

rethinking
software.



1-Tages-Workshop:

Cyber Security Resilienz in der Bahnwelt

Cyberattacken können immense Schäden anrichten. Die Folgen können von Betriebsstörungen oder -ausfällen über Datenverlust bis zu Sicherheitsrisiken für Bahnbetriebe reichen. Um dem Risiko von Cyberattacken zu begegnen, ist eine systematische Herangehensweise an das Thema **IT-/OT-Security** dringend empfohlen. Für kritische Infrastrukturen gemäß Kritis-Verordnung sowie gemäss des EU weiten Cyber Resilience Acts (kurz CRA) sieht das Gesetz Mindestsicherheitsstandards für die Umsetzung vor. Weitergehende Normen zur Cyber Security aus der Industrie und Bahnwelt (EN50126, TS50701 und IEC62443) befassen sich bereits konkret zur Umsetzung dazu.

Unser **1-Tages-Workshop „Cyber Security Resilienz in der Bahnwelt“** richtet sich an **Fachkräfte in der Bahnindustrie**. Wir zeigen Ihnen einen Einblick in die Materie, um Ihnen bei der Umsetzung zu helfen und bieten jede Menge Raum für Ihre Fragen.

Das erwartet Sie unter anderem:

Überblick über den CRA

Dokumentation und Meldepflichten

Lifecycle- und Schwachstellenmanagement

Intended Use, Threat Modelling, Risikomanagement
und die Security Requirements

Wann: 26. Februar 2026

Wo: Eisenbahnbetriebslabor Schweiz AG, Überlandstrasse
271, 8600 Dübendorf

Preis: 650CHF pro Teilnehmenden

Anmeldung: an thomas.eichmann@infoteam-software.ch

* Für detailliertes Programm siehe nächste Seite



infoteam Software AG

Thomas Eichmann

Telefon: +41 79 420 70 94

thomas.eichmann@infoteam-software.ch

<https://infoteam.de/unsere-maerkte/transportation>

Weitere Infos zum Thema Cybersecurity

<https://infoteam.de/unsere-know-how/cyber-security>



Zeit	Abschnitt	Ausgewählte Fragestellungen
08:45	Vorstellung und Einstieg in das Thema (Einstieg mit UseCase an der EBL-Anlage)	
09:30 - 11:15	CRA Überblick und gesetzliche Vorgaben	Was ist der CRA (Cyber Resilience Act)? Warum wird CRA eingeführt? Welche gesetzlichen Anforderungen gibt es? Welche Anforderungen stellt CRA an die Dokumentation und Supply Chain? Welche Melde- und Zeitfristen gelten? Welche zusätzlichen Anforderungen stellt der CRA an System-Integrator und Komponenten-Hersteller?
Pause		
11:30 - 12:30	Intended Use, Security-Architektur	Was muss ich vor wem Schützen? Was hat es mit Zones & Conduits auf sich? Warum hilft mir der CRA Zeit und Geld zu sparen? Warum State of the Art?
Steh-Lunch		
13:15 - 15:00	Threat Modelling und Risikomanagement	Wie lassen sich durch Threat Modelling Sicherheitsschwachstellen schon in der Planungsphase erkennen? Wie kann ich mit Cyber Security Risk Assessment die wahren Schwachstellen erkennen und Gegenmaßnahmen ergreifen?
	Entwicklung	Was macht das Defense-in-Depth-Prinzip so wirkungsvoll? Wie kann Secure-by-Design dazu beitragen, Sicherheitslücken zu vermeiden und Kosten zu sparen? Welche Systemcharakteristika beeinflussen die Sicherheit von Anfang an? Warum sind Security Requirements und Bad User Storys für den Schutz von Software entscheidend?
Zusammenfassung des Themenblocks		
Pause		
15:15 - 16:30	Lifecycle- und Schwachstellenmanagement, Meldepflichten	Was ändert sich durch den CRA am Lifecycle Management? Warum Schwachstellenmanagement so wichtig ist? Was hat das mit Supply Chain zu tun? Was und warum soll ich Melden? Muss ich mein Qualitätsmanagement anpassen?
Zusammenfassung		
Anschließend: Aperó & Austausch an der EBL Anlage		



infoteam Software AG

Thomas Eichmann
 Telefon: +41 79 420 70 94
 thomas.eichmann@infoteam-software.ch
<https://infoteam.de/unsere-maerkte/transportation>

Weitere Infos zum Thema Cybersecurity

<https://infoteam.de/unsere-know-how/cyber-security>

