Whitepaper

Cybersicherheit im ÖV

Die wachsende Gefahr von Cyberbedrohungen für den öffentlichen Verkehr

In einer Zeit, in der die digitale Vernetzung den Verkehrssektor revolutioniert, sind Verkehrsunternehmen einer zunehmenden Bedrohung durch Cyberangriffe ausgesetzt. Diese unsichtbaren Gefahren zielen nicht nur auf sensible Daten, sondern auch auf die Integrität und Sicherheit der gesamten Verkehrsinfrastruktur. Die daraus resultierenden Herausforderungen, mit denen Verkehrsunternehmen konfrontiert sind, zeigen auf, wie dringend es ist, sich gegen Cyberbedrohungen zu schützen und die erforderlichen Sicherheitsmassnahmen zu ergreifen.

Welchen Cybergefahren ist der öffentliche Verkehr ausgesetzt?

Es lauern verschiedene potenzielle Bedrohungen wie zum Beispiel:

Schwachstellen in vernetzten Fahrzeugen
Moderne Verkehrsmittel sind zunehmend vernetzt. Schwachstellen in diesen Systemen könnten von Angreifenden ausgenutzt werden, um den Betrieb zu beeinträchtigen.

Fehlende Software-Updates
Wenn Software in Verkehrssystemen nicht regelmässig aktualisiert wird, sind bekannte Sicherheitslücken eine Einladung für Angriffe.

Digitale Schnittstellen
Nicht ausreichend gesicherte Schnittstellen zu externen Diensten und Plattformen könnten Einfallstore für Angriffe darstellen.

Datenklau und -manipulation
Cyberkriminelle entwenden persönliche Daten, um sie zu analysieren und beispielsweise für zusätzliche Angriffe zu nutzen, im Darknet zu veräussern oder zu manipulieren. Diese Manipulation kann darauf abzielen, Schaden bei den Opfern anzurichten oder den normalen Betriebsablauf zu stören.

Ransomware-Angriffe

Die steigende Verbreitung von Ransomware bedeutet, dass Verkehrsunternehmen zunehmend erpresserischen Angriffen ausgesetzt sind, die den Betrieb beeinträchtigen und hohe Lösegeld-forderungen mit sich bringen.

Physische Sicherheitsrisiken

Cyberangriffe können nicht nur virtuell sein. Die Manipulation von Verkehrssignalen, Weichen oder anderen Infrastrukturelementen kann physische Gefahren für Passagiere und Personal verursachen.

Dringender Handlungsbedarf

Medien berichten regelmässig über Cyberangriffe auf Infrastrukturen des öffentlichen Verkehrs. Die Auswirkungen sind für Passagiere wie Betreiber gleichermassen unangenehm und schaden dem Vertrauen der Bevölkerung in die Sicherheit des öffentlichen Verkehrs.

Die EU hat mit der NIS2-Directive und mit dem Cyber Resilience Act (CRA) die Mitgliedstaaten verpflichtet, für einen besseren Schutz kritischer Infrastrukturen zu sorgen. Erste Überprüfung der IKT-Resilienz kritischer Infrastrukturen durch lokale Stellen zeigen auf, dass das Management von Cyber-Risiken verbessert werden muss. Abwarten ist daher keine Option.

Wie schützt man sich und wie kann man potenziellen Risiken vorbeugen?

Aktives Managen der Sicherheitsrisiken

Wichtigste Massnahme ist der Aufbau eines aktiv gelebten Information Security Management System (ISMS). Dieses definiert die technischen und organisatorischen Massnahmen zum aktiven Managen von Sicherheitsrisiken.

Identifikation, Analyse und Minderung von Cyber-Risiken

Die Erstellung eines Inventars aller IKT-Systeme und deren Analyse auf Cyberrisiken bilden die Grundlage für die einzuführenden Sicherheitsvorgaben und technischen Massnahmen.

Prävention und Schulung

Durch die Aufklärung und Schulung werden Mitarbeitende auf die Erkennung von Gefahren, wie zum Beispiel Social-Engineering und Phishing, sensibilisiert.

Regelmässige Sicherheitsaudits

Kontinuierliche Überprüfungen der Netzwerke und Systeme, um potenzielle Schwachstellen zu identifizieren und zu beheben.

Notfallpläne und Verantwortlichkeiten

Vorkehrungen für den Fall von Cyberangriffen, um eine schnelle Reaktion und Wiederherstellung des Betriebs zu gewährleisten.

Fazit

Die Bedrohung durch Cyberangriffe auf Verkehrsunternehmen und ihre Infrastruktur ist real und wächst. Nur durch proaktive Massnahmen, wie unter anderem eine robuste Cybersicherheitsstrategie, ein gelebtes Risikomanagement und regelmässige Überprüfungen, können Verkehrsunternehmen ihre Systeme und Passagiere vor den Gefahren von Cyberattacken schützen. Durch eine enge Zusammenarbeit innerhalb der Branche können die dazu nötigen Ressourcen und Kosten reduziert werden.

Handlungsbedarf und Lösungsansätze

Die onway ag hat im Oktober 2023 den Grundstein für die Sensibilisierung im Bereich Cybersicherheit im öffentlichen Verkehr mit einem Event für Kunden und Interessierte gelegt. Weiterführend bieten wir in Zusammenarbeit mit unserem Partner Compass Security Workshops an. Im Fokus steht hier die praxisnahe Umsetzung von Security-Richtlinien durch ein Information Security Management System (ISMS) sowie das Verständnis der Auswirkungen auf Betrieb und Prozesse. Zudem vermitteln wir das erforderliche Domänenwissen zur effektiven Umsetzung von Cybersicherheitsmassnahmen in den Bereichen Systeme, Netzwerke und Anwendungen.

onway unterstützt Unternehmen des öffentlichen Verkehrs bei der Analyse ihrer Cyber-Risiken und der Implementierung und Optimierung von Schutzmassnahmen. Dabei verfolgen wir einen strukturierten Ansatz: Evaluate, Design, Apply, Control und Respond. Die daraus resultierenden technischen und organisatorischen Schutzmechanismen sind angelehnt an EN 62443 sowie TS 50701 und integrieren sich ebenso nahtlos in ein Information Security Management System (ISMS), z.B. nach ISO 27001.

Eine Initiative für die Sicherheit im öffentlichen Verkehr

- Link zu unseren Workshops
- Link zur Erklärung der onway-Lösung
- Link zu Security-Beratung «5 Schritte zu einer sicheren Infrastruktur»
- Link zum Video «Die smarte Lösung für die mobile Welt»
- Link zu unserem Partner Compass Security

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