EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

Prüfung der IT-Applikationslandschaft

Bundesamt für Verkehr

EFK-17383 | inkl. Stellungnahmen | 28. Juni 2018 | FinDel D5/2018

Bestelladresse Adresse de commande Indirizzo di ordinazione Ordering address	Eidgenössische Finanzkontrolle (EFK) Monbijoustrasse 45 3003 Bern Schweiz
Bestellnummer Numéro de commande Numero di ordinazione Ordering number	1.17383.802.00283
Zusätzliche Informationen Complément d'informations Informazioni complementari Additional information	www.efk.admin.ch info@efk.admin.ch twitter: @EFK_CDF_SFAO + 41 58 463 11 11
Abdruck Reproduction Riproduzione Reprint	Gestattet (mit Quellenvermerk) Autorisée (merci de mentionner la source) Autorizzata (indicare la fonte) Authorized (please mention source)

Inhaltsverzeichnis

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 Funktionentrennung 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.

Audit de l'environnement applicatif informatique
Office fédéral des transports

L'essentiel en bref

En tant qu'autorité de surveillance, l'Office fédéral des transports (OFT) est responsable des transports publics en Suisse. Les domaines des chemins de fer, des installations de transport à câbles, des trolleybus, des tramways, des autobus et de la navigation relèvent de sa compétence. L'OFT attribue à cet effet des moyens financiers s'élevant annuellement à environ 4 milliards de francs aux entreprises de transport partenaires pour maintenir la substance des infrastructures et indemniser les frais d'exploitation.

Le Contrôle fédéral des finances (CDF) a mené une analyse préliminaire de l'environnement applicatif informatique auprès de l'OFT et effectué un audit approfondi de l'application « Répertoire des entreprises de transport » (RET). Le CDF a évalué la stabilité, la sécurité, la fiabilité et la rentabilité du RET. Il a en outre vérifié l'échange des informations relatives à la comptabilité dans RET dans le système comptable de SAP.

La maintenance de RET est assurée par l'entreprise Geocloud AG et son exploitation par l'Office fédéral de l'informatique et de la communication.

Une haute priorité devrait être accordée au respect de la loi sur la protection des données

En décembre 2015, des champs de données supplémentaires ont été introduits dans RET dans le cadre d'une modification de cette application. Il ne s'agit pas uniquement de données personnelles telles que le nom, le prénom, la date de naissance et le lieu d'origine, mais aussi de données particulièrement sensibles, par exemple des informations concernant des infractions ou des sanctions pénales et des indications sur des problèmes médicaux. Or l'application RET n'était pas conçue pour protéger ces données, ce qui signifie que des directives de la loi sur la protection des données n'ont pas été respectées. Le CDF a informé l'OFT et les services compétents du département (notamment le Préposé fédéral à la protection des données) par écrit.

L'OFT a alors pris des mesures immédiates et présenté un plan d'action au CDF. En l'état des connaissances actuelles, ce dernier juge le plan d'action approprié pour réaliser les améliorations nécessaires. Étant donné qu'un processus formel n'est pas encore défini pour apporter des modifications à des applications, l'OFT doit élaborer et appliquer un processus de changement clair en réglementant l'autorisation des modifications, leurs tests et validation ainsi qu'en attribuant des fonctions distinctes à chaque service concerné.

Un concept de protection des accès et de rôles doit être établi et mis en œuvre

Des processus clairs doivent être définis et appliqués pour l'administration et la gestion des droits d'accès des comptes d'utilisateurs dans l'application RET. La documentation correspondante, comme l'analyse des besoins de protection, devrait également être mise en jour.

Texte original en allemand

Verifica delle applicazioni informatiche
Ufficio federale dei trasporti

L'essenziale in breve

Quale autorità di vigilanza, l'Ufficio federale dei trasporti (UFT) è competente per i trasporti pubblici in Svizzera. Sotto la sua vigilanza rientrano le ferrovie, gli impianti di trasporto a fune, i filobus, i tram, gli autobus e i battelli. In questo contesto l'UFT disciplina l'assegnazione delle risorse finanziarie, pari a circa 4 miliardi di franchi all'anno, alle imprese di trasporto affiliate per effettuare investimenti volti a mantenere la sostanza delle infrastrutture e a indennizzare i costi di esercizio.

Il Controllo federale delle finanze (CDF) ha condotto un'analisi preliminare delle applicazioni informatiche in uso presso l'UFT e ha scelto di sottoporre a una verifica approfondita l'applicazione «Banca dati delle imprese di trasporto» (BDIT). Il CDF ne ha esaminato la stabilità, la sicurezza, l'affidabilità e la redditività con cui è gestita. Ha inoltre analizzato il flusso d'informazioni per le registrazioni finanziarie da BDIT alla contabilità in SAP.

L'azienda Geocloud AG è responsabile della manutenzione di BDIT, mentre l'esercizio compete all'Ufficio federale dell'informatica e della telecomunicazione.

Una priorità elevata dovrebbe essere attribuita all'osservanza della legge federale sulla protezione dei dati

A dicembre 2015, nell'ambito di una modifica all'applicazione BDIT sono stati inseriti alcuni campi di dati supplementari che non riguardavano unicamente dati personali quali nomi, cognomi, date di nascita e luoghi d'origine, bensì anche dati personali degni di particolare protezione, come informazioni su reati, sanzioni penali o problemi medici. L'applicazione non era concepita in modo da proteggere questo genere di dati e, di conseguenza, le prescrizioni della legge federale sulla protezione dei dati non sono state osservate. Il CDF ha informato per lettera l'UFT e i servizi competenti del dipartimento (in particolare l'incaricato federale della protezione dei dati e della trasparenza) di questa situazione.

L'UFT ha quindi intrapreso una serie di misure immediate e sottoposto al CDF un piano d'azione. Allo stato attuale, il CDF ritiene che questo piano sia adeguato per ottenere i miglioramenti necessari. Poiché non è stata ancora definita, sul piano formale, una procedura per apportare modifiche alle applicazioni, l'UFT deve istituire e implementare un change management chiaro, che disciplini l'approvazione delle modifiche, i test e le convalide correlati nonché la separazione delle funzioni tra i servizi interessati.

Piano per definire i ruoli e garantire la protezione dell'accesso

Riguardo alla gestione degli account degli utenti in BDIT, è necessario stabilire e implementare procedure chiare per l'amministrazione e l'assegnazione dei diritti. Occorre inoltre aggiornare la pertinente documentazione di BDIT, ad esempio quella sull'analisi del bisogno di protezione.

Testo originale in tedesco

Audit of the IT application landscape
Federal Office of Transport

Key facts

The Federal Office of Transport (FOT) is the supervisory authority responsible for public transport in Switzerland. It supervises railways, cable cars, trolleybuses, trams, buses and ships. In this respect, the FOT regulates the allocation of approximately CHF 4 billion p.a. to the affiliated transport companies for investments for the preservation of value and compensation for operating expenses.

The Swiss Federal Audit Office (SFAO) carried out a preliminary analysis of the IT application landscape at the FOT and selected the "transport company directory" (TU-V) application for an in-depth audit. The SFAO examined the extent to which the TU-V is operated in a stable, secure, reliable and economical manner. In addition, it examined the information flow for financial postings from the TU-V to SAP accounting.

Geocloud AG is responsible for the maintenance of the TU-V application. It is operated by the Federal Office of Information Technology, Systems and Telecommunication.

Compliance with the Data Protection Act should be ensured as a high priority issue

Additional data fields were included in the TU-V in December 2015 as part of a program change. These included not only personal data such as surnames, first names, dates of birth and places of origin, but also particularly sensitive personal data such as information on criminal offences and criminal sanctions, as well as information on medical problems. As the application was not designed to protect this data, this led to non-compliance with the provisions of the Data Protection Act. The SFAO informed the FOT and the competent units of the department (particularly the Federal Data Protection and Information Commissioner) about the issue in a letter.

The FOT thereupon took immediate measures and submitted an action plan to the SFAO. Based on current knowledge, the SFAO considers this plan appropriate for achieving the necessary improvements. Since a formal process workflow for making changes to programs has not yet been defined, the FOT must define and implement a clear change process for change management. The approval of changes, their testing and release, and the functional separation of the units involved is to be regulated in this.

An access protection and role concept is to be created and implemented

Regarding the administration of user accounts within the TU-V, clear processes for administration and the assignment of rights must be defined and implemented. Likewise, the corresponding TU-V documentation, e.g. the protection requirements analysis, should be updated.

Original text in German

Generelle Stellungnahme der Geprüften

Das BAV bedankt sich für die konstruktive Zusammenarbeit mit der EFK.

Die Empfehlungen decken sich mehrheitlich mit bereits gemachten, eigenen Feststellungen. Aus diesem Grund sind Arbeiten für die Umsetzung der Empfehlungen bereits im Gang. Die weiteren Arbeiten werden entsprechend den Stellungnahmen bei den einzelnen Empfehlungen umgesetzt.

1 Auftrag und Vorgehen

1.1 Ausgangslage

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.

Auch wesentliche Bereiche des Güterverkehrs fallen in den Verantwortungsbereich des BAV. Diesbezüglich obliegt ihm die Aufgabe, einen hohen, aber dennoch finanzierbaren Sicherheitsstandard für die Bahnen, Busse, Schiffe und Seilbahnen zu gewährleisten.

Die Eidgenössische Finanzkontrolle (EFK) beurteilte in einer Voranalyse zu dieser Prüfung die IT-Anwendungslandschaft des BAV im Hinblick auf seine Aufgabenerfüllung. Dabei stellte die EFK fest, dass die Anwendung «Transportunternehmens-Verzeichnis» (TU-V) zur Regelung der Finanzierung bzw. der Zuordnung von Unterhaltskosten für die in Betrieb befindliche Bahninfrastruktur für die Aufgabenerfüllung des BAV eine zentrale Rolle einnimmt.

Diese Anwendung dient der Bearbeitung von Informationen der durch das BAV beaufsichtigten Transportunternehmen und deren Infrastruktur sowie Leistungen in den Bereichen Eisenbahn, Binnenschifffahrt, Seilbahnen und öffentlicher Strassenverkehr. Ebenso sind darin die mit Bezug auf die Koordination des Verkehrs relevanten Angaben über Inhaber von Konzessionen, Bewilligungen oder Genehmigungen der Eidgenossenschaft gespeichert.

Die Anwendung TU-V befindet sich in der Mitte ihres Lebenszyklus. Sie wurde in der jetzigen Version im Jahr 2008 durch die heutige Firma Geocloud AG, Schlieren (damaliger Firmenname: bdh. Solutions AG) mehrheitlich neu entwickelt. Seither werden laufend notwendige Anpassungen aufgrund gesetzlicher oder betrieblicher Anforderungen umgesetzt.

Als jüngste wesentliche Erweiterung wurden Webschnittstellen zu den Transportunternehmen in Betrieb genommen. Diese dienen der Erfassung wesentlicher Verkehrsdaten durch die Transportunternehmen.

1.2 Prüfungsziel und -fragen

Ziel der Prüfung war es, im Rahmen der Vorbereitung, eine Übersicht über die IT-Anwendungen im BAV zu gewinnen und mittels einer Risikoanalyse die relevanten Anwendungen zu identifizieren. In der Folge sollte für eine ausgewählte Anwendung und deren Schnittstellen eine vertiefte Anwendungsprüfung durchgeführt werden. Ausgewählt wurde die Anwendung TU-V.

Die Prüfungsfragen lauteten:

- Stellt das BAV in Zusammenarbeit mit dem Dienstleister einen stabilen, wirtschaftlichen Betrieb resp. eine Weiterentwicklung der Anwendung TU-V sicher?
- Ist das 3rd Party Service Management angemessen?
- Sind die IT-Sicherheitsrisiken angemessen adressiert?

- Bestehen angemessene Vorkehrungen zur Betriebskontinuität (hinsichtlich der Anwendung abhängiger Prozesse)?
- Sind die Schnittstellen verlässlich?
- Ist die Anwendung zukunftsfähig, besteht ein angemessenes Lifecycle-Management?

1.3 Prüfungsumfang und -grundsätze

Die Prüfungsarbeiten fanden vom 10. bis 21. Juli und vom 4. bis 15. Dezember 2017 sowie vom 5. bis 16. Februar 2018 beim BAV statt. Die EFK analysierte relevante Dokumentationen, führte Interviews mit den fachverantwortlichen Personen durch und nahm Prüfungshandlungen an der Anwendung TU-V vor. Als Prüfungsgrundlage wurden die IKT-Sicherheitsvorgaben des Bundes, CobiT sowie die Kontrollziele zu den generellen IKT-Kontrollen der EFK angewandt. Die Prüfung wurde von Rolf Schaffner (Revisionsleitung), Hans-Ulrich Wiedmer und Roland Gafner durchgeführt.

1.4 Unterlagen und Auskunftserteilung

Im Rahmen der Prüfungsarbeiten wurden die für die jeweiligen Zuständigkeitsbereiche verantwortlichen Personen des BAV sowie der Dienstleistungserbringerin Geocloud AG beigezogen.

Die notwendigen Auskünfte wurden der EFK von allen Beteiligten in offener und konstruktiver Weise erteilt. Die EFK hatte Zugriff auf sämtliche relevanten Projekt- und Betriebsunterlagen.

1.5 Schlussbesprechung

Die Schlussbesprechung fand am 23. Mai 2018 statt. Teilgenommen haben seitens des BAV der Direktor, die Leiterin Betriebswirtschaft und Organisation, der Leiter Informatik und GEVER sowie der Leiter Revision. Die EFK war vertreten durch den verantwortlichen Fachbereichsleiter und den Prüfungsleiter.

Die EFK dankt für die gewährte Unterstützung und erinnert daran, dass die Überwachung der Empfehlungsumsetzung den Amtsleitungen bzw. den Generalsekretariaten obliegt.

EIDGENÖSSISCHE FINANZKONTROLLE

2 Betrieb und Weiterentwicklung des TU-V

2.1 Das Änderungswesen weist Schwachstellen auf

Bei der Erweiterung «Road Package» wurden wesentliche Kontrollen unterlassen

Im Dezember 2015 wurde die Erweiterung «Road Package» implementiert. Mittels dieser Erweiterung können im TU-V auch jene Informationen bearbeitet werden, welche zur Beurteilung der Integrität und Vertrauenswürdigkeit der registrierten Strassentransportunternehmen notwendig sind.

Die EFK stellte fest, dass zusätzliche Datenfelder eingefügt wurden. Dabei handelte es sich nicht nur um Personendaten wie Namen, Vornamen, Geburtsdaten und Bürgerorte, sondern auch um besonders schützenswerte Personendaten wie Informationen zu Straftaten und strafrechtlichen Sanktionen sowie Hinweise zu medizinischen Problemen.

Die Anwendung war grundsätzlich nicht auf den Schutz dieser Daten ausgelegt. Dies führte dazu, dass Vorgaben des Datenschutzgesetzes nicht eingehalten wurden.

Wie unten dargestellt, konstatierte die EFK zudem, dass diese Daten innerhalb des Bundesnetzes nur ungenügend vor unerlaubtem Zugriff geschützt waren.

In der Schutzbedarfsanalyse für das TU-V vom 17. März 2013 ist festgehalten, dass hinsichtlich Vertraulichkeit kein Schutzbedarf bestehe und dass keine Personendaten gespeichert würden. Mit der Realisierung der Erweiterung «Road Package» erfolgte keine Anpassung der Schutzbedarfsanalyse. Weiterhin stellte die EFK fest, dass die vorgeschriebene Anmeldung der Datensammlung beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) entsprechend dem Bundesgesetz über den Datenschutz (DSG) Art. 11, Bst. a zum Zeitpunkt der Prüfung noch nicht erfolgt war.

Mit Schreiben vom 16. Januar 2018 setzte die EFK das BAV über diese Feststellungen in Kenntnis. Daraufhin wurden seitens des BAV Sofortmassnahmen zum Schutz vor unerlaubtem Zugriff auf diese Daten umgesetzt. Das BAV stellte in seiner Stellungnahme vom 25. Januar 2018 an die EFK die vorgesehenen Verbesserungsmassnahmen in einem nach Phasen unterteilten Plan dar.

Beurteilung

Im Rahmen der Realisierung der Erweiterung «Road Package» wurde es unterlassen, den Schutzbedarf der neuerdings im TU-V zu bearbeitenden Daten zu erheben und entsprechende Sicherheitsvorkehrungen sowie auch die vom DSG vorgeschriebenen Anmeldungen vorzunehmen.
Die durch das BAV im Schreiben vom 25. Januar 2018 dargestellten Verbesserungsmassnahmen erscheinen der EFK aufgrund des aktuellen Kenntnisstandes als angemessen, um die notwendigen Verbesserungen zu erreichen.

Für das Änderungswesen ist kein formeller Prozess implementiert

Die Geocloud AG ist mit der Wartung der Anwendung TU-V beauftragt. Der Betrieb des TU-V erfolgt durch das Bundesamt für Informatik und Telekommunikation (BIT). Für die ausgelagerten Dienste bestehen Service-Level-Agreements, welche der EFK zum Zeitpunkt der Prüfung vorgelegt wurden.

Änderungen werden im Rahmen von Aufträgen mit entsprechender Koordination zwischen BAV, Geocloud AG und BIT abgewickelt. Die diesbezüglichen Regelungen sind im Wartungs- und Supportvertrag mit der Geocloud AG sowie in den Service-Level-Agreements mit dem BIT dokumentiert.

Die Geocloud AG betreibt für das TU-V eine Testumgebung. Zudem betreibt das BIT eine Abnahme- und eine Produktionsumgebung. Die Änderungen werden nach der Durchführung der Tests auf der Produktionsumgebung eingeführt. Hierfür werden die Vorgaben des BIT angewandt. Seitens BAV besteht keine formelle Vorgabe für die Abwicklung von Änderungen.

Beurteilung

Da zum Change-Management innerhalb des BAV kein formeller Prozessablauf mit Dokumentationsvorgaben festgelegt ist, war zum Zeitpunkt der Prüfung nicht nachvollziehbar, wie vorgenommene Änderungen freigegeben worden waren und ob die Funktionentrennung in den Änderungsprozessen angemessen war.

Empfehlung 1 (Priorität 1)

Die EFK empfiehlt dem BAV für das Änderungswesen einen klaren Prozess mit nachvollziehbarer Dokumentation festzulegen. Dieser sollte insbesondere die Bewilligung von Änderungen sowie deren Tests und die Freigabe regeln. Ebenso sollte die Überwachung der Änderungen und die Sicherstellung der Funktionentrennung der involvierten Personen vorgegeben werden.

Stellungnahme des Geprüften

Das BAV führt den definierten ACRM-Prozess (Anforderungs-, Change, Release-Management-Prozess) gemäss Massnahmenplan ein.

2.2 Die Zugriffsschutzmassnahmen sind zu verbessern

Die Sicherheitsdokumente sollten aktualisiert werden

Eine Aktualisierung der Sicherheitsdokumente hat gemäss den WIsB mindestens alle fünf Jahre oder bei einem Technologiewechsel zu erfolgen. In diesem Fall wurden ein Zonenwechsel von der DMZ («demilitarisierte» sicherheitstechnische Zone des Netzwerks) in die CAZ («Central Access Zone») vorgenommen und die Transferprotokolle von http auf https (Secure Socket Layer-Verschlüsselung) umgestellt. Diese massgeblichen Änderungen wurden in der Schutzbedarfsanalyse und im ISDS-Konzept mit Stand Dezember 2013 nicht berücksichtigt.

Wie oben dargestellt, befindet sich die Schutzbedarfsanalyse auch hinsichtlich der Sensitivität der im TU-V bearbeiteten Daten nicht auf aktuellem Stand. Das BAV stellte in seiner Stellungnahme vom 25. Januar 2018 an die EFK dar, dass die Aktualisierungen im Rahmen der Phase 2 der Umsetzung von Verbesserungsmassnahmen vorgesehen sind.

Für die Benutzerverwaltung ist kein formeller Prozess implementiert

Ein klar geregelter und formalisierter Prozess zur Benutzermutation (Ein-, Aus- und Übertritt) ist nicht vorhanden. Die Rechtevergabe erfolgt ohne angemessene Überprüfung der Funktionentrennung und basiert auf Vertrauen. Nicht registrierte Benutzer innerhalb des Bundesnetzes verfügen über den Rechte-Umfang des «Anonymous User». Diese Leserechte nicht registrierter Benutzer umfassten zum Prüfungszeitpunkt teilweise den Zugriff

auf sensitive Informationen, welcher nur einem dafür ausgewählten Personenkreis gewährt werden sollte. So konnten beispielsweise auch die nicht im TU-V registrierten Benutzer im Bundesnetz, «Anonymous-User», die besonders schützenswerten Personendaten einsehen.

Beurteilung

Die Benutzer und deren Rollen sind nur im System hinterlegt und nicht zusätzlich dokumentiert. Das Fehlen eines Zugriffsschutz- und Rollenkonzepts erschwert eine einheitliche Handhabung der Rechtevergabe und birgt das Risiko einer mangelnden oder fehlerhaften Umsetzung. So ist es möglich, dass ein Administrator einem User oder einer Rolle (beabsichtigt oder unbeabsichtigt) falsche (und privilegierte) Rechte zuteilt.

Eine Protokollierung der Rechtevergabe im System erfolgt nicht. Dadurch besteht das Risiko nicht nachvollziehbarer temporärer Zuweisungen hoher Privilegien. Ein Missbrauch von Berechtigungen wird dadurch erleichtert. Zum Prüfungszeitpunkt bestand kein Reporting, das dargestellt hätte, welcher Person zu welchem Zeitpunkt welche Rechteprofile zugeordnet waren.

Die Verantwortlichkeit des Dateneigentümers ist im BAV nicht konkret festgelegt. Die mit der Bearbeitung der Daten betrauten Personen verfügen teilweise nicht über angemessene Detailkenntnis hinsichtlich der Sensitivität dieser Informationen.

Empfehlung 2 (Priorität 1)

Die EFK empfiehlt dem BAV, ein Zugriffsschutz- und Rollenkonzept zu erstellen und darauf basierend die Prozesse zur Benutzerverwaltung zu implementieren.

Stellungnahme des Geprüften

Ein Rollenkonzept ist teilweise bereits vorhanden, wird aber bis Ende 2018 vervollständigt und im Rahmen des nächsten CR einbezogen. Zeitplan: 31.12.2018 für Konzept, 30.06.2019 für Implementierung

Empfehlung 3 (Priorität 2)

Die EFK empfiehlt dem BAV die Aufgaben des Dateneigentümers zu definieren und die geeigneten Personen mit den entsprechenden Aufgaben zu betrauen. Bedarfsweise sollten diese Personen hinsichtlich der geltenden Vorschriften des Datenschutzgesetzes und IT-sicherheitsrelevanter Aspekte geschult werden, um auch in diesem Bereich eine angemessene Sensibilisierung zu erreichen.

Stellungnahme des Geprüften

Das BAV beabsichtigt, der Empfehlung zu entsprechen und bis Ende dieses Jahres an einem geeigneten Ort (z. B. durch Erweiterung der Weisung BGÖ um den Aspekt DSG) zu präzisieren, wer als Dateneigentümer mit welchen Aufgaben betraut ist und eine Mitarbeiterschulung durchzuführen.

2.3 Die Prozesse für den Betrieb des TU-V müssen ergänzt werden

Die Wartung und der Betrieb des TU-V sind an externe Leistungserbringer ausgelagert

Das BIT betreibt die Anwendung TU-V gemäss den zwischen BIT und BAV festgelegten Service-Level-Agreements. Es sind bisher keine wesentlichen Betriebsstörungen hinsichtlich des TU-V vorgefallen.

Die Wartung wird durch die Firma Geocloud AG wahrgenommen. Auch hierfür bestehen Vereinbarungen, worin Leistungen, Kosten sowie die Modalitäten für die Realisierung, Tests und Implementation von Änderungen festgelegt sind.

Die Leistungserbringung ist zwischen BIT, Geocloud AG und BAV abgestimmt. In der praktischen Umsetzung sind den Darstellungen des BAV zufolge bisher keine Probleme aufgetreten.

Beurteilung

Die EFK hat in den Service-Level-Agreements zwischen BAV und BIT und zwischen BAV und Geocloud AG – mit Ausnahme der nachstehend dargestellten Problemstellung – keine Mängel festgestellt.

Daten des TU-V werden regelmässig gesichert, die Wiederherstellung wird jedoch nicht getestet

Aufgrund der bestehenden Service-Level-Agreements zwischen BAV und BIT stellt das BIT sicher, dass in den vereinbarten zeitlichen Intervallen eine Sicherung der Daten des TU-V vorgenommen wird.

Seit der Inbetriebnahme des TU-V durch das BIT hat das BAV noch keine Tests hinsichtlich einer korrekten Wiederherstellung durchgeführt.

Beurteilung

Die IKT-Grundschutz-Anforderung 12.3.2, wonach die Verfahren zur korrekten Wiederherstellung der Daten nach einem Zwischenfall regelmässig durch Tests überprüft werden müssen, wird nicht berücksichtigt.

Empfehlung 4 (Priorität 2)

Die EFK empfiehlt dem BAV, regelmässig Restore-Tests für das TU-V durchzuführen. Allfällige Mängel sollten zeitnah behoben werden.

Stellungnahme des Geprüften

Das BAV plant einen Restore-Test Mitte 2019 durchzuführen. Danach 2-jährlich oder bei der Umsetzung von massgeblichen Changes.

3 Organisatorisches und technisches Umfeld sowie Schnittstellen der Anwendung TU-V

3.1 Die Transportunternehmen nutzen eine Standard Webplattform zur Dateneingabe im TU-V

Die Abteilung Finanzierung des BAV erarbeitet mit den Schweizer Transportunternehmen Lösungen zur Finanzierung der anfallenden Bedürfnisse. Jedes Jahr nimmt sie die Zuteilung von Subventionen im Umfang von circa vier Milliarden Franken vor.

Für die Bemessung von Subventionen an die Schweizer Verkehrsbetriebe werden Kennzahlen angewandt, welche kontinuierlich und in hohem Detaillierungsgrad im TU-V eingepflegt werden. Hierfür stehen den angeschlossenen Verkehrsbetrieben webbasierte Eingabeplattformen zur Verfügung (TU-V-Web). Das BAV reichert die seitens der Verkehrsbetriebe eingebrachten Informationen an und nimmt die Qualitätssicherung der erfassten Kennzahlen wahr.

Die TU-V-Webdienste werden, wie TU-V selber, durch das BIT betrieben. Es bestehen automatische Schnittstellen zwischen der TU-V-Webplattform und der Anwendung TU-V. Es liegen keine weiteren automatischen Schnittstellen zwischen TU-V und anderen Systemen vor.

In der Organisation des BAV sind Kontrollvorgänge festgelegt, die sicherstellen sollen, dass die in TU-V-Web erfassten Kennzahlen durch Mitarbeitende des BAV überprüft werden und erst nach entsprechender Prüfung in das TU-V übernommen werden. Die BAV-Mitarbeiter haben auch die Zugriffsrechte, um Eingaben der Transportunternehmen im Bedarfsfall zu korrigieren.

Beurteilung

Die EFK ist der Ansicht, dass dem BAV in TU-V-Web und in TU-V grundsätzlich geeignete Abfragemöglichkeiten zur Verfügung stehen.

Die Regelung der Zugriffsberechtigungen auf diese Informationen sollte zusammen mit der Sicherstellung einer angemessenen Funktionentrennung in einem Zugriffsschutz und Rollenkonzept festgelegt werden (siehe Abschnitt 2.2).

Im Sinne der Nachvollziehbarkeit sollten die Kontrollvorgänge hinsichtlich der durch die Transportunternehmen erfassten Daten in angemessener Weise geregelt werden. Für die Erfassung und Mutation von Bewegungs- und Stammdaten im TU-V werden nicht durchgehend Aufzeichnungen mit Angabe des Datums und der Benutzeridentifikation erstellt.

Die Verifizierung der Richtigkeit der erfassten Daten durch das BAV setzt weitreichende Kenntnis über die betriebswirtschaftlichen Voraussetzungen für die Leistungserbringung durch die Transportunternehmen voraus. Vielfach sind hierzu Vergleiche von Kennzahlen verschiedener Transportunternehmen notwendig, die aus dem bestehenden Berichtswesen des TU-V nicht automatisch ableitbar sind.

Empfehlung 5 (Priorität 2)

Die EFK empfiehlt dem BAV, seine Kontrollvorgänge hinsichtlich der durch die Transportunternehmen erfassten Daten mit Angabe der Personenidentifikation und des Zeitpunkts der Durchführung zu registrieren. Ebenso sollte das BAV für die Erfassung und die Mutation von Bewegungs- und Stammdaten im TU-V Aufzeichnungen mit der jeweiligen Angabe der Benutzeridentifikation und des Zeitpunkts erstellen.

Stellungnahme des Geprüften

Die Möglichkeiten für eine weitergehende Aufzeichnung der Mutationstätigkeiten werden bis Ende 2018 analysiert und im Rahmen des nächsten CR umgesetzt. Zeitplan: 31.12.2018 für Konzept, 30.06.2019 für Implementierung.

3.2 Finanzrelevante Daten werden manuell in SAP verbucht

Basierend auf den im TU-V bearbeiteten Kennzahlen werden durch das BAV im Buchhaltungssystem SAP die finanzrelevanten Geschäftsvorfälle erfasst und verbucht. Hierfür werden im TU-V entsprechende Berichte aufbereitet und ausgedruckt. Diese physischen Dokumente mit den buchungsrelevanten Informationen durchlaufen im BAV daraufhin den festgelegten Kontrollablauf. Dabei überprüfen die mit der Kontrolle beauftragten Personen die dargestellten Kennzahlen sowie Buchungsinformationen und quittieren ihre Kontrollen mit Visum. Danach werden die visierten Dokumente dem Rechnungswesen des BAV übergeben. In der Finanzbuchhaltung werden die entsprechenden Buchungen erfasst und verbucht.

Beurteilung

Die EFK stellte hinsichtlich dieser Verfahrensregelung keine Sachverhalte fest, welche auf besondere Risiken in der Abwicklung der entsprechenden finanzwirksamen Transaktionen hinweisen würden.

4 Wirtschaftlichkeit

Aufgrund der bestehenden Befristungen der Verträge mit Geocloud AG bereitet das BAV eine Ausschreibung der benötigten Wartungs- und Entwicklungsleistungen vor. Auf dieser Basis wird angestrebt, weiterhin eine möglichst kostengünstige Lösung für die erforderlichen Dienste nutzen zu können. Wegen der Ausschreibung wird auf eine Darstellung der aktuellen Kosten in dieser Berichterstattung verzichtet.

Das BAV betreibt nebst TU-V auch weitere kleinere Anwendungen, welche vielfach auf Microsoft-Office-Access-Plattformen betrieben werden. Diesbezüglich führte die EFK im Rahmen dieser Prüfung keine spezifischen Untersuchungen durch.

Beurteilung

Die Plattform, auf welcher TU-V betrieben wird, ist kostengünstig, weist eine zukunftssichere Architektur auf und ist von der Kapazität her wenig belastet. Die EFK erachtet es als sinnvoll, eine Überführung von bisher auf Microsoft-Office-Access basierten Kleinanwendungen auf die Plattform des TU-V zu prüfen. Dies könnte Kosteneinsparungen nach sich ziehen und einen verlässlicheren Betrieb solcher Kleinanwendungen ermöglichen.

Empfehlung 6 (Priorität 3)

Die EFK empfiehlt dem BAV zu prüfen, ob die heute bestehenden Microsoft-Office-Access-Lösungen mit vertretbarem Aufwand auf die TU-V-Plattform migriert werden könnten.

Stellungnahme des Geprüften

Das BAV prüft im Rahmen des IT-Architekturmanagements und dem LifeCycle-Management grundsätzlich ob Anwendungen wirtschaftlicher betrieben werden können. Dabei steht die effiziente Unterstützung der Geschäftsprozesse im Vordergrund.

Dies auf MS-Office-Access-Lösungen zu beschränken und dabei nur die TU-V-Plattform als Zielsystem zu betrachten erachten wir als zu einschränkend.

Zeitplan: Laufend bei Bedarf.

Anhang 1: Rechtsgrundlagen

Rechtstexte
Bundesgesetz über die Eidgenössische Finanzkontrolle (Finanzkontrollgesetz, FKG) vom 28. Juni 1967 (Stand am 1. Januar 2012), SR 614.0
Bundesgesetz über den Datenschutz vom 19. Juni 1994, Stand am 1. Januar 2014
Si001 – IKT-Grundschutz in der Bundesverwaltung vom 19. Dezember 2013: Vorgabe des ISB (Informatik-Steuerungsorgan des Bundes) gestützt auf Ziffer 3.1 der Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung (WIsB1) vom 1. Juli 2015
Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung vom 1. Juli 2015

Anhang 2: Abkürzungen

BIT	Bundesamt für Informatik und Telekommunikation
CAZ	Central Access Zone
DMZ	Demilitarized Zone
DSG	Bundesgesetz über den Datenschutz
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EFK	Eidgenössische Finanzkontrolle
ISB	Informatiksteuerungsorgan des Bundes
TU-V	Transportunternehmensverzeichnis
WIsB	Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung

Anhang 3: Glossar

Access Management	Massnahmen zur Sicherstellung eines angemessenen logischen Zugriffsschutzes
Backup	Im produktiven Betrieb einer IT-Anwendung sollten die Daten periodisch (z. B. täglich) auf Sicherungsdatenträger kopiert werden, sodass im Falle einer Nichtverfügbarkeit der in der Produktion bearbeiteten Daten auf diese Datensicherung zurückgegriffen werden kann.
BDH Solutions AG	Die heutige Geocloud AG, Schlieren (Realisierungs- und Wartungspartnerin des BAV für die Anwendung TU-V) ging aus der BDH Solutions AG hervor.
Benchmarking	Das Benchmarking in der Betriebswirtschaft ist ein systematischer und kontinuierlicher Prozess des Vergleichens von Produkten, Dienstleistungen, Kosten und Prozessen.
Central Access Zone (des IT-Netzwerks)	Sicherheitstechnisch für den zentralen Zugriff festgelegte Zone des Netzwerks
Change Management	Prozesse und Massnahmen des Programmänderungswesens
Demilitarisierte Zone (des IT-Netzwerks)	Sicherheitstechnisch abgegrenzte (segmentierte) Zone des Netzwerks
Operations Management	Massnahmen für einen sicheren Betrieb der Anwendungen sowie zur rechtzeitigen Erkenntnis von Ausnahmesituationen
Primäre IT-Kontrollen oder Primary Control Procedures	Die EFK beurteilt hinsichtlich der generellen IT-Kontrollen folgende primären IT-Kontrollen: - Access Management (logischer Zugriffsschutz) - Change Management (Programm-Änderungswesen) - Operations Management (sicherheitstechnische Ausgestaltung des Betriebes der IT-Plattform)
Restore	Rückladen von Daten, welche auf einem Sicherungsdatenträger gespeichert sind
Service-Level-Agreement	Vertragliche Vereinbarung zwischen dem Erbringer von Informatik-Dienstleistungen und dem Leistungsbezüger (im vorliegenden Fall BAV)

Priorisierung der Empfehlungen

Die Eidg. Finanzkontrolle priorisiert die Empfehlungen nach den zugrunde liegenden Risiken (1 = hoch, 2 = mittel, 3 = klein). Als Risiken gelten beispielsweise unwirtschaftliche Vorhaben, Verstösse gegen die Recht- oder Ordnungsmässigkeit, Haftungsfälle oder Reputationsschäden. Dabei werden die Auswirkungen und die Eintrittswahrscheinlichkeit beurteilt. Diese Bewertung bezieht sich auf den konkreten Prüfgegenstand (relativ) und nicht auf die Relevanz für die Bundesverwaltung insgesamt (absolut).