



TRAFICOM
Liikenne- ja viestintävirasto

Kyberturvallisuus rautateillä

Ratafoorumi 2026
Ville Lahti

Rautateiden kyberturvallisuus

- Mitä on kyberturvallisuus rautateilla?
- Esimerkkejä rautateiden kyberturvallisuuden poikkeamista
- Yhteenveto: Rautateiden kyberturvallisuuden tavoitetilä ja tulevaisuus

Mitä rautateiden kyberturvallisuus tarkoittaa?

- Rautatiejärjestelmä on maanpuolustuksellisesti merkityksellistä kriittistä infrastruktuuria, jota tulee pystyä käyttämään kaikissa oloissa.
- Rautateiden kyberturvallisuudella tarkoitetaan digitaalisten järjestelmien suojaamista kyberuhilta. Uhat voivat olla tahallisia tai tahattomia, ihmisen tai luonnon aiheuttamia.
- Rautateiden kybertoimintaympäristö jaotellaan usein IT- ja OT-järjestelmiin.
 - *Rahat lasketaan IT:llä ja rahat tehdään OT:llä.*
 - Esimerkiksi rautateiden turvalaite- ja kauko-ohjausjärjestelmät sisältäen niiden käyttäjät ja järjestelmiin liittyvät prosessit ja käytännöt muodostavat rautateiden kybertoimintaympäristön.
- Rautateiden jatkuvuudenhallinnalla varmistetaan toiminnan jatkuminen vakavien kyberpoikkeamien aikana ja palaudutaan niistä.

Palvelunestohyökkäykset IT-järjestelmiin

- Venäjämielinen haktivistiverkosto NoName057(16) on kohdistanut laajasti hajautettuja palvelunestohyökkäyksiä (DDoS) Euroopassa.
- Esimerkiksi syys-lokakuussa 2023 väitettyjen hyökkäysten kohteena olivat muun muassa:
 - 11.10. Suomen raide- ja muut liikennetoimijat
 - 8.10. Espanjan liikennesektori mukaan lukien raidetoimijoita
 - 7.10. Suomen raide- ja muut liikennetoimijat
 - 1.10. Iso-Britannian raide- ja liikennetoimijat (ml. West Yorkshire Metro)
 - 28.9. Iso-Britannian raide- ja liikennetoimijat (mm. metrot Newcastle ja Sunderland, Edinburgin raitiovaunut)
 - 24.9. Viron rautatie- ja liikennetoimijat (ml. Viron rautatiet)
 - 23.9. Suomen raide- ja muut liikennetoimijat
 - 21.9. Espanjan raide- ja liikennetoimijat (ml. Espanjan rautatiet ja Valencia metro)
 - 20.9. Viron rautatie- ja liikennetoimijat (ml. Viron rautatiet)
 - 18.9. Suomen raide- ja muut liikennetoimijat
 - 10.9. Ranskan raideliikenne- ja liikennetoimijat (ml. Nizzan raitiovaunut)
 - 10.9. Iso-Britannian rautatietoimija Cross Country
 - 9.9. Viron rautatie- ja liikennetoimijat (ml. EVR)
 - 6.9. Ranskan raideliikenne- ja liikennetoimijat (ml. Eurolines ja Nizzan raitiovaunut)
 - 4.9. Viron rautatie- ja liikennetoimijat (ml. EVR)

Lähteet:
t.me/noname05716

PALVELUNESTOHYÖKKÄYKSET INFORMAATIOVAIKUTTAMISENA

Kybermaailman mielenilmaus

Palveluiden estäminen on usein haktivistien väline hakea **viestilleen huomiota**. Tavoitteena on mahdollisimman laaja näkyvyys.



Kiristyshaittaohjelma rautatieyrityksessä

- Italian rautatieyhtiön (RFI) on Italian valtion omistama rautatieliikenteenharjoittaja ja infrastruktuurin omistaja (16 700 km), joka operoi Italiassa ja muissa EU-jäsenmaissa. Henkilöstö 26 400, liikevaihto n. 2 500 M\$
- RFI keskeytti 23.3.2022 toimipisteissä ja lippuautomaateilla lipunmyynnin epäillyn kiristyshaittaohjelmahyökkäyksen takia. Lipunmyynti verkkokaupassa jatkui normaalisti, mutta päällekkäisiä paikkavarauksia pystyi syntymään. Useat logistiikkayritykset raportoi rautateiden rahtiliikenteessä olleen noin 15 tunnin katkos.
- Vuonna 2025 Italian rautateiden (Ferrovie dello Stato Italiane, FS) tietoja on vuotanut IT-palveluntarjoaja Al mavivaan kohdistuneen tietomurron seurauksena. Hakkeri väittää varastaneensa 2,3 teratavua arkaluonteista dataa.
- Italian FS ja RFI ovat samaa konsernia.

- Lähteet: <https://www.bleepingcomputer.com/news/security/hacker-claims-to-steal-23tb-data-from-italian-rail-group-almaviva/> ; https://eurepoc.eu/table-view/?cyber_incident=5052 ; <https://www.reuters.com/world/us/italys-state-railway-may-have-been-target-cyber-attack-2022-03-23/> ;

Rautatieinfrastruktuurin fyysinen vahingoittaminen

- Saksassa 2022-2023 uutisoitu useista rautateihin liittyvistä tuhopoltoista ja vahingonteoista.
- 8.10.2022 Pohjois-Saksan rautatieliikenne pysähtyi ja katkos kesti noin kolmen tunnin ajan.
 - Deutsche Bahnin mukaan liikenteelle välttämättömiin kaapeleihin tehdyn sabotaasin vuoksi Deutsche Bahnin oli pysäytettävä pohjoisen rautatieliikenne melkein kolmen tunnin ajaksi.
 - DB:n mukaan häiriö ilmeni teknisenä ongelmana, jonka takia junien digitaalisessa radioviestintäjärjestelmässä oli häiriöitä.
 - Häiriö todennäköisesti ilmeni GSM-R radioverkossa, jota käytetään junien ja liikenteenohjauksen väliseen viestiliikenteeseen.
 - Saksan viranomaisten mukaan epäillyn sabotaasin taustalta ei ole löydetty ulkomaista vaikuttamista.

Lähteet:
<https://apnews.com/article/germany-hamburg-railway-fires-disruptionaa38536091fe6e7b4205429b53684f5c>
<https://www.thelocal.de/20231006/german-anti-terror-police-probe-rail-and-geothermal-plant-fires>
<https://www.reuters.com/world/europe/no-sign-that-foreign-state-was-behind-german-rail-sabotage-police-2022-10-09/>
<https://nordot.app/951448228698734592> <https://www.hs.fi/ulkomaat/art-2000009122264.html>
<https://www.dw.com/en/rail-sabotage-police-find-no-signs-of-foreign-interference/a-63385121>
<https://www.spiegel.de/panorama/deutsche-bahn-derzeit-kein-fernverkehr-in-norddeutschland-a-3e03e230-ae20-463d-a91c-da6edfec8bf6>
<https://www.dw.com/en/rail-sabotage-police-find-no-signs-of-foreign-interference/a-63385121>

Kyberpoikkeama ei aina ole tahallinen hyökkäys

- 8/25 Alankomaat rautatieyhtiö NS: **DNS päivityksen virheestä** seurasi, että DNSSEC ei toiminut. Seurauksena oli, että NS:n verkkosivusto, tietyt sovellukset ja lippuautomaatit eivät toimineet.
- 3/22 Puolassa Polskie linjan 33 paikallisesta asetinlaitekeskusta (Lokalnych Centrów Sterowania) 19 lamautui, joka välillisesti vaikutti jopa 80 % Puolan rautatieliikenteestä. Häiriön syynä oli **ohjelmistovirhe**, joka liittyi ohjelmakoodissa kellonajan muodon käsittelyyn. Ohjelmistovirhe korjattiin nopeasti. Laitteiston on toimittanut Alstom -yhtiö (ent. Bombardier).
- 12/23 Puolassa Newag vetureissa havaittiin **tahallisia haitallisia ohjelmakoodin osia**.
 - 1) Veturi ei käynnisty, mikäli se on yli 10 vuorokautta tietyissä koordinaateissa. 2) Ohjelmakoodi tarkastaa veturin komponenttien sarjanumeron ja estää käynnistymisen tarvikevaraosien kanssa. 3) Veturin kompressori määritetään rikkiäiseksi tiettyinä päivämäärinä, vaikka kompressori toimisi normaalisti.
- Lähteet: <https://tweakers.net/nieuws/238400/site-app-en-kaartautomaten-van-ns-liggen-eruit-vermoedelijk-door-migratie.html> ; <https://badcyber.com/dieselgate-but-for-trains-some-heavyweight-hardware-hacking/> ; <https://www.reuters.com/world/europe/technical-fault-halts-polish-railways-key-ukraine-exit-route-2022-03-17/>

Radioteknologian häiriöitä

- 8/23 Puolassa tahallisesti **lähetettiin radiolaitteella "häätä-seis" komentoja**, joka vaikutti noin 20 junaan aikataulusta viivästymisinä. Radioliikenne sisälsi myös Venäjän kansallislaulun ja presidentti Putinin puheen. (GSM-R ei käytössä)
- 9/25 Yhdysvalloissa tavarajunien langaton jarrujärjestelmä on käytössä n. 45 000 veturissa, joista n. **25 000 veturin laitteet ovat haavoittuvia**. Junan keulan ja viimeisen vaunun välisessä AAR S-9152 -protokollassa on heikko todennus, jolloin ohjelmistoradiolla voisi antaa hätäjarrutuksen aloittavan komennon. Haavoittuvuus tunnettu mahdollisesti yli 10 vuoden ajan.
- 8/25 Tietoturvatutkijat julkaisivat useita **TETRA-teknologiaan liittyviä haavoittuvuuksia**. Päivittämättömien tiettyjen laitteiden salausalgoritmi voisi olla murrettavissa, viestintää voisi kuunnella ja tallentaa sekä tuottaa puhetta.
- Lähteet: <https://www.wired.com/story/poland-train-radio-stop-attack/> ; <https://industrialcyber.co/industrial-cyber-attacks/critical-cyber-flaw-linked-to-eot-module-ignored-in-us-rail-systems-for-12-years-fix-not-expected-until-2027/> ; <https://blackhat.com/us-25/briefings/schedule/#2-cops-2-broadcasting-tetra-end-to-end-under-scrutiny-46143>

Venäjän hyökkäyssodan kybervaikutuksia

- 1/22 Valko-Venäjän rautatieverkkoon väitetysti tunkeuduttiin ja asennettiin kiristyshaittaohjelma. Liikenne siirtyi väliaikaisesti osin käsikäyttötilaan. Hyökkäyksen jälkeen julkaistiin aidoksi väitettyjä kuvia varastetuista tiedostoista, varmuuskopioiden formatoinnista ja yhtiön sisäverkon rakenteesta.
- 1/24 Ukrainan tiedustelupalvelu väitetysti lamautti venäläisen junavaunujen hyväksyntä-, rekisteröinti-, kunnossapito- ja romutuspalveluita tarjoavan yrityksen OOO "РЕГИОН-ТРАНС СЕРВИС" serverit (78 kpl) ja työasemat (211 kpl).
- 1/24 Venäjän rautateiden RZD:n Galaxy –palveluun väitetysti murtauduttiin ja 390 virtuaalipalvelimen ja työaseman tiedot tuhottiin.
- 2/25 Venäjän rautateiden työntekijäportaaliin (my.rzd.ru) väitetysti murtauduttu ja 570 000 henkilön tiedot varastettu.
- 3/25 Ukrainan rautateiden lipunmyyntijärjestelmään kohdistui poikkeama, jonka seurauksena lippuja pystyi ostamaan vain fyysisistä myyntipisteistä.

- Lähteet: <https://arstechnicTa.com/information-technology/2022/01/hactivists-say-they-hacked-belarus-rail-system-to-stop-russian-military-buildup/> ; <https://suspijne.media/917837-gur-atakuvalo-rosijskij-regiontransservis-z-ladu-viveli-vsi-serveri/> ; <https://dailydarkweb.net/russian-railways-portal-allegedly-breached-570k-records-exposed/>

Yhteenveto

- Ajatus rautateiden kyberturvallisuuden tavoitetilaksi
 - **Turvallisuus:** Kyberturvallisuus ei vaaranna ihmisten henkeä ja terveyttä. Kyberturvallisuus mahdollistaa turvallisuuskriittisten järjestelmien suunnitellun toiminnan.
 - **Saatavuus:** Digitaaliset järjestelmät ovat koko elinkaaren ajan käytettävissä kaikissa oloissa. Poikkeamat tunnisteen ja palvelut palautuvat hallitusti vajaatoimintatilanteista.
 - **Liiketoiminta:** Kyberturvallisuus tukee yritysten liiketoimintaa ja taloudelliset riskit ovat hallinnassa.
 - **Luottamuksellisuus:** Rautatiejärjestelmän toimijoiden ja asiakkaiden tiedot on suojattu.
- Rautateiden kyberturvallisuus tulevaisuudessa
 - Digitalisaation eteneminen laajentaa hyökkäyspinta-alaa, lisää keskinäisriippuvuutta ja järjestelmien monimutkaisuutta. Mahdollisesti fyysiset uhat vähenevät. Riskitason hallinta edellyttää riittäviä resursseja.
- Huolehdi omasta osaamisesta: Raideliikenteen kyberturvallisuuden verkkokurssi (5 op) ilmaiseksi opiskeltavissa: <https://koulutuskalenteri.xamk.fi/avoimen-amkn-kurssit/raideliikenteen-kyberturvallisuus-nonstop-aloitus-5-op-2/>

Kiitos!

Ville Lahti

Puh. 0295346812

etunimi.sukunimi@traficom.fi

Liikenne- ja viestintävirasto (Traficom)

Maaliikennesektori

Maaliikenteen turvallisuus -yksikkö

