

Prüfung der IT-Applikationslandschaft

Bundesamt für Verkehr

Das Wesentliche in Kürze

Das Bundesamt für Verkehr (BAV) ist als Aufsichtsbehörde zuständig für den öffentlichen Verkehr in der Schweiz. Unter seine Aufsicht fallen Eisenbahnen, Seilbahnen, Trolleybusse, Trams, Autobusse und Schiffe. Diesbezüglich regelt das BAV die Zuweisung finanzieller Mittel im Umfang von circa 4 Milliarden Franken jährlich an die angeschlossenen Transportunternehmen für Investitionen zum Substanzerhalt und zur Abgeltung des Betriebsaufwands.

Die Eidgenössische Finanzkontrolle (EFK) führte eine Voranalyse der IT-Applikationslandschaft beim BAV durch und wählte die Anwendung «Transportunternehmensverzeichnis» (TU-V) für eine vertiefte Prüfung aus. Die EFK prüfte inwieweit das TU-V stabil, sicher, verlässlich und wirtschaftlich betrieben wird. Zudem untersuchte sie den Informationsfluss für Finanzbuchungen vom TU-V zur Buchhaltung in SAP.

Die Firma Geocloud AG ist mit der Wartung der Anwendung TU-V beauftragt. Dessen Betrieb erfolgt durch das Bundesamt für Informatik und Telekommunikation.

Die Einhaltung des Datenschutzgesetzes sollte mit hoher Priorität sichergestellt werden

Im Rahmen einer Programmänderung wurden im Dezember 2015 im TU-V zusätzliche Datenfelder eingefügt. Dabei handelte es sich nicht nur um Personendaten wie Namen, Vornamen, Geburtsdaten und Bürgerorte, sondern auch um besonders schützenswerte Personendaten, etwa Informationen zu Straftaten und strafrechtlichen Sanktionen sowie Hinweise zu medizinischen Problemen. Die Applikation war nicht auf den Schutz dieser Daten ausgelegt, was dazu führte, dass Vorgaben des Datenschutzgesetzes nicht eingehalten wurden. Das BAV und die zuständigen Stellen des Departements (insbesondere der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte) wurden von der EFK brieflich über diesen Sachverhalt orientiert.

Das BAV ergriff daraufhin Sofortmassnahmen und unterbreitete der EFK einen Massnahmenplan. Dieser Plan erscheint der EFK aufgrund des aktuellen Kenntnisstandes als angemessen, um die notwendigen Verbesserungen zu erreichen. Da ein formeller Prozessablauf für die Vornahme von Änderungen an Programmen noch nicht festgelegt ist, muss das BAV für das Änderungswesen einen klaren Change-Prozess festlegen und implementieren. Hierin sind die Bewilligung von Änderungen, deren Tests und Freigabe sowie die Funktioneentrennung der beteiligten Stellen zu regeln.

Ein Zugriffsschutz- und Rollenkonzept ist zu erstellen und umzusetzen

Hinsichtlich der Verwaltung von Benutzerkonten innerhalb des TU-V sind klare Prozesse für die Administration und die Rechtevergabe festzulegen und zu implementieren. Ebenso sollten die entsprechenden Dokumentationen des TU-V, beispielsweise die Schutzbedarfsanalyse, aktualisiert werden.