Prüfung der IKT-Resilienz kritischer Infrastrukturen – Umsetzung des Minimalstandards bei Steuerungsanlagen der Eisenbahn

Bundesamt für Verkehr, Lausanne-Echallens-Bercher-Bahn, Freiburgische Verkehrsbetriebe, Zentralbahn und Rhätische Bahn

Das Wesentliche in Kürze

Kritische Infrastrukturen (KI) stellen die Versorgung der Schweiz mit unverzichtbaren Gütern und Dienstleistungen sicher. Um diese KI zu schützen, muss eine möglichst permanente Funktionstüchtigkeit gewährleistet sein. In diesem Zusammenhang kommt der Resilienz der Informations- und Kommunikationstechnik (IKT) bzw. dem Schutz der kritischen Infrastrukturen (SKI) vor Cyberbedrohungen eine hohe Bedeutung zu. Der Bundesrat hat am 8. Dezember 2017 die nationale Strategie zum SKI (2018–2022) verabschiedet. Dazu gehört der Schienenverkehr. Der Bund gibt jährlich rund 4,5 Milliarden Franken für den Substanzerhalt und den Ausbau der Bahninfrastruktur aus.

Mittels einer Querschnittsprüfung hat die Eidgenössische Finanzkontrolle (EFK) bei vier Bahnunternehmen[1] die Einhaltung von Minimalanforderungen zum IKT-Schutz gegen Cyberangriffe geprüft. Dabei kam der vom Bundesamt für wirtschaftliche Landesversorgung (BWL) veröffentlichte «Minimalstandard zur Verbesserung der IKT-Resilienz» zum Einsatz. Dieser deckt im Wesentlichen die fünf Themenbereiche «Identifizieren», «Schützen», «Detektieren», «Reagieren» und «Wiederherstellen» ab und bietet ein Bündel konkreter Massnahmen zur Umsetzung an. Das BWL empfiehlt den Betreibern von KI, den IKT-Minimalstandard umzusetzen.

Grosse Unterschiede beim Stand der Informationssicherheit

Im Hinblick auf die Maturität, welche das Schutzniveau beschreibt, hat die Prüfung ein heterogenes Bild ergeben: von «deutlich unter dem empfohlenen Minimalwert» bis «Minimalwert klar übertroffen». Bei der Umsetzung der Informationssicherheit gibt es bei allen Geprüften noch Handlungsbedarf.

Bereits im Bereich der Organisation der Informationssicherheit war festzustellen, dass bei drei der geprüften Bahnen die erforderlichen Rollen nicht oder nur ungenügend definiert sind. Auch die Wahrnehmung der IKT-Risiken ist bei den Mitarbeitenden sehr unterschiedlich.

Ein vollständiges Inventar der zu schützenden Informationen und Systeme stellt die wichtigste Grundlage zur Umsetzung der IKT-Sicherheit dar. Die Bahnunternehmen sind sich dessen bewusst und führen ein Inventar ihrer Werte. Teilweise sind diese noch in verschiedenen Datenquellen, ohne miteinander verknüpft zu sein. Diverse Projekte sollen diesen Zustand in Zukunft verbessern.

[1] Lausanne-Echallens-Bercher-Bahn, Freiburgische Verkehrsbetriebe, Zentralbahn und Rhätische Bahn

Das Zugriffmanagement muss bei drei Bahnen verbessert werden. Die Verwaltung der Benutzerkonten und die Vergabe der Rechte weisen in mancher Hinsicht erhebliche Mängel auf. Fernzugriffe durch Lieferanten müssen in der Kontrolle der Kunden sein und nachvollziehbar dokumentiert werden. Hier besteht für die betroffenen Bahnen ein umfangreicher Handlungsbedarf.

Der physischen und umgebungsbezogenen Sicherheit muss generell mehr Beachtung geschenkt werden. So ist in einem Fall der Zutritt zur Leitzentrale ungesichert, sodass die sich darin befindenden IKT-Systeme technisch nicht gegen unbefugte Zugriffe geschützt sind. Geräte für die Wartung des Rollmaterials sind teilweise unverschlossen zugänglich. Beim Brandschutz sind Massnahmen, die sich stark voneinander unterscheiden implementiert. Während verschiedene Stellwerke über keine Brand- oder Rauchmeldesysteme verfügen und die Löschmittel für eine allfällige Erstintervention fehlen, fand die EKF bei einer Bahn in den kritischen Anlagen redundante, automatische Löschsysteme vor.

Die Hälfte der geprüften Bahnen führt die Betriebszentralen mehrfach und an verschiedenen Standorten, wodurch der Betrieb bei einer Störung nicht beeinträchtigt werden sollte.

Das Testen von Notfallszenarien und Wiederherstellungsverfahren sollte als ständiger Prozess betrachtet werden. Damit kann sichergestellt werden, dass im Ereignisfall Systeme und Prozesse funktionieren. Um in diesem Bereich einen angemessenen Stand zu erreichen, muss bei vereinzelten Bahnen noch einiges aufgearbeitet werden.

Die Vorgaben zur Informationssicherheit: eine grosse Herausforderung für kleine Bahnbetriebe

Die Querschnittsprüfung hat gezeigt, dass grössere Bahnen hinsichtlich der IKT-Sicherheit besser aufgestellt sind als kleinere. Für kleine Betriebe stellt sie eine grosse finanzielle und personelle Herausforderung dar. Eine enge Zusammenarbeit mit grösseren Bahnen und der Bezug externer Dienstleistungen können aber eine positive Wirkung haben.

In diesem Jahr wurden die Ausführungsbestimmungen zur Eisenbahnverordnung durch das Bundesamt für Verkehr (BAV) überarbeitet und verabschiedet. Darin werden die Aspekte der Informationssicherheit erstmals explizit verankert. Mit dem Inkrafttreten der Vorgaben sind alle Bahnunternehmen ab dem 1. November 2020 verpflichtet, ein Informationssicherheitsmanagementsystem aufzubauen und zu betreiben. Das BAV spezifiziert allerdings weder die Mindestanforderungen noch die Frist zur Umsetzung. Indem es seine Erwartungen präzisiert und Arbeitsmittel zur Verfügung stellt, könnte das BAV den Bahnbetrieben eine wesentliche Unterstützung bieten.