista toiminnoista (ks. seuraava kalvo)
- Kirjatkaa valitsemistanne kyberturvallisuushkista Bowtie-menetelmän mukaisesti ylös:
 - Tapahtuma/Vaaratilanne
 - Käynnistävät tekijät, jotka voivat johtaa tapahtumaan
 - Estävät tai ennaltaehkäisevät suojaukset
 - Palauttavat suojaukset
 - Tapahtuman/vaaratilanteen seuraamukset
- Varautukaa esittelemään tapauksenne päivän päätteeksi
- Aikaa käsittelyyn on 1 h/tapaus ja esittelyyn 5 min/tapaus

Skenaario sijoittuu riskikuvaan vakavuuspisteiden ja todennäköisyyspisteiden perusteella



Ryhmäkohtaiset toiminnot

- **Liikennehallinta ja matkustajainformaatio**
- **Junan sisäiset järjestelmät ja lipunmyyntijärjestelmä**
- **Henkilöstö ja alihankinta**
- **Kyberhyökkäykset**