Whitepaper

Cybersecurity in Public Transport

The Growing Danger of Cyber Threats to Public Transport

At a time when digital networking is revolutionising the transport sector, transport companies are facing an increasing threat from cyber attacks. These invisible threats target not only sensitive data, but also the integrity and security of the entire transportation infrastructure. The resulting challenges faced by transportation companies highlight the urgency of protecting against cyber threats and taking the necessary security measures.

What Cyber Threats is Public Transport Exposed To?

There are various potential threats such as:

Vulnerabilities in Connected Cehicles

Modern means of transportation are increasingly interconnected. Vulnerabilities in these systems could be exploited by attackers to compromise their operations.

Missing Software Updates

If the software in transportation systems is not updated regularly, known security vulnerabilities are an invitation for attacks.

Digital Interfaces

Interfaces to external services and platforms could be gateways for attacks if they are not adequately secured.

Data Theft and Manipulation

Cybercriminals steal personal data in order to analyse them and use them for various reasons, such as for additional attacks, for commercial reasons by selling them on the darknet or by manipulating them. This manipulation may be aimed at causing damage to the victims or disrupting normal business operations..

Ransomware Attacks

The growing prevalence of ransomeware means that transportation companies are increasingly exposed to extortionate attacks that disrupt operations and result in high ransom demands

Physical Security Risks

Cyber attacks can be more than just virtual. The manipulation of traffic signals, switches or other infrastructure elements can cause physical dangers for passengers and staff.

Urgent Need for Action

Media reports regularly cover cyberattacks on public transport infrastructure. The consequences are equally unpleasant for both passengers and operators, damaging public trust in the safety of public transportation.

With the NIS2 Directive and the Cyber Resilience Act (CRA), the EU has obligated member states to enhance the protection of critical infrastructure. Initial reviews of the ICT resilience of critical infrastructure by local authorities indicate that the management of cyber risks must be improved. Waiting is therefore not an option.

How to Protect Yourself and Prevent Potential Risks?

Active Management of Security Risks

The most important measure is the establishment of a proactively implemented Information Security Management System (ISMS). This system defines the technical and organizational measures for actively managing security risks.

Identification, Analysis, and Mitigation of Cyber Risks

Creating an inventory of all ICT systems and analyzing them for cyber risks form the foundation for the security policies and technical measures to be implemented.

Prevention and Training

Through education and training, employees are sensitised to recognising dangers such as social engineering and phishing.

Regular Security Audits

Continuous checks of networks and systems to identify and eliminate potential vulnerabilities.

Emergency Plans and Responsibilities

Precautions in the event of cyber attacks to ensure a rapid response and restoration of operations.

Conclusion

The threat of cyber attacks on transport companies and their infrastructure is real and growing. Only through proactive measures, such as robust cyber security strategy, active risk management and regular checks, can transport companies protect their systems and passengers from the dangers of cyber attacks. Close cooperation within the industry can reduce the necessary resources and costs.

Need for Action and Solution Approaches

In October 2023, onway ag laid the foundation for raising awareness of cybersecurity in public transportation by hosting an event for customers and interested parties. Building on this, we offer workshops in collaboration with our partner Compass Security. These workshops focus on the practical implementation of security policies through an Information Security Management System (ISMS) and the understanding of their impact on operations and processes. Additionally, we provide the necessary domain knowledge for effectively implementing cybersecurity measures in systems, networks, and applications.

onway supports public transport companies in analyzing their cyber risks and implementing and optimizing protective measures. We follow a structured approach: Evaluate, Design, Apply, Control, and Respond. The resulting technical and organizational protection mechanisms align with EN 62443 and TS 50701 and seamlessly integrate into an Information Security Management System (ISMS), such as ISO 27001.

An initiative for security in public transport

- Link to the workshops
- Link to our onway-solution explanation
- Link to security advice «5 steps to a secure »
- Link to the video «The smart solution for the mobile world»
- Link to our partner Compass Security

onway ag | Stauffacherstrasse 16 | 8004 Zurich | Switzerland | phone +41 55 214 18 30 | info@onway.ch | www.onway.ch