We put the security guidelines into context

CySec in Public Transport

Workshop

Cybersecurity in public transport – need for action and solutions

Cybersecurity is becoming increasingly important in public transport. The integrity and availability of data are crucial for smooth operations. Railway companies and infrastructure managers must therefore take measures to protect facilities, systems and vehicles containing information technology systems from unauthorized access and to meet today's requirements.

This requires a clear allocation of responsibilities in the area of cybersecurity, regular security audits and risk-based measures to ensure appropriate information security.

Topics

Companies are facing new challenges, especially when it comes to navigating the complex landscape of cybersecurity issues and regulations. We provide you with an overview.

Processes

Information Security Management System (ISMS) | Security Monitoring | Supplier Management | Dealing with Cloud Service Providers | Business Continuity Management | Employee Management | Asset Management | Roles and Responsibilities | Data protection and Privacy | Access Control

Innovation and Change Management

Requirements for IT and OT measures | Cloud Development Environment (test data) | CI/CD Pipelines (automated software deployment process) | Application Security Tests (DAST/SAST) | Security Checks and CISO Approval | Use of Cryptographic Procedures

Operation of Systems and Network

Availability | Identity Management Authentication | Segmentation/Zoning | Configuration and Change Management | Remote Working | Vulnerability Management | Asset Management | Installation of Software on OT Aystems | System Integrity | Endpoint and OT Device Protection | Monitoring and Security Alerts | Incident Management | Tamper Protection (physical protection) | Penetration Testing

Theoretical concepts are illustrated using demonstrations and practical examples. Participants are actively involved in workshops to develop and implement content based on company scenarios and put them into practice.

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

Aim of the course

We enable you to implement security guidelines through an information security management system (ISMS) and to understand their impact on operations and processes. We also impart the domain knowledge required to implement cybersecurity measures in the areas of systems, networks and applications.

Course preparation

A questionnaire on the topic of 'Cybersecurity in the company' forms the basis for the workshops and the mutual exchange. The time required for this is around 2 to 3 hours.

Prerequisites

This course is held in German. Understanding the basics of ICT is required.

Target audience

Project managers and engineers from the public transport sector who deal with the topic of cyber-security (CySec Rail).

Duration and effort

The course runs over two days, held three weeks apart. Between the course days, participants are given an assignment in which they present the situation in their own company. This is dealt with on the second course day. The time required for preparation is around 1 to 2 hours.

Teaching methods

- Fact-based presentations with storytelling elements
- Edutainment
- Demonstrations
- Workshops
- Cliffhanger exercise (preparation for Day 2)

Speakers

Beat Stettler
Managing Director
onway ag

Ivan Bütler
Cyber Security Specialist
Compass Security AG

Costs

CHF 2450, including course materials, lunch and refreshments during breaks.

Location and time

The course takes place at Compass Security AG on Josefstrasse in Zurich, from 9 a.m. to noon and from 1 p.m. to 5 p.m.

Contact and registration

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

0-04-2026_new