Liikenteenohjausjärjestelmän tietoturva – Cyberuhkat, onko niitä?

> On olemassa vain kahdenlaisia yrityksiä. Sellaisia, joihin on hakkeroitu ja sellaisia, joihin tullaan vielä hakkeroimaan (FBI:n johtaja **Robert Mueller**).

Sami Hyyryläinen
Mipro Oy

Liikenteenohjausjärjestelmät Suomessa ovat kehittyneet voimakkaasti viime vuosina. Perinteiset rautatieliikenteen kauko-ohjausjärjestelmät ovat liittymässä ja integroitumassa koko rataverkon kattavaksi liikenteenhallintajärjestelmäksi. Turvallisuuteen liittyvät liikenteenohjausprosessit ovat siirtymässä entistä lähemmäksi julkisia verkkoja. Tämä muutos kasvattaa järjestelmään kohdistuvaa riskiä altistua tietoturvahaavoittuvaisuuksille ja -uhkille, jotka liittyvät moderneihin tietojärjestelmiin.

Rautatieliikenteenohjaus jakaantuu toiminnallisiin kerroksiin, joissa turvallisuus, käytettävyys ja tietoturvallisuus painottuvat. Turvallisuuskriittisin osuus, asetinlaitejärjestelmä varmistaa junaliikkeiden turvallisen kulun rataverkolla. Suomessa käytössä olevat ns. perinteiset asetinlaitejärjestelmät on hajautettu maantieteellisesti pitkin rataverkkoa. Asetinlaitteet liittyvät infran omistajan tai kaupallisten verkkojen avulla keskitettyihin kauko-ohjausjärjestelmiin. Kauko-ohjausjärjestelmän avulla liikenteenohjaajat ohjaavat junaliikennettä järjestelmän automatiikan avustamana. Alun perin ratakapasiteetin jakoon kehitetty Liike-järjestelmä alijärjestelmineen (liikenteenhallintajärjestelmä) on tänä päivänä tärkeä osa liikenteenohjaajan operatiivista työtä. Liikenteenhallintajärjestelmän avulla hallitaan koko Suomen rataverkkoa muun muassa kaikkien junien aikatauluja. Järjestelmän eri osa-alueita käyttävät lähes kaikki rautatieliikenneprosessin osapuolet. Lisäksi järjestelmä tuottaa tietoa julkisiin rajapintoihin esimerkiksi junien aikataulut.

Liikenteenhallintajärjestelmän rooli kasvaa

Liikenteenohjauksen työ tulee muuttumaan tulevaisuudessa. Viime vuosiin asti liikenteenohjauksen turvallisuuskriittiset prosessit ovat perustuneet liikenteenohjaajan aktiiviseen rooliin turvallisuuden hallinnassa. Junakulkuteiden asetuksesta vastaa liikenteenohjaaja joko manuaalisilla komennoilla tai kauko-ohjausjärjestelmän junanumeroautomatiikan avulla. Turvallisuuskriittinen viestintä juniin ja radalla toimiviin ratatyöyksiköihin on perustunut suurelta osin puheviestintään ja puolimanuaalisiin prosesseihin.

Tulevaisuudessa ja osittain jo tänä päivänä kauko-ohjausjärjestelmät ja liikenteenhallintajärjestelmät tulevat integroitumaan tiiviimmin yhteen. Liikenteenhallintaympäristön työkalut tulevat osallistumaan entistä aktiivisemmin liikenteen operatiiviseen ohjaukseen. Automaation aste ja liikenteen automaattinen optimointi tulevat lisääntymään. Liikenteenohjausten keskittyessä yhdellä järjestelmällä ohjataan entistä suurempia alueita. Häiriöt järjestelmien toiminnassa vaikuttavat isompaan määrään junia ja matkustajia. Turvallisuuden kannalta liikenteenhallintajärjestelmä tulee lähemmäksi ja osaksi turvallisuuskriittisiä toimintoja ja prosesseja, näistä esimerkkinä ratatyön suojaus ja kriittiset rajoitteet rataverkon käytössä (liikenteenohjauksen ilmoitukset).

Haasteena laaja ja hajautettu järjestelmien verkko

Kauko-ohjausjärjestelmästä on perinteisesti ollut vain muutamia rajapintoja liikenteenhallintajärjestelmiin. Kauko-ohjausjärjestelmät ovat ohjanneet rajattua aluetta rataverkolta. Järjestelmän tietoturva on nojannut suurelta osin muista järjestelmistä ja Internetistä täysin eristettyyn järjestelmään ja rajattuun käyttäjäjoukkoon. Järjestelmien laajentuessa, rajapintojen lisääntyessä, käyttäjämäärien kasvaessa tietoturvariskit kasvavat. Kauko-ohjausjärjestelmän suurimmat haasteet liittyvät laajaan ja hajautettuun prosessiin, jossa pitkin rataverkkoa hajautettuna sijaitsevat asetinlaitteet paikallisine ohjauspisteineen liittyvät kaupallisten tietoverkkojen avulla toisiinsa. Infran haltijan on vaikea hallita koko järjestelmän fyysistä tietoturvallisuutta. Tietoliikenneverkkojen ja järjestelmien tietoturvavastuu on hajautettu eri organisaatioiden ja erilaisten sopimusmallien taakse.

Liikenteenhallinnan työkalut (mm. Liike, JETI, Kupla, Ruma) on suunniteltu käytettäviksi hyödyntämään julkisia internetyhteyksiä ja toimimaan erilaisissa laitekokoonpanoissa ja mobiililaitteissa. Käyttäjiä järjestelmillä on useita satoja eri organisaatioissa. Samoilla työasemilla käytetään internetin web-sovelluksia ja sähköpostia. Edellä mainituista syistä johtuen järjestelmät ovat luonnostaan alttiimpia tietoturvauhkille ja haavoittuvuuksille.

Tietoturvauhkien uudet reitit

Liikenteenohjausjärjestelmän kerroksellisuus, hajauttaminen sekä turvallisuuteen liittyvien prosessien perinteiset (manuaaliset) toimintatavat ovat tähän asti minimoineet julkisten verkkojen kautta tulevien uhkien vaikutuksen. Erityisesti ja suoraan rautatiejärjestelmään kohdistuvista sähköisistä hyökkäyksistä ei Suomessa ole ainakaan julkisuudessa kirjoiteltu. Muualta Euroopasta löytyy tunnistettuja murtautumisyrityksiä rautatiejärjestelmiä vastaan. Vaarallisen vian aiheuttaminen turvallisuustoimintoihin vaatii rautatiejärjestelmän syvällistä tuntemusta ja fyysistä pääsyä järjestelmään. Todennäköisempää on, että kunnossapito- tai käyttöhenkilöstö kytkee vahingossa järjestelmän tietoverkkoon ”saastuneen” laitteen, esimerkiksi kannettavan tietokoneen. Virus tai haittaohjelma levitessään voi pahimmassa tapauksessa estää tai rajoittaa järjestelmän käyttöä ja sitä kautta aiheuttaa merkittävää pitkäkestoista häiriötä junaliikenteelle.

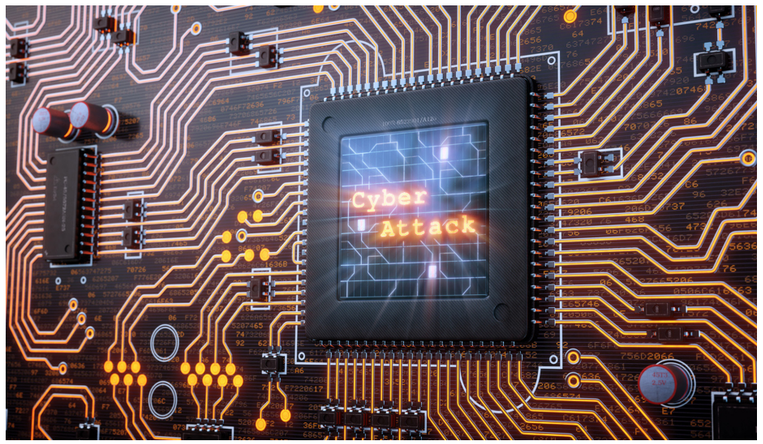
Järjestelmään rakennetun kerroksellisuuden keveneminen uusien rajapintojen myötä sekä turvallisuuteen liittyvien prosessien siirtyminen liikenteenhallintajärjestelmään lähemmäksi avoimia tietoverkkoja kasvattaa riskiä vakaville ja jopa vaarallisille tietoturvapoikkeamille. Yhteys julkiseen verkkoon mahdollistaa erityisesti rautatiejärjestelmään kohdistettujen hyökkäysten toteuttamisen. Todennäköisin uhka on julkisen verkon kautta aiheutettu ns. palvelunestohyökkäys, joka lamauttaa järjestelmän toiminnan joltakin osin tai jopa kokonaan.

Euroopassa nopeasti yleistyvän uuden ERTMS/ETCS (Level 2) liikenteenohjausjärjestelmän käyttöönoton yhteydessä tulee varautua entistä vaarallisempiin uhkiin. Järjestelmässä junan turvalliseen kulkuun liittyvää dataa välitetään GSM-R-verkon välityksellä. Tunkeutuminen järjestelmään terroristisessa tarkoituksessa voisi johtaa vakavaan junaturmaan.

Miten uhkia hallitaan

Rautatiejärjestelmät luokitellaan yhteiskunnan kannalta kriittisiin toimintoihin. Vaatimukset kriittisten järjestelmien tietoturvalle periytyvät EU:n NIS-direktiivin (Directive on security of network and information systems) kautta. Kansallinen toimeenpano ja soveltaminen ovat käynnissä mm. Liikennevirastossa. Rautatiejärjestelmien haasteena ovat järjestelmien monimuotoisuus ja osittain järjestelmien pitkät elinkaaret. Vie vuosia ennen kuin direktiivin mukaiset toiminnot on jalkautettu ja viety eri organisaatioiden järjestelmiin ja organisaatioiden toimintaan. Tämä vaatii erilaisia nykyisistä poikkeavia sopimusmalleja ja päivityksiä nykyisiin järjestelmiin. Tärkeintä on luoda tietoturvan hallinnasta jatkuva prosessi, joka mahdollistaa prosessien ja järjestelmien muuttamisen niiden elinkaaren aikana.

Kauko-ohjausjärjestelmien tietoturva on nojannut suurelta osin muista järjestelmistä ja Internetistä täysin eristettyyn järjestelmään ja rajattuun käyttäjäjoukkoon sekä liikenteenohjaajan aktiiviseen rooliin turvallisuuden hallinnassa.



Turvallisuuteen liittyvät liikenteenohjausprosessit ovat siirtymässä entistä lähemmäksi julkisia verkkoja, mikä lisää liikenteenohjausjärjestelmään kohdistuvaa riskiä altistua tietoturvahaavoittuvaisuuksille ja -uhkille.