Wir bringen die Security-Richtlinien in einen Kontext

CySec in Public Transport

Workshop

Cybersecurity im ÖV – Handlungsbedarf und Lösungsansätze

Cybersicherheit gewinnt im öffentlichen Verkehr zunehmend an Bedeutung. Die Integrität und Verfügbarkeit von Daten sind von entscheidender Bedeutung für einen reibungslosen Betrieb. Bahnunternehmen und Infrastrukturbetreiber müssen daher Massnahmen ergreifen, um Anlagen, Systeme und Fahrzeuge, die informationstechnologische Systeme beinhalten, vor unerlaubten Zugriffen zu schützen und den heutigen Anforderungen gerecht zu werden. Dies erfordert eine klare Zuweisung von Verantwortlichkeiten im Bereich der Cybersicherheit, regelmässige Sicherheitsaudits sowie risikobasierte Massnahmen zur Gewährleistung angemessener Informationssicherheit.

Themen

Unternehmen stehen vor neuen Herausforderungen, insbesondere in Bezug auf die Navigation durch die komplexe Landschaft von Cybersecurity Themen und Vorschriften. Wir verschaffen Ihnen den Überblick.

Prozesse

Information Security Management System (ISMS) | Security-Monitoring | Lieferanten Management | Umgang mit Cloud-Service-Providern | Business Continuity Management | Mitarbeitermanagement | Asset Management | Rollen und Verantwortlichkeiten | Datenschutz und Privatsphäre | Zugangskontrolle

Innovation und Changemanagement

Anforderungen an IT- und OT-Massnahmen | Cloud-Entwicklungsumgebung (Testdaten) | CI/CD Pipelines (automatisierter Softwarebereitstellungsprozess) | Anwendungssicherheitstests (DAST/SAST) | Sicherheitsüberprüfungen und CISO-Freigabe | Einsatz kryptographischer Verfahren

Betreiben von Systemen und Netzwerk

Verfügbarkeit | Identitätsmanagement/Authentifizierung | Segmentierung/Zonierung | Konfigurations- und Änderungsmanagement | Remote-Arbeit | Schwachstellenmanagement | Asset Management | Installation von Software auf OT-Systemen | Systemintegrität | Schutz von End- und OT-Geräten | Überwachung und Sicherheitswarnungen | Incident Management | Manipulationssicherheit (physischer Schutz) | Penetrationstests

Anhand von Demonstrationen und Praxisbeispielen werden theoretische Konzepte veranschaulicht. Teilnehmer werden aktiv in Workshops eingebunden, um Inhalte anhand von Unternehmensszenarien zu erarbeiten und umzusetzen.

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

Ziel der Schulung

Wir befähigen Sie, Security-Richtlinien durch ein Informationssicherheitsmanagementsystem (ISMS) zu realisieren und deren Auswirkungen auf Betrieb und Prozesse zu verstehen. Zudem vermitteln wir das erforderliche Domänenwissen zur Umsetzung von Cybersecurity-Massnahmen in den Bereichen Systeme, Netzwerke und Anwendungen.

Kursvorbereitung

Ein Fragebogen zur Thematik «Cybersecurity im Unternehmen» bildet die Grundlage für die Workshops und den gegenseitigen Austausch. Der Zeitaufwand dafür ist etwa 2 bis 3 Stunden.

Voraussetzungen

ICT-Grundlagenwissen.

Zielgruppe

Projektleiter und Ingenieure aus dem öffentlichen Verkehr, die sich mit dem Thema Cybersecurity (CySec Rail) beschäftigen.

Dauer und Aufwand

Der Kurs umfasst zwei Tage, die im Abstand von drei Wochen stattfinden. Zwischen den Kurstagen erhalten die Teilnehmenden eine Aufgabe, bei der sie die Situation im eigenen Unternehmen einbringen. Am zweiten Tag des Kurses wird dies behandelt. Der Zeitaufwand für die Vorbereitung liegt bei rund 1 bis 2 Stunden.

Unterrichtsmethoden

- Faktenbasierte Referate mit Storytelling-Elementen
- Edutainment
- Demonstrationen
- Workshops
- Cliffhanger-Aufgabe (Vorbereitung auf Tag 2)

Referenten

Beat Stettler
Managing Director
onway ag

Ivan Bütler
Cyber Security Spezialist
Compass Security AG

Kosten

CHF 2450, inklusive Unterrichtsmaterial, Mittagessen und Pausenverpflegungen.

Durchführungsort und -zeiten

Der Kurs findet bei Compass Security AG an der Josefstrasse in Zürich statt, jeweils von 9 bis 12 Uhr und von 13 bis 17 Uhr.

Kontakt und Anmeldung

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