TRAFICOM
Finnish Transport and Communications Agency

Finland's approach on Railway Cybersecurity

1.12.2022 ERA & ENISA conference

Content

- What is Finnish Transport and Communications Agency (Traficom)
  - Railway Safety Agency (NSA-FI) and National Cyber Security Centre (NCSC-FI)
- How Traficom understands railway cybersecurity: Resilience
- What we do for railway cybersecurity: Cooperation
- Concreate examples: Guidance and exercise
- How we see the near future: NIS2 and Finland’s Digirail (5G and ERTMS)

Transport and Communications Agency (Traficom)

- National safety authority for railway, aviation, maritime and road transport
  - Railway personnel in total 35 (railway resilience team ~5, railway cybersecurity ~1)
- NIS-directive: Competent authority on transportation
  - Dedicated cyber experts for rail, maritime, aviation and intelligent transport systems
- National Cyber Security Centre (NSCS-FI, CERT/CSIRT, NCSA)
  - Also dedicated experts of logistics cybersecurity

Railway cybersecurity - resilience

- Railway cybersecurity insidents OSINT database:
  - At least 19 publicly reported railway cybersecurity incidents in Europe 2022.
    - Year 2021: Four in Europe, 9 in Europe/G20 countries
  - No direct impacts on safety
  - Economical/reputational impact
  - Mostly ransomware and DDoS, also physical attacks and unintentional deeds
- National legislation (competence)
  - ERA's Safety Management System ~ no cyber (?)
  - NIS1 directive ~ the only national legislation on cyber risk management

Railway cybersecurity by cooperation

- National railway cybersecurity cooperation network
  - Voluntary information sharing based on trust
  - Discussion on cybersecurity incidents
  - Competent authoritys understanding of the cybersecurity maturity level
- Digirail cybersecurity workshops
- Bilateral and international cooperation
  - Traficom has started cooperation with FR, DK, DE, NO, SE and EE.
  - EU Landsec&Railsec, IEC railway applications – cybersecurity, ENISA Transsec(?)
- National Cyber Security Centre (NSCS-FI)
  - Logistic-ISAC, case-by-case support, ER-ISAC

Examples: Guidance and excercise

- Guidance on Railway cybersecurity (non-binding)
  - Threat landscape (general) and OSINT database (specific)
  - Minimum requirements for management of railway cybersecurity
    - National Cybermeter level 1, ISO/IEC 27001:2022 or other int. standard
  - Every organisation should evaluate their maturity
- Finland’s first railway cybersecurity excersise 2022
  - Organised by NSA with zero budget
  - Half a day tabletop excercise
  - 20+ organisations participated on CISO/CSO level
  - Indispensable support from NSCS-FI

Railway cybersecurity – Near future

- 2023-2024 NIS2 directive: The sigle most import piece of cybersecurity regulation
- 2025: IEC railway cybersecurity standard (Cenelec TS50701)
- 2026: Finland's Digirail project: Commercial 5G network, ETCS hybrid level 2-3, ATO GoA2 (semi-automatic)
  - Cybersecurity based on TS50701 (and IEC 62443 series), managed under ISO/IEC 27001:2022 (certified?)
- EU: More cooperation on railway cybersecurity needed
  - Ambiquity and diversity of forums & platforms continue?