Authentifizierungsmanagement im Bordnetzwerk eines Triebzuges

Studiengang: MAS Cyber Security

Die Anforderungen an die IT- und OT-Infrastruktur moderner Personenzüge sind in den letzten Jahren stark gewachsen. Mit zunehmender Vernetzung der Züge steigen auch die Anforderungen an die Cyber Security an Bord. Ein wichtiger Teil davon ist das Authentifizierungsmanagement: Wie wird sichergestellt, dass nur berechtigte Personen Zugriff auf die Netzwerke an Bord erhalten?

Ausgangslage

Die Bahnreisenden möchten in Echtzeit über ihre Anschlussverbindungen am Zielbahnhof informiert sein. Auf der anderen Seite möchte man dem Unterhaltspersonal auch aus der Ferne Zugriff auf aktuelle Diagnosedaten der Fahrzeuge ermöglichen. Damit können die Lokführerinnen und Lokführer bei einer Störung schon am Telefon optimal unterstützt werden. Beides erfordert neben der klassischen Fahrzeugsteuerung (OT) auch eine umfangreiche IT-Infrastruktur an Bord. Ans fahrzeuginterne Ethernet-Netzwerk sind bei einem modernen Triebzug etwa 70 bis 100 Geräte angeschlossen, Tendenz steigend. Das Bundesamt für Verkehr hat auf diese Entwicklung reagiert und im Juli 2024 die Richtlinie Cybersicherheit Eisenbahn in Kraft gesetzt.

Problemstellung

Die Richtlinie verlangt ein striktes Identifikations- und Authentifizierungsmanagement für alle Arbeiten, welche nicht während des kommerziellen Betriebs ausgeführt werden. Dies sind insbesondere Änderungen an Softwarekonfigurationen oder Parametern. Mit dieser Masterthesis sollen die Grundlagen geschaffen werden, um ein Identifizierungs- und Authentifizierungssystem an Bord von Eisenbahnfahrzeugen einzuführen. Die angestrebte Lösung ergänzt die bisherigen Sicherheitsmassnahmen. Dabei muss beachtet werden, dass die Lösung für kleine und mittelgrosse Bahnunternehmen umsetzbar ist, welche nicht über die Strukturen und Ressourcen eines Grosskonzerns verfügen.

Vorgehen

Im ersten Schritt wird in Erfahrung gebracht, ob andere Eisenbahnverkehrsunternehmen bereits Authentifizierungslösungen umgesetzt haben und wie die Unternehmen planen, diese Anforderung der Richtlinie Cybersicherheit Eisenbahn umzusetzen. Dazu werden Interviews mit den verantwortlichen Fachleuten anderer Bahnunternehmen geführt. Als nächstes werden die Anforderungen an ein Identifizierungs- und Authentifizierungssystem definiert. Dabei wird auch die Usability mit einbezogen: Um eine gute Akzeptanz beim Personal zu erreichen, muss das System einfach bedienbar sein und zuverlässig funktionieren. Damit dies erreicht werden kann, müssen entsprechende Rückfallebenen vorgesehen werden. Anschliessend wird ein Konzept erstellt, wie das Identifizierungs- und Authentifizierungssystem umgesetzt werden kann. Das Konzept wird gemäss der Norm CLC/TS 50701 „Bahnanwendungen - Cybersecurity“ aufgebaut.

David Bellwald

Ergebnisse

Das erarbeitete Konzept basiert auf der Verwendung von bereits im Unternehmen vorhandenen Chipkarten des Schliesssystems. Die Identitäten, Rollen und Berechtigungen werden von der zentralen Verwaltung automatisiert auf die Fahrzeuge provisioniert. Im Gegenzug werden Logdaten vom Fahrzeug an die zentrale Datenbank übermittelt. Der fahrzeugseitige Teil des Systems stellt sicher, dass die Authentifizierung auch bei einem Unterbruch der Mobilfunkverbindung zur zentralen Infrastruktur funktioniert. Die Berechtigungen und gewisse Stammdaten der angemeldeten Person (wie z.B. Name und Personalnummer) werden an die Fahrzeugsteuerung weitergegeben.

Ausblick

Nach Abschluss der Masterthesis muss sich das erarbeitete Konzept in einem Proof of Concept beweisen. Falls nötig, können noch Optimierungen eingebracht werden. Verläuft dies erfolgreich, wird das Identifizierungs- und Authentifizierungssystem etappenweise in die Fahrzeugflotten integriert.