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 Lösegeldforderungen 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.

Was macht Verkehrsunternehmen und deren Infrastruktur angreifbar und warum stehen sie im Fokus?

Digitale Transformation

Die zunehmende Integration von IoT und digitalen Technologien macht den Verkehrssektor anfälliger für Cyberangriffe, da mehr Angriffspunkte und damit potenzielle Schwachstellen entstehen.

Hohe Abhängigkeit von Automatisierung

Moderne Verkehrssysteme setzen stark auf Automatisierung, was die Abhängigkeit von digitalen Steuerungen erhöht und gleichzeitig das Risiko von Angriffen auf diese Systeme verstärkt.

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

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 mit ihrem Event im Oktober 2023 den Grundstein für die Sensibilisierung im Bereich Cybersicherheit im öffentlichen Verkehr für Kunden und Interessierte gelegt.

Ab 2024 bietet das Unternehmen in Zusammenarbeit mit seinem Partner Compass Security Workshops an. Im Fokus der ersten Schulungen steht die praxisnahe Umsetzung von Security-Richtlinien durch ein «Information Security Management System (ISMS)» sowie das Verständnis der Auswirkungen auf Betrieb und Prozesse. Der Workshop vermittelt zudem das erforderliche Domänenwissen zur effektiven Umsetzung von Cybersicherheitsmassnahmen in den Bereichen Systeme, Netzwerke und Anwendungen. Für die zweite Hälfte 2024 ist ein weiterführender Workshop geplant.

Eine Initiative für die Sicherheit im öffentlichen Verkehr

- Link zum Workshop und Flyer
- Link zur Erklärung der onway-Lösung
- 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