TRAFICOM
Liikenne- ja viestintävirasto

Työkaluja raideliikenteen kyberturvallisuuteen

18.1.2023 Rata2023

EU komission julkaisu: Liikenteen kyberturvallisuutta koskeva välineistö

- Kohderyhmät:
  - Kaikki raideliikenteen parissa työskentelevät
  - Päätöksentekijät, jotka vastaavat raideliikenteen kyberturvallisuutta
- Ymmärrettävyys: Ei vaadi pohjatietoa kyberturvallisuudesta
- Tarkoitus: Kyberturvallisuustyön aloittaminen.
- Julkaistu 20.7.2021
  - *https://transport.ec.europa.eu/transport-themes/security-safety/cybersecurity_fi*

Peruskäsitteet yksinkertaistettuna

- Tietoturvallisuus = Tiedon saatavuus, eheys ja luottamuksellisuus
- Kyberturvallisuus = Digitaalisen ja verkottuneen organisaation turvallisuutta ja vaikutuksia sen toimintoihin
- Raideliikenteen IT-järjestelmät = tietokoneet ja tietoliikenne, joilla tarkoitus käsitellä tietoa. Esim. sähköposti ja verkkosivut
- OT-järjestelmät = Operatiivisen teknologian ympäristöt, missä laitteet ja ohjelmistot kontrolloivat tai valvovat fyysisiä laitteita. Esim. sähkörata, liikenteenohjauksen kaukokäyttö

Kyberturvallisuuden uhkaympäristö

- Riskienhallinnassa kaikki oleelliset uhkat tulisi huomioida
- Ihmisen ja luonnon aiheuttamat
- Tahalliset ja tahattomat
- Ulkoiset tapahtumat ja sisäpiiri
- Digitaalisen tai fyysisen maailman tapahtuma

Uhka #1: haittaohjelmat

Haitalliset ohjelmistot, jotka voivat vaikuttaa henkilöihin tai organisaatioihin eri liikennemuodoissa

Uhka #2: (hajautettu) palvelunesto

Kyberturvallisuushyökkäys, jolla estetään henkilöitä tai organisaatioita käyttämästä tiettyjä liikennepalveluja ja -resursseja

Uhka #3: luvaton käyttö ja varkaus

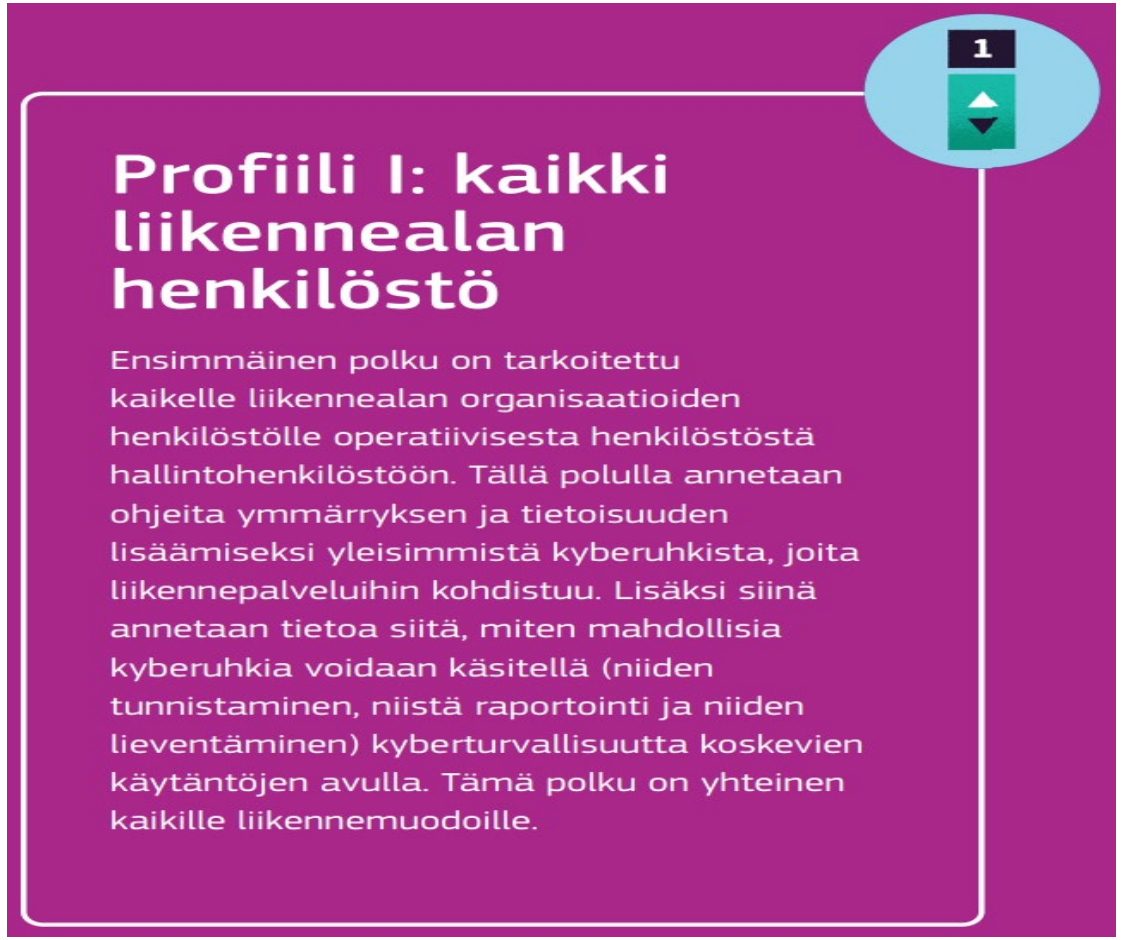
Kriittisten resurssien luvaton käyttö, varastaminen ja hyödyntäminen

Uhka #4: ohjelmistojen manipulointi

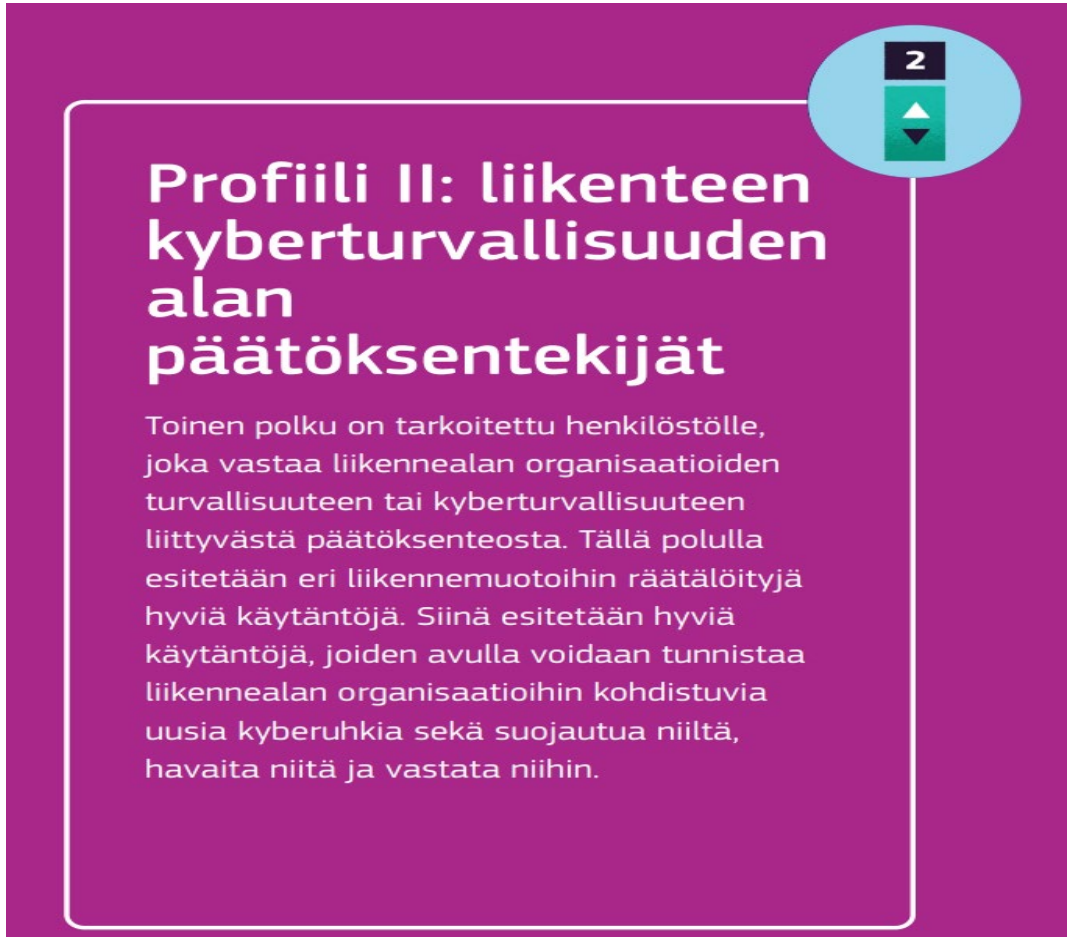
Kyberturvallisuushyökkäys, joka kohdistuu ohjelmistoihin ja jolla pyritään muokkaamaan ohjelmiston toimintaa ja toteuttamaan kohdistettuja hyökkäyksiä

Esimerkkejä kyberturvallisista käytännöistä

- Noudata ohjeita
- Varmuuskopioi
- Suojaa laitteet ja järjestelmät
- Älä avaa odottamattomien sähköpostien liitteitä tai linkkejä
- Pidä asennetut ohjelmistot päivitettyinä



Päätöksentekijät



- Tulee järjestää kyberturvallisuuden johtaminen ja riskienhallinta
- Suojaavia toimenpiteitä toteutetaan
- Uhkia kyetään havaitsemaan
- Poikkeamiin reagoidaan ja niistä palaudutaan suunnitelmallisesti

Päätöksentekijät

- Tulee osoittaa kyberturvallisuudessa johtajuutta ja määrittää hallinto
- Kyberturvallisuuden riskienhallinnan järjestäminen hallintajärjestelmää hyödyntäen
- Kyberuhkilta suojautumisen mitoittaminen riittäväksi ja oikeasuhtaiseksi
- Kyberturvallisuustoimenpiteet pysyvät ajan kuluessa tehokkaina ja merkitykselliset kybertapahtumat havaitaan
- Tulee määrittää, toteuttaa ja testata poikkeamien hallintamenettelyitä, joilla varmistetaan palveluiden ja toimintojen jatkuvuus.

Traficom raideliikenteen kyberturvallisuudessa

- Osaltaan koordinoi, kehittää ja valvoo raideliikenteen kyberturvallisuutta
- Traficomin päivitetty suositus raideliikenteen kyberturvallisuuden edistämisestä julkaistaan tammikuussa 2023
  - Kaikkia organisaatioita suositetaan arvioimaan ja mittaamaan omaa tasoa
  - Suositetaan ylittämään Kyberturvallisuuskeskuksen Kybermittarin tason 1 tai hyödyntämään ISO/IEC 27001:2022 tietoturvallisuuden hallintajärjestelmää
- Traficom yhdessä Maakuljetuspoolin kanssa järjestää toiminnallisen raideliikenteen kyberturvallisuusharjoituksen keväällä 2023.