CER
The Voice of European Railways

Compendium

Brussels, 26 April 2023

Cybersecurity Resilience Act

CER Compendium on the Cybersecurity Resilience Act

Cyber security and the European railway sector

The Community of European Railway and Infrastructure Companies (CER) brings together close to 70 railway undertakings, their national associations as well as infrastructure managers and vehicle leasing companies. CER members represent 71% of the European railway network length, 76% of the European freight business and 92% of rail passenger operations in Europe. Railways are a potential target of cyber attacks and the railway stakeholders are committed to fulfil their obligations to keep passengers and goods safe, trains protected, and the critical infrastructure secure. The CER members are supportive of sound measures at EU level for the railway stakeholders (both the railway operating community and the rail supply industry) protecting railway systems, networks, and programs from digital attacks.

EU Cyber Resilience Act (CRA)

The European Commission’s proposal for a new Cyber Resilience Act (CRA) aims to safeguard consumers and businesses buying or using products or software with a digital component.
CER highly welcomes the introduction of the CRA and is convinced that it will be a major instrument for increasing the overall cyber security maturity of European infrastructure in general and specifically for railways. CER presented its initial position on the CRA as input to the EC public consultation “Cyber resilience act – new cybersecurity rules for digital products and ancillary services”[1] on 19 January 2023.

Cybersecurity and the railway stakeholders – CRA to include the railway operating community and the rail supply industry

CER has serious concerns excluding the rail supply sector from the CRA. In a highly digitalised world, an overall policy, like CRA, is crucial to maintain a horizontal cyber security baseline for all digital products with sectorial (vertical) legislation as potential add-on . Excluding sectors from the CRA - especially excluding vendors which serve critical infrastructure like railways - will weaken the cyber security resilience of the EU, leaving railways as the **weak link in the cyber security chain of EU’s critical infrastructure. It is important to mention that cyber security attacks on railways can cause massive harm to safety, as safety functions are realised in a digitalised manner.**

[1] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services/F3375669_en

CER sees a lack of adequate implementation of cyber security requirements being in place through existing standards. **For CER, cyber security certification is not yet adequately addressed in existing standards for railways**. Additional legislation is needed to support an adequate level of cyber security in the sector, either by horizontal legislation like the CRA or by extending sectorial (vertical) legislation.

CER acknowledges there will be initial costs for all involved actors to implement such a holistic approach to cyber security. However, the initial costs will be minimal in the long term when compared to all potential consequences of cyber attacks, especially considering railways are already heavily targeted by such attacks from third parties and foreign actors. [2]

Summary

Given the current threat landscape for railways and the fact that foreign threat actors are already preparing & training[3] for large scale cyberattacks on EU critical infrastructure, like railways, power-supplies and water-supplies, no supplier or vendor of digital products shall be excluded from the CRA unless equivalent sectorial legislation is in place.

[2] https://www.spiegel.de/international/world/the-vulkan-files-a-look-inside-putin-s-secret-plans-for-cyber-warfare-a-4324e76f-cb20-4312-96c8-1101c5655236

[3] https://www.spiegel.de/international/world/the-vulkan-files-a-look-inside-putin-s-secret-plans-for-cyber-warfare-a-4324e76f-cb20-4312-96c8-1101c5655236