



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr,
Energie und Kommunikation UVEK
Bundesamt für Verkehr BAV
Abteilung Sicherheit

CH-3003 Bern BAV

Per E-Mail

An die Eisenbahnunternehmen

Aktenzeichen: BAV-041.4-3/11/3/8/1/25/1/3

Ittigen, 23. April 2025

Cloud Computing für Eisenbahnanwendungen

Sehr geehrte Damen und Herren

Aufgrund der rasant fortschreitenden technologischen Entwicklung und Digitalisierung gewinnt Cloud Computing¹ auch im Eisenbahnbereich zunehmend an Bedeutung.

Die Auslagerung von Anwendungen und Daten in die Cloud ermöglicht unter anderem eine hohe Flexibilität und Skalierbarkeit bei geringen Investitionskosten. Dem steht jedoch ein weitgehender Kontroll- und Souveränitätsverlust gegenüber. Beim Einsatz von Cloud Computing für Eisenbahnanwendungen², d.h. technische Systeme mit Relevanz für den Eisenbahnbetrieb, ist eine sorgfältige Abwägung der Vor- und Nachteile unabdingbar.

Die heutigen hoheitlichen Vorgaben³ regeln den Einsatz von Cloud Computing nicht explizit, stellen aber generelle Anforderungen an die Verfügbarkeit und die Zuverlässigkeit, die Instandhaltbarkeit, die Sicherheit (Safety und Security) und an die Wirtschaftlichkeit der Eisenbahnanwendungen. Werden diese Anforderungen über den gesamten Lebenszyklus einer Anwendung nachweislich erfüllt, ist Cloud Computing grundsätzlich zulässig.

Ziel dieses Schreibens ist es, die Eisenbahnunternehmen für die Notwendigkeit eines bewussten Umgangs mit Cloud Computing zu sensibilisieren. Zu diesem Zweck werden die oben genannten hoheitlichen Vorgaben in den folgenden Abschnitten in Form eines allgemeinen Grundsatzes und detaillierter Anforderungen konkretisiert.

¹ Mit Cloud Computing werden Computerressourcen (Datenspeicher, Rechenleistung und/oder Software) bezeichnet, die «as a Service» durch einen externen Serviceprovider zur Verfügung gestellt werden.

² In der Norm SN EN 50126-1 werden folgende Bereiche den Bahnanwendungen zugeordnet: Zugsteuerung, Zugsicherung und Signalgebung (Signaltechnik), Bahnfahrzeuge und Stromversorgung für die Bahn (ortsfeste Anlagen). Im vorliegenden Dokument wird der Begriff Bahnanwendungen für alle Systeme verwendet, die Einfluss auf den Bahnbetrieb haben.

³ Unter anderem [Eisenbahnverordnung \(EBV\)](#) und [Ausführungsbestimmungen zur Eisenbahnverordnung \(AB-EBV\)](#).



Allgemeiner Grundsatz

Cloud Computing darf in einer Eisenbahnanwendung erst eingesetzt werden, nachdem das Risiko «Ausfall der Cloud mit betriebs- oder sicherheitsrelevanten Folgen» untersucht wurde.

Diese Untersuchung umfasst:

- die Bestimmung des Risikos solcher Ausfälle, indem ihre qualitative Wahrscheinlichkeit⁴ und ihr Ausmass betrachtet werden und
- die Bewertung dieses Risikos einschliesslich seiner bewussten Akzeptanz durch das Eisenbahnternehmen.

Detailanforderungen

- [Cloud-1] Szenarien über Vorfälle in **der Cloud mit sicherheits- oder verfügbarkeitsrelevanten Auswirkungen auf den Bahnbetrieb** sind systematisch zu identifizieren. Dabei sind insbesondere die folgenden Ursachen unter **Einbezug der ganzen Lieferkette** zu berücksichtigen (siehe auch [Richtlinie Cybersicherheit Eisenbahn](#), Control B-09 Business Continuity Management und B-18 Schutz der Daten und Informationen):
- Technisch bedingte Ausfälle (stochastische Ausfälle, systematische Fehler);
 - Ausfälle auf Grund von Fehlhandlungen (Betrieb, Instandhaltung);
 - Cybervorfälle (inklusive Sabotage mittels Datenmanipulation und Insiderattacken);
 - Mutwilliger Serviceunterbruch durch den Service Provider, z.B. auf Befehl einer politischen Instanz.
- [Cloud-2] **Wahrscheinlichkeit** (qualitativ) **und Ausmass** (Dauer, Auswirkungen für den Bahnbetrieb und allgemein für das Unternehmen) **dieser Vorfälle** sind zu bestimmen. Dabei sind auch die Rückwirkungen auf andere Systeme zu berücksichtigen.
- [Cloud-3] In Hinblick auf die Akzeptanz des Restrisikos sind **Kompensationsmaßnahmen** (Rückfalllebenen, die innert einer nützlichen Frist zum Einsatz kommen) zur Sicherstellung eines vollen oder reduzierten Bahnbetriebs zu untersuchen (siehe auch [Richtlinie Cybersicherheit Eisenbahn](#), Control B-09 Business Continuity Management).
- [Cloud-4] Unter **Berücksichtigung der Systemrelevanz** des Unternehmens ist zu bewerten, ob das Restrisiko akzeptiert werden kann.
- [Cloud-5] **Der Entscheid über den Einsatz einer Cloud hat**, basierend auf der gemäss [Cloud-1] bis [Cloud-4] durchgeführten Risikobewertung, **durch eine dafür geeignete Instanz des Unternehmens zu erfolgen**. Dieser Entscheid ist periodisch und bei relevanten Änderungen zu prüfen (siehe auch [Richtlinie Cybersicherheit Eisenbahn](#), Control B-06 Massnahmen im Bereich Cloud).
- [Cloud-6] Die Anforderungen an die Cloud sowohl funktionaler, wie auch nicht funktionaler Art (z.B. Prozesse für die Meldung von Vorfällen) sind festzulegen und vertraglich mit dem Service Provider festzuhalten (siehe auch [Richtlinie Cybersicherheit Eisenbahn](#), Control B-04 Lieferantenmanagement und B-20 Schwachstellenmanagement).
- [Cloud-7] Die Risikobewertung und der Entscheid müssen dokumentiert und dem BAV im Rahmen von Verfahren oder auf Verlangen zur Verfügung gestellt werden.

⁴ Im Bereich der Cybersicherheit ist es in der Regel nicht möglich, die Eintrittswahrscheinlichkeit eines Ereignisses zu quantifizieren. In den Cybersicherheits-Normen im Eisenbahnbereich bezeichnet der englische Begriff «Likelihood» eine nur qualitativ oder semiquantitativ abgeschätzte Wahrscheinlichkeit.

- [Cloud-8] Die Zweckmässigkeit einer Aufnahme des Prozesses der Risikobewertung im Zusammenhang mit Clouds ins Managementsystem des Eisenbahnunternehmens ist zu prüfen.
- [Cloud-9] Eine ausführliche Übersicht über alle durch das Eisenbahnunternehmen verwendeten, betrieblich oder sicherheitstechnisch relevanten Clouds, muss geführt werden.

Überwachung

Das BAV wird in Zukunft im Rahmen seiner Aufsichtstätigkeiten sowohl auf Verfahrensebene (Plangenehmigungen und Typenzulassungen) als auch im Rahmen seiner Überwachungstätigkeit (Audits und Betriebskontrollen) die Umsetzung der oben genannten Anforderungen überprüfen. Diese Prüfung wird risikoorientiert durchgeführt, wobei den Themen Lieferantenmanagement und Business Continuity Management besondere Bedeutung beigemessen wird.

Wir danken Ihnen, dass Sie sich für einen sicheren, zuverlässigen und wirtschaftlichen öffentlichen Verkehr einsetzen.

Bei Fragen wenden Sie sich bitte an BAV-Sicherheitstechnik@bav.admin.ch

Freundliche Grüsse

Bundesamt für Verkehr

Rudolf Sperlich
Vizedirektor

Leo Brunner
Sektionschef Sicherheitstechnik

Zur Kenntnis an:

- Verband öffentlicher Verkehr (VöV)
- RAILplus
- Swissrail