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

Prüfung des DTI-Schlüsselprojektes Rechenzentren VBS/Bund 2020

Gruppe Verteidigung – Armeestab

EFK-21462 | inkl. Stellungnahmen | 30. Mai 2022 | FinDel D4/2022

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	525.21462
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

Mit Nennung der männlichen Funktionsbezeichnung ist in diesem Bericht, sofern nicht anders gekennzeichnet, immer auch die weibliche Form gemeint.

Inhaltsverzeichnis

Prüfung des DTI-Schlüsselprojektes Rechenzentren VBS/Bund 2020

Armeestab

Das Wesentliche in Kürze

Mit dem im Juli 2014 vom Bundesrat genehmigten Rechenzentren-Verbund soll die heterogene Rechenzentren-Landschaft der Bundesverwaltung in einen Verbund von vier Rechenzentren (RZ) konsolidiert werden. Damit kann die Zahl der RZ deutlich gesenkt und der zukünftige Kapazitätsbedarf der Bundesinformatik kostengünstiger sowie umweltschonender sichergestellt werden. Das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) plante in diesem Rahmen den Neubau von drei RZ. Zwei dieser Anlagen werden mit militärischem Vollschutz gebaut, um das Funktionieren der armeerelevanten Anwendungen und Systeme in allen Lagen zu gewährleisten. Das dritte RZ, wird auch von zivilen Bundesstellen genutzt. Umgesetzt werden diese Vorhaben im Rahmen des DTI-Schlüsselprojektes «Rechenzentren VBS/Bund 2020». Das Projekt umfasst auch den Aufbau der Digitalisierungsplattform der Armee, also den IKT-Teil der Rechenzentren. Die Gesamtkosten für das Projekt belaufen sich über alle Ausbaustufen hinweg auf rund 900 Millionen Franken für den Immobilienteil und auf 320 Millionen für die IKT-Mittel.

Die Prüfungsergebnisse der Bauvorhaben zeigen ein durchaus positives Bild. Das Projektmanagement ist zielführend aufgestellt und die Termine sowie Kosten konnten weitgehend eingehalten werden. Die Gebäudeautomation wurde in den Anlagen «FUNDAMENT» und «CAMPUS» zweckmässig umgesetzt und die Steuerung und Überwachung erfolgen nach gängigen Standards. Die Konzepte zum Aufbau der Digitalisierungsplattform beschreiben eine hochsichere und skalierbare Technologie und basieren auf erprobten Technologien.

Erfreulicher Stand bei den Bauprojekten

Die Bauprojekte sind gut strukturiert und die Dokumentationen auf einem detaillierten und guten Stand. Trotz partieller Verzögerungen sind die Projekte teilweise abgeschlossen oder auf Kurs. Der Kreditrahmen in den Projekten «CAMPUS» und «FUNDAMENT» konnte eingehalten werden und das Kostenmanagement erwies sich als effektiv. Die Kostenschätzung für das Projekt «KASTRO II» steht zum Prüfzeitpunkt allerdings noch aus. Aufgrund des Standortwechsels und der Tatsache, dass die Anlage neu gebaut werden soll, ist mit merklichen Mehrkosten zu rechnen.

Das Risiko- und Qualitätsmanagement ist etabliert und wirksam aufgestellt. Dennoch sollten besonders risikobehaftete Bestandteile künftig über alle Projektphasen einer vertieften Qualitätssicherung unterzogen werden.

Die Vorgabe aus dem Pflichtenheft zur Verfügbarkeitsklasse des RZ «FUNDAMENT» wurde gemäss einem frühen Gutachten in zwei Bereichen nicht erfüllt. Mit technischen Massnahmen konnte die geforderte Verfügbarkeit für die Verbrennungsluft der Notstromanlage erreicht werden. Die Abgasführung wurde mit baulichen Massnahmen verbessert. Im Projekt zum Bau des RZ «KASTRO II» sollte eine derartige Überprüfung in allen Phasen erfolgen.

Handlungsbedarf bei den Domotik-Systemen

Der Sicherheit der Domotik-Systeme wurde in den beiden neu gebauten RZ ein hoher Stellenwert eingeräumt. Die Implementierung erfolgte dem Bedarf entsprechend nach den hohen Sicherheitsanforderungen des Bundes und des VBS. Die vorgeschriebenen Sicherheitsdokumente liegen vor, weisen jedoch Differenzen zu den Betriebshandbüchern und den Servicevereinbarungen auf. Diese Widersprüche müssen bereinigt werden. Die in den Informationssicherheits- und Datenschutz (ISDS)-Konzepten beschriebenen Massnahmen zur Risikoreduktion sind noch nicht konsequent implementiert und deren Umsetzung muss terminiert und überwacht werden.

Domotik-Anwendungen müssen generell vor der Inbetriebnahme auf einer Integrations- und Testumgebung geprüft werden. Eine solche Umgebung existiert für diese Systeme noch nicht. Hier besteht dringender Handlungsbedarf, welcher aber vom VBS erkannt ist.

Etablierte Standards und neue Technologien für die Digitalisierungsplattform der Armee

Mit dem Teilprojekt «Architektur und Infrastruktur (IKT A&I)» wird die hochsichere Plattform für die Digitalisierung der Armee aufgebaut. Die eingesetzte Technologie und geplante Kommunikation entsprechen dem heutigen Standard hinsichtlich der Technik und Sicherheit für hochsichere Plattformen. Der Betrieb und die Weiterentwicklung der Digitalisierungsplattform stellen eine grosse Herausforderung für das sich im Aufbau befindliche Kommando Cyber dar.

Kapazitätsreserven zur Ablösung kleinerer RZ und Systemräumen

Die neuen RZ sind zum Prüfzeitpunkt zu 20 Prozent ausgelastet. Reserven für die Bestückung mit weiteren Systemen und Infrastrukturen sind in den gebauten Teilen vorhanden. Mit den geplanten Migrationen soll bis ca. Ende 2024 eine Auslastung der militärischen und zivilen RZ von etwa 50 Prozent erreicht werden.

Das Bundesamt für Polizei (fedpol) betreibt Spezialanwendungen mit hohen Sicherheits- und Verfügbarkeitsanforderungen. In den Jahren 2008–2016 wurde der Systemraum im G1 von fedpol mit dem Bundesamt für Bauten und Logistik geplant und per 2018 fertiggestellt. DTI stufte diesen als RZ-Raum ein und erteilte auch für den Betrieb der Anwendungen eine zeitlich begrenzte Ausnahmegenehmigung. In enger Zusammenarbeit mit dem Informatik Service Center des Eidgenössischen Justiz- und Polizeidepartements (ISC-EJPD) wurde nun eine Lösung zur weiteren Synergienutzung erarbeitet. Das RZ G1 soll für fedpol künftig in der Verantwortung des ISC-EJPD betrieben werden und somit Teil des RZ-Verbunds werden, um die heutigen sowie die neuen Schengen-Anforderungen an die Höchstverfügbarkeit durch ein zweifach redundantes Regionenkonzept abdecken zu können.

Die Empfehlungen aus früheren Prüfungen wurden umgesetzt. Die Resultate sind tabellarisch in Anhang 4 dargestellt.

Audit du projet TNI clé Centres de calcul DDPS/Confédération 2020

État-major de l'armée

L'essentiel en bref

Approuvé en juillet 2014 par le Conseil fédéral, le projet réseau de centres de calcul vise à consolider l'infrastructure hétérogène de l'administration fédérale en un réseau de quatre centres de calcul (CC). Ceci pour réduire sensiblement le nombre de CC et pour répondre aux besoins futurs de l'informatique fédérale à un moindre coût, tout en étant plus respectueux de l'environnement. Dans ce cadre, le Département fédéral de la défense, de la protection de la population et des sports (DDPS) a prévu la construction de trois nouveaux CC, dont deux dotés d'une protection militaire intégrale pour garantir le fonctionnement des applications et systèmes pertinents pour l'armée dans toutes les situations. Le troisième CC sera aussi utilisé par les offices fédéraux civils. Ces réalisations s'inscrivent dans le cadre du projet « Centres de calcul DDPS/Confédération 2020 », projet clé de transformation numérique et gouvernance de l'informatique (TNI). Le projet comprend aussi la mise en place de la plateforme de digitalisation de l'armée, donc de la composante informatique des CC. Pour toutes les étapes du développement, le total des coûts du projet s'élève à environ 900 millions de francs pour la partie immobilière et à 320 millions de francs pour les moyens informatiques.

Les résultats de l'audit du projet de construction donnent une image tout à fait positive. La gestion du projet est bien établie, et les délais et les coûts ont pu être respectés dans une large mesure. La domotique a été mise en œuvre de façon appropriée dans les installations « FUNDAMENT » et « CAMPUS », et le pilotage et la surveillance sont conformes aux normes usuelles. Les concepts de développement de la plateforme de digitalisation décrivent une technologie de haute sécurité et évolutive et se fondent sur des technologies éprouvées.

La situation des projets de construction est réjouissante

Les projets de construction sont bien structurés et les documents sont détaillés et de bonne qualité. Malgré des retards partiels, les projets sont en partie terminés ou en cours. La ligne de crédit des projets « CAMPUS » et « FUNDAMENT » a été respectée et la gestion des coûts s'est avérée efficace. Cependant, l'estimation des coûts du projet « KASTRO II » n'était pas encore disponible lors de l'audit. En raison du changement de site et du fait que l'installation doit être reconstruite, il faut s'attendre à des coûts supplémentaires importants.

La gestion des risques et de la qualité est en place et elle est efficace. A l'avenir cependant, les éléments présentant des risques particuliers devraient être soumis à une assurance qualité approfondie durant toutes les phases du projet.

Selon une expertise antérieure, l'exigence du cahier des charges concernant la classe de disponibilité du CC « FUNDAMENT » n'a pas été remplie dans deux domaines. Des mesures techniques ont permis d'atteindre la disponibilité exigée pour l'air comburant de la génératrice de secours. Des mesures de construction ont amélioré la conduite des gaz d'échappement. Dans le cadre du projet de construction du CC « KASTRO II », une telle vérification devrait être faite durant toutes les phases.

Des actions sont nécessaires pour les systèmes domotiques

Une grande importance a été accordée à la sécurité des systèmes domotiques dans les deux nouveaux CC. Ceux-ci ont été mis en place en fonction des besoins et des exigences de sécurité élevées de la Confédération et du DDPS. Les documents de sécurité prescrits sont disponibles, mais ils présentent des divergences avec les manuels d'exploitation et les accords de services. Ces divergences doivent être supprimées. Les mesures de réduction des risques décrites dans les concepts de sûreté de l'information et de protection des données (SIPD) ne sont pas encore appliquées de manière cohérente et leur mise en œuvre doit être planifiée et surveillée.

Les applications domotiques doivent en général être testées dans un environnement d'intégration et de test avant leur mise en service. Un tel environnement n'existe pas encore pour ces systèmes. Il faut agir d'urgence, mais le DDPS en est conscient.

Normes établies et nouvelles technologies pour la plateforme de digitalisation de l'armée

Avec le sous-projet « Architecture et infrastructure (IKT A&I) », la plateforme de haute sécurité pour la digitalisation de l'armée est mise en place. La technologie utilisée et la communication prévue répondent à la norme actuelle en matière de technique et de sécurité pour les plateformes de haute sécurité. L'exploitation et le développement de la plateforme de digitalisation constituent un grand défi pour le commandement Cyber, en cours de constitution.

Réserves de capacité pour remplacer les CC et les salles système plus petits

Lors de l'audit, les nouveaux CC sont utilisés à 20 %. Des réserves pour l'ajout d'autres systèmes et infrastructures sont disponibles dans les parties bâties. Les migrations prévues doivent permettre d'atteindre un taux d'utilisation des CC civils et militaires d'environ 50 % d'ici à fin 2024.

L'Office fédéral de la police (fedpol) exploite des applications spéciales avec des exigences élevées en matière de sécurité et de disponibilité. Dans les années 2008–2016, fedpol a planifié, avec l'Office fédéral des constructions et de la logistique, la salle système G1 qui a été achevée en 2018. Le secteur TNI l'a qualifiée d'espace CC et lui a aussi accordé une dérogation temporaire pour l'exploitation des applications. Une solution pour l'exploitation d'autres synergies a été élaborée en étroite collaboration avec le Centre de services informatiques du Département fédéral de justice et police (CSI-DFJP). A l'avenir, le CC G1 doit être exploité pour fedpol sous la responsabilité du CSI-DFJP et faire ainsi partie du réseau des CC pour pouvoir répondre aux exigences actuelles et nouvelles de haute disponibilité de Schengen grâce à un concept de géo-redondance.

Les recommandations des audits précédents ont été mises en œuvre. Les résultats sont présentés sous la forme de tableau dans l'annexe 4.

Texte original en allemand

Verifica del progetto chiave TDT centro di calcolo DDPS/Confederazione 2020

Stato maggiore dell'esercito

L'essenziale in breve

Grazie alla rete dei centri di calcolo approvata dal Consiglio federale nel luglio del 2014 si intende consolidare l'ambiente eterogeneo dell'Amministrazione federale in una rete composta di quattro centri di calcolo (CC). In tal modo se ne può ridurre sensibilmente il numero e assicurare il futuro fabbisogno in termini di capacità informatica dell'Amministrazione federale in maniera più economica e rispettosa dell'ambiente. In questo contesto, il Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS) aveva pianificato la costruzione di tre nuovi CC. Due di questi impianti vengono costruiti con una protezione militare completa, per garantire in ogni situazione il funzionamento delle applicazioni e dei sistemi rilevanti per l'esercito. Il terzo CC è utilizzato anche dai servizi dell'Amministrazione federale civile. Questo progetto globale viene attuato nel quadro del progetto chiave TDT «CC DDPS / CONFEDERAZIONE 2020» e include anche la creazione della piattaforma di digitalizzazione dell'esercito, quindi la parte TIC dei CC. I costi complessivi riguardano tutte le fasi di ampliamento e ammontano a circa 900 milioni di franchi per gli immobili e a 320 milioni per i mezzi informatici.

I risultati della verifica del progetto di costruzione sono nel complesso positivi. La gestione dei progetti è organizzata in modo mirato e la maggior parte delle scadenze e delle uscite ha potuto essere rispettata. L'automazione degli edifici è stata attuata in maniera appropriata negli impianti «FONDAMENTA» e «CAMPUS», la gestione e il monitoraggio vengono effettuati tramite standard abituali. I piani per la trasformazione della piattaforma di digitalizzazione descrivono una tecnologia altamente sicura e scalabile e si basano su tecnologie comprovate.

I progetti di costruzione si trovano in uno stadio apprezzabile

I progetti di costruzione sono ben strutturati e la documentazione è ben fatta e dettagliata. Nonostante alcuni ritardi, una parte dei progetti è conclusa e gli altri sono a buon punto. Il credito quadro dei progetti «CAMPUS» e «FUNDAMENT» ha potuto essere rispettato e la gestione dei costi è risultata efficace. Tuttavia, al momento della verifica la stima dei costi del progetto «KASTRO II» non era ancora disponibile. A causa del cambiamento di sede e del fatto che viene costruito un impianto del tutto nuovo, si devono prevedere costi aggiuntivi sostanziali.

La gestione dei rischi e della qualità è consolidata ed efficace. Ciononostante, componenti particolarmente a rischio dovrebbero essere sottoposti a un esame approfondito della qualità in tutte le fasi del progetto.

Secondo una perizia precedente, la prescrizione del capitolato d'oneri riguardante la classe di disponibilità del CC «FUNDAMENT» non è stata soddisfatta in due ambiti. Delle misure tecniche hanno permesso di raggiungere la disponibilità richiesta per l'aria di combustione dell'impianto elettrico d'emergenza. La condotta dei gas di scarico è stata migliorata tramite provvedimenti edilizi. Nel progetto per la realizzazione del CC «KASTRO II» si dovrebbe effettuare una verifica di questo tipo in ogni fase.

Necessità di intervento nei sistemi domotici

È stata attribuita una grande importanza alla sicurezza dei sistemi domotici dei due CC di nuova costruzione. L'implementazione è avvenuta nel rispetto degli elevati requisiti di sicurezza della Confederazione e del DDPS. I documenti di sicurezza prescritti sono disponibili, ma presentano delle differenze rispetto ai manuali d'esercizio e agli accordi di servizio. Queste discrepanze devono essere rettificate. Le misure descritte nei piani di sicurezza dell'informazione e di protezione dei dati (SIPD) volte a ridurre i rischi non sono ancora state implementate con coerenza, la loro attuazione deve essere programmata e controllata.

Generalmente, le applicazioni domotiche devono essere controllate in un ambiente di prova e d'integrazione prima della messa in esercizio. Per questi sistemi tale ambiente non esiste ancora. In questo ambito c'è un'urgente necessità di intervenire, riconosciuta dal DDPS.

Standard consolidati e nuove tecnologie per la piattaforma di digitalizzazione dell'esercito

Con il progetto parziale concernente le architetture e le infrastrutture informatiche viene creata una piattaforma con un'elevata sicurezza per la digitalizzazione dell'esercito. La tecnologia impiegata e la comunicazione prevista sono conformi agli standard attuali della tecnica e della sicurezza per piattaforme con un'elevata sicurezza. L'esercizio e lo sviluppo della piattaforma di digitalizzazione costituiscono una grande sfida per il Comando Ciber, attualmente in fase di allestimento.

Riserve di capacità per sostituire CC di dimensioni minori e locali per i server

Al momento della verifica i nuovi CC erano utilizzati al 20 per cento. Nelle parti di nuova costruzione sono disponibili delle riserve per l'equipaggiamento con ulteriori sistemi e infrastrutture. Con le migrazioni previste si mira a raggiungere un'utilizzazione dei CC militari e civili pari a circa il 50 per cento approssivativamente entro la fine del 2024.

L'Ufficio federale di polizia (fedpol) gestisce applicazioni speciali con elevati requisiti di sicurezza e di disponibilità. Tra il 2008 e il 2016 il locale per i server situato in G1 di fedpol è stato progettato d'intesa con l'Ufficio federale delle costruzioni e della logistica e completato nel 2018. Il TDT lo ha classificato come locale adibito a CC e ha rilasciato un'autorizzazione eccezionale limitata nel tempo anche per l'esercizio delle applicazioni. In stretta collaborazione con il Centro servizi informatici del Dipartimento federale di giustizia e polizia (CSI-DFGP) è stata ora sviluppata una soluzione per sfruttare ulteriormente le sinergie. In futuro, il CC G1 dovrà essere gestito per fedpol sotto la responsabilità del CSI-DFGP e quindi diventare parte della rete di CC, al fine di soddisfare i requisiti vigenti e nuovi di Schengen riguardanti la massima disponibilità tramite un piano a doppia ridondanza basato sulle regioni.

Le raccomandazioni formulate in verifiche precedenti sono state attuate. I risultati sono illustrati nella tabella dell'allegato 4.

Testo originale in tedesco

Audit of the DTI key project: Data centres DDPS/Confederation 2020

Armed Forces Staff

Key facts

The data centre network approved by the Federal Council in July 2014 is intended to consolidate the heterogeneous data centre landscape of the Federal Administration into a network of four data centres. This will enable the number of data centres to be significantly reduced and the future capacity requirements of the federal IT system to be met in a more cost-effective and environmentally friendly manner. Within this framework, the Federal Department of Defence, Civil Protection and Sport (DDPS) planned the construction of three new data centres. Two of these facilities will be built with full military protection to ensure the functioning of applications and systems relevant to the Armed Forces under any circumstances. The third data centre will also be used by civilian federal offices. These projects are being implemented as part of the DTI key project "Data centres DDPS/Confederation 2020". The project also includes the development of the digitalisation platform of the Armed Forces, i.e. the ICT section of the data centres. The total costs for the project, including all expansion stages, amount to around CHF 900 million for real estate and CHF 320 million for ICT resources.

The audit results of the construction projects painted a rather positive picture. The project management is structured in a target-oriented manner and the deadlines and costs have been largely met. The building automation was implemented appropriately in the FUNDAMENT and CAMPUS facilities, and the management and monitoring are in line with common standards. The concepts for setting up the digitalisation platform describe a highly secure and scalable technology and are based on tried and tested technologies.

Encouraging progress in construction projects

The construction projects are well structured and the documentation is detailed and in good order. Despite partial delays, the projects have either been completed or are on schedule. The credit framework in the CAMPUS and FUNDAMENT projects was respected and cost management proved to be effective. However, the cost estimate for the KASTRO II project was still pending at the time of the audit. Due to the change of location and the fact that the plant is to be built from scratch, significant additional costs are to be expected.

Risk and quality management is established and effective. Nevertheless, particularly risky components should be subjected to more rigorous quality assurance in all future project phases.

According to an early assessment, the requirement from the specifications concerning the availability level of the FUNDAMENT data centre was not fulfilled in two areas. The required availability for the combustion air of the emergency power system was achieved by technical means and the exhaust gas routing was improved through structural measures. In the construction project for the KASTRO II data centre, such reviews are to be carried for all phases.

Action needed for the home automation systems

The security of the home automation systems was given high priority in the two newly built data centres. They were implemented in accordance with the high security requirements of the Confederation and the DDPS. The prescribed security documents are available, but they differ somewhat from the operating manuals and the service agreements. These inconsistencies must be resolved. The risk reduction measures described in the information security and data protection (ISDS) concepts have not yet been consistently implemented, so this must be scheduled and monitored.

Home automation applications generally need to be tested in an integration and test environment before being put into operation. Such an environment does not yet exist for these systems. There is an urgent need for action here, but this has been recognised by the DDPS.

Established standards and new technologies for the digitalisation platform of the Armed Forces

The "Architecture and Infrastructure (ICT A&I)" sub-project is creating the high-security platform for the digitalisation of the Armed Forces. The technology used and the planned communication methods are in line with current technology and security standards for high-security platforms. The operation and further development of the digitalisation platform represent a major challenge for the Cyber Command, which is currently being set up.

Capacity reserves to replace smaller data centres and system rooms

At the time of the audit, the new data centres were being used at 20% of their capacity. Reserves exist in the completed parts which can be used to install additional systems and infrastructures. The planned migrations are intended to achieve a usage rate of about 50% for the military and civilian data centres by approximately the end of 2024.

The Federal Office of Police (fedpol) operates special applications which have stringent requirements in terms of security and availability. The Federal Office for Buildings and Logistics, together with fedpol, planned the system room in centre G1 between 2008 and 2016, and it was completed in 2018. The DTI classified this as a data centre room and also granted a temporary exemption for the operation of the applications. In close cooperation with the IT Service Centre of the Federal Department of Justice and Police (ISC-FDJP), a solution has now been developed for the further exploitation of synergies. In the future, data centre G1 is to be operated for fedpol under the responsibility of the ISC-FDJP and thus become part of the data centre network, in order to be able to satisfy the existing requirements, as well as the new Schengen ones, for maximum availability through a dual-redundant regional concept.

The recommendations from previous audits have been implemented. The results are presented in the tables in Appendix 4.

Original text in German

Generelle Stellungnahme der Geprüften

fedpol

fedpol bedankt sich bei den Prüfenden für die intensive Auseinandersetzung mit den Themen rund um das RZ-G1. Wir haben die sich daraus ergebenden, interessanten Diskussionen im Rahmen der Interviews sehr geschätzt. Die Erkenntnis der EFK, dass das RZ G1 für fedpol künftig in der Verantwortung des ISC-EJPD betrieben und Teil des RZ-Verbunds werden soll, bestätigt uns in unserer mit dem ISC-EJPD bereits eingeschlagenen Stossrichtung zur weiteren Synergienutzung der RZ-Kapazitäten im EJPD.

Gruppe Verteidigung und armasuisse

Gruppe Verteidigung und armasuisse bedanken sich bei der EFK für die stets transparente und zielführende Zusammenarbeit und Diskussion. Praktisch alle von der EFK gemachten Empfehlungen betreffen Sachthemen, bei welchen auch die Gruppe V und armasuisse Handlungsbedarf sehen und diesen zu beträchtlichen Teilen bereits vor der Prüfung durch die EFK in Angriff genommen haben. Es ist im Gesamtrahmen hilfreich und bestätigt unsere eigenen Analysen, wenn die Aussensicht der EFK dieselben Punkte aufbringt und die Gruppe V und armasuisse in ihren Wahrnehmungen bestätigt und die Umsetzung der entsprechenden Massnahmen gutheisst bzw. fordert und somit unterstützt.

1 Auftrag und Vorgehen

1.1 Ausgangslage

Der Bundesrat (BR) strebt mit der IKT-Strategie des Bundes einen Verbund der Rechenzentren (RZ) für die zentrale Bundesverwaltung (BV) an. Am 2. Juli 2014 hat der BR das Konzept «Rechenzentren-Verbund für die zentrale Bundesverwaltung» genehmigt, welches als Zielbild vier bundeseigene RZ vorsieht. Vorgesehen sind zwei mit militärischem Vollschutz sowie zwei mit einem Schutzniveau, das den gängigen zivilen Anforderungen entspricht. Es handelt sich um die militärischen Rechenzentren «FUNDAMENT» und «KASTRO II», das neu erbaute RZ «CAMPUS» in Frauenfeld sowie um das bestehende zivile Rechenzentrum (RZ) «PRIMUS» in Bern. Das RZ «CAMPUS» in Frauenfeld wird sowohl zivil als auch militärisch genutzt und ist seit Anfang 2021 in Betrieb.

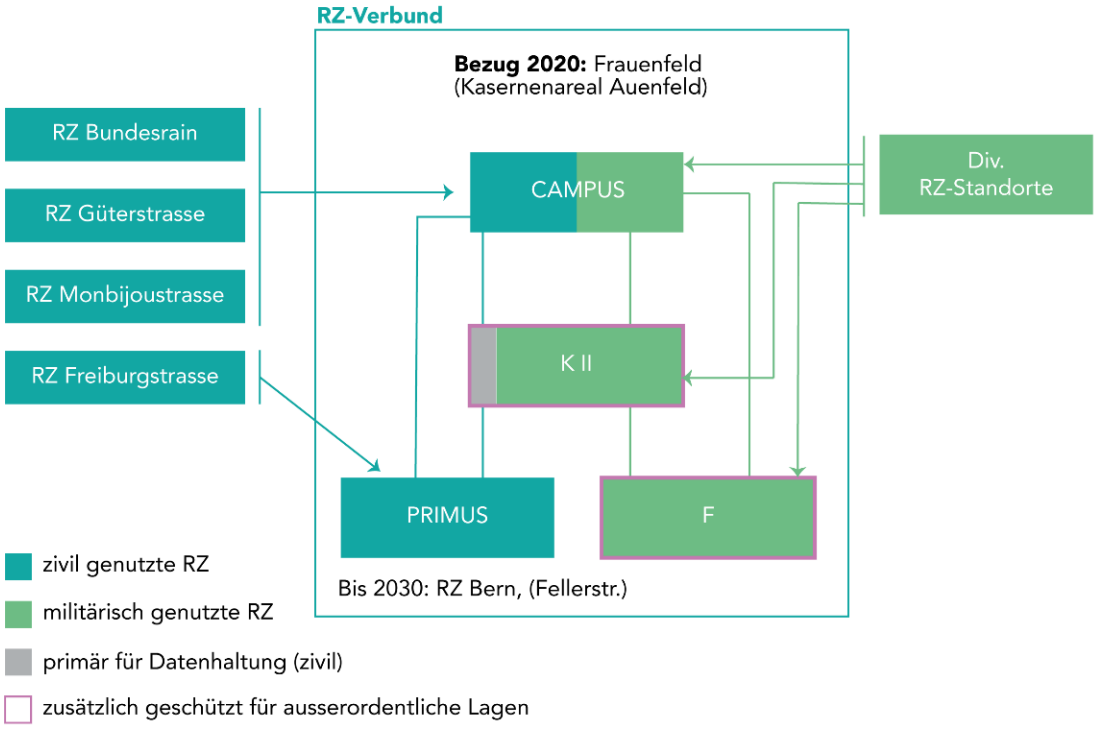

Abbildung 1: Zielbild RZ-Verbund (Quelle: EFK)

Der Bau des RZ-Verbunds der BV ist Teil der Datacenter-Strategie Bund. Mit dem DTI-Schlüsselprojekt «RZ VBS/Bund 2020» der Armee werden die drei Rechenzentren – «FUNDAMENT», «KASTRO II» und «CAMPUS» – im Zeitraum von 2014 bis 2028/29 im Rahmen des Programms «FITANIA» realisiert. Die Gesamtkosten für den militärischen Teil des Projekts belaufen sich über alle Ausbaustufen hinweg auf rund 900 Millionen Franken für den Immobilienteil und auf 320 Millionen für die IKT-Mittel.

1.2 Prüfungsziel und -fragen

Mit der Prüfung beurteilt die EFK das DTI-Schlüsselprojekt hinsichtlich der Projektrisiken und der Zielerreichung. Die Prüffragen lauteten:

1. Läuft das Projekt inhaltlich, zeitlich und kostenmässig nach Plan?
2. Besteht ein angemessenes Risiko- und Qualitätsmanagement?
3. Sind die Angaben im letzten halbjährlichen Reporting über die DTI-Schlüsselprojekte des Bundes zuhanden der Finanzdelegation verlässlich bzw. plausibel?
4. Besteht eine belastbare Kapazitäts- und damit abgestimmte Migrationsplanung?
5. Besteht eine belastbare auf die Betriebsanforderungen und Risiken abgestimmte IKT-Sicherheitsarchitektur?
6. Werden kritische Abhängigkeiten (Lieferanten, Architektur, andere Projekte, Ressourcen, Externe) in den Projekten gesamthaft und wirksam gesteuert?
7. Wurden relevante als erledigt gemeldete Empfehlungen aus früheren Prüfungen (15511, 16613, 17410, 18491) umgesetzt?

1.3 Redimensionierung des Prüfauftrages

Eine Durchsicht der Projektstatusberichte der letzten Jahre ergab ein durchzogenes Bild: Während die drei Bauprojekte «CAMPUS», «FUNDAMENT» und «KASTRO II» per Ende Juni 2021 allesamt ʻgrünʼ rapportieren, wird für das Teilprojekt «Architektur und Infrastruktur (IKT A&I)» bereits seit 2020 ein ʻroterʼ Status gemeldet.

«IKT A&I», unter der Verantwortung der Führungsunterstützungsbasis (FUB) bzw. dem Projekt Kommando Cyber (Kdo Cy)[1], ist für die bedarfsgerechte IKT-Ausrüstung der Rechenzentren verantwortlich. Der ‘rote’ Status des Teilprojekts «IKT A&I» wird mit dem Mangel an geeigneten Personalressourcen begründet. Das Ziel, gleichzeitig den Aufbau der künftigen Plattformen wie auch den Betrieb der bestehenden IKT-Landschaft sicherzustellen erschien gefährdet. Dies führte dazu, dass nun auch der Gesamtstatus des DTI-Schlüsselprojekts «RZ VBS/Bund 2020» im Bericht per Ende Juni 2021 mit ‘rot’ rapportiert wird. Dies ist insofern nachvollziehbar, als ein RZ ohne ausgebaute IKT-Infrastruktur lediglich eine Bauhülle ohne jeden weiteren Nutzen darstellt.

Gemäss dem Bericht «DTI-Schlüsselprojekte des Bundes – Statusbericht» per Ende Juni 2021 wird rapportiert, dass die internen Ressourcen im Bereich der bestehenden Infrastrukturen für das Testing, den Knowhow-Aufbau sowie den eigenständigen, sicheren Betrieb der neuen Plattformen nicht zur Verfügung gestellt werden können. Von der Armeeführung bewilligte Massnahmen wie die «Fokussierung der FUB» sowie eine revidierte «Gesamtplanung V» hätten bezüglich Personalsituation im 2. Quartal 2021 noch nicht die erhoffte Wirkung gezeigt. Der Projektabschluss von «IKT A&I» per Mitte 2026 könne nur gehalten werden, sofern Ressourcen und Finanzen garantiert werden. Sofern die neuen Plattformen durch das Teilprojekt «IKT A&I» nicht bereitgestellt werden können, sind auch weitere zentrale Projekte des VBS gefährdet, da sie nicht auf der zentralen Plattform des VBS in den neuen Rechenzentren aufgesetzt werden

[1] Siehe Exkurs in Kapitel 2.2.

können. Als besonders kritisch wurde die Finanzierung des Teilprojekts «Secure Data Interchange» (SDI) innerhalb von «IKT A&I» bewertet, da dessen Finanzierung bis und mit Ende Mai 2021 nicht zugesichert werden konnte.

Diese Probleme haben bereits eine hohe Visibilität und Aufmerksamkeit und werden bearbeitet. Die EFK hat sich daher aus Risikoüberlegungen entschieden, sich auf die Bauprojekte und die verbleibenden Fragen 4 bis 6 und Teile von 7 zu fokussieren. Die offenen Empfehlungen aus der Prüfung 16613 beziehen sich ebenfalls auf eine DTI-Schlüsselprojektprüfung und wurden daher auch nicht in dieser Prüfung verifiziert.

1.4 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Roland Gafner (Revisionsleiter), Nadine Sünneke, Stefan Schmidt, Roger Brodmann und Daniel Wyniger vom 16. August bis 1. September 2021 durchgeführt. Die Federführung lag bei Bernhard Hamberger. Das Revisionsteam wurde durch eine externe Firma unterstützt.

Die Beurteilungen orientieren sich in technischer Hinsicht an der «Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (CyRV)», dem «IKT-Grundschutz der Bundesverwaltung[2]» und der «Netzwerksicherheit in der Bundesverwaltung[3]». Weiter kamen die Empfehlungen der International Organization for Standardization (ISO/IEC) Standards 2700x und das TIER Classification System des Uptime Institut zur Anwendung.

Das frühere Projekt «KASTRO II» ist nicht Bestandteil dieser Prüfung. Der Standortwechsel und seine Auswirkungen wurden nicht geprüft.

Die Ergebnisbesprechung hat am 4. November 2021 stattgefunden. Der vorliegende Bericht berücksichtigt nicht die weitere Entwicklung nach der Ergebnisbesprechung.

1.5 Unterlagen und Auskunftserteilung

Die notwendigen Auskünfte wurden der EFK von den geprüften Verwaltungseinheiten (VE) umfassend und zuvorkommend erteilt. Die gewünschten Unterlagen standen dem Prüfteam vollumfänglich zur Verfügung.

1.6 Schlussbesprechung

Die Schlussbesprechung fand am 25. April 2022 statt. Teilgenommen haben seitens Gruppe Verteidigung, der Projektleiter Kommando Cyber, der Chef Führungsunterstützungsbasis a.i., der Programmmanager FIATANIA, der Chef Betrieb, der Chef Erneuerung, der Chef Cyber Security und der Projektleiter und Projektleiter Stv. «RZ VBS/Bund 2020». Die armasuisse war vertreten durch den Leiter armasuisse Immobilien und den Leiter Baumanagement Mitte. Das GS-VBS war durch den Stabschef vertreten. Die Bundeskanzlei war vertreten durch den Delegierten Digitale Transformation und IKT-Lenkung. Von Seiten EJPD haben teilgenommen, der Abteilungschef Infrastruktur, Betrieb & Services und der Bereichsleiter Informatik. Die EFK war vertreten durch zwei Mandatsleiter, den Federführenden und den Revisionsleiter.

[2] Si001 – IKT-Grundschutz in der Bundesverwaltung, Version 4.6 vom 19. Dezember 2013 (Stand 1. April 2021)
[3] Si003 – Netzwerksicherheit in der Bundesverwaltung

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

EIDGENÖSSISCHE FINANZKONTROLLE

2 Das Projekt RZ VBS/Bund 2020

2.1 Die Projektorganisation entspricht den Anforderungen

Das Projekt «RZ VBS/Bund 2020» ist in vier Teilprojekte gegliedert, drei Bauprojekte und ein IKT-Projekt.

- Die drei Rechenzentren werden geografisch getrennt voneinander realisiert und redundant betrieben. Anfang 2020 wurde das teilgeschützte RZ «CAMPUS» dem IT-Betrieb übergeben. Systeme des Bundesamts für Informatik und Telekommunikation (BIT) und des Informatik Service Center des Eidgenössischen Justiz- und Polizeidepartements (ISC-EJPD) sind bereits produktiv. Ende 2020 wurde das vollgeschützte RZ «FUNDAMENT» ebenfalls dem Betrieb übergeben.
- Das dritte RZ «KASTRO II» ist wie das RZ «FUNDAMENT» vollgeschützt und soll gemäss aktuellem Stand im laufenden Jahrzehnt in Betrieb genommen werden. Weitere Ausbauetappen werden entsprechend den Bedürfnissen der Benutzer voraussichtlich in den 2030er Jahren realisiert werden.
- Das Teilprojekt «IKT A&I» soll mit einer standardisierten Digitalisierungs-Plattform die Voraussetzungen für einen robusten, hochsicheren und effizienten Betrieb von einsatzrelevanten Anwendungen der Armee über alle Lagen schaffen.

Die Schnittstelle zwischen Bau- und IKT-Projekt ist bei allen drei Rechenzentren gleich definiert. Das Bauprojekt beinhaltet die Installation der Racks und die integralen Tests der technischen Gebäudekomponenten und den Nachweis der geforderten Funktionalitäten unter Volllast. Die Installation der Server und aller weiteren IKT-Komponenten in den Rechenzentren liegt beim IT-Betrieb.

Die Projektorganisation ist nach HERMES aufgebaut und berücksichtigt die unterschiedlichen Akteure.

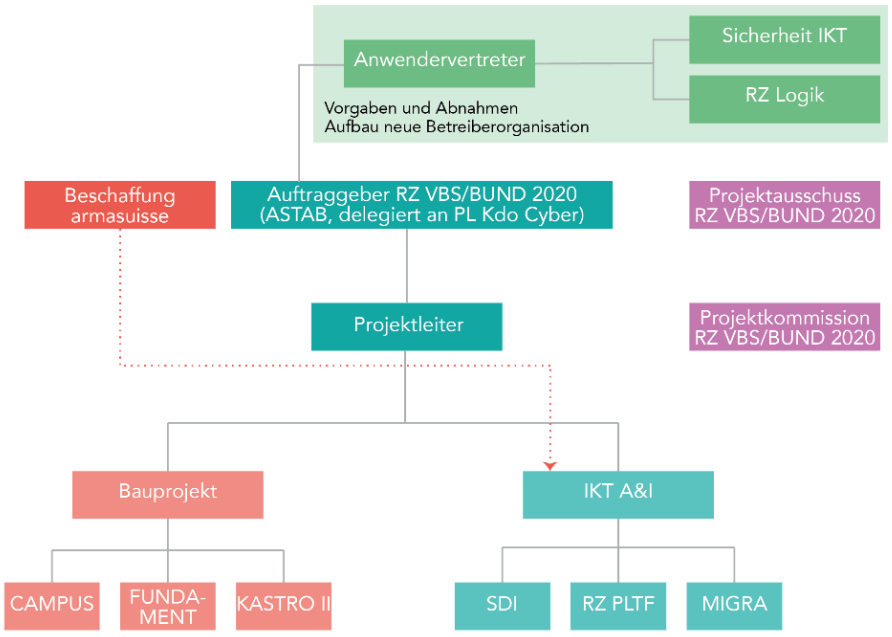

Abbildung 2: Vereinfachte Darstellung der Projektorganisation (Quelle: Kdo Cy, Darstellung: EFK)

Erläuterungen zu «IKT A&I»:

- SDI = Teilprojekt Secure Data Interchange (siehe Kapitel 5)
- RZ PLTF = Teilprojekt Plattform
- MIGRA = Teilprojekt Migration (siehe Kapitel 2.2)

2.2 Hohe Abhängigkeiten und ein knapper Zeitplan

Die Projekte «Telekommunikation der Armee», «RZ VBS/Bund 2020» und «Führungsnetz Schweiz (Fhr Netz CH)» hängen stark voneinander ab und werden untereinander über das Programm Führungsinfrastruktur, Informationstechnologie und Anbindung an die Netzinfrastruktur der Armee (FITANIA) koordiniert. Dabei stimmen sich die Gesamtprojektleitung und die Projektleiter viermal jährlich mit dem Programm FITANIA und dem Chef der Armee (CdA) ab.

Innerhalb des Projekts RZ VBS/Bund 2020 finden neben vier Projektausschuss (PA) Sitzungen pro Jahr unterschiedliche Austausch- und Steuerungsmeetings zwischen Gesamtprojektleitung und Projektleiter und zwischen Projektleiter und Teilprojektleiter statt.

Das Projekt «IKT A&I» verfügt, trotz der zum Prüfzeitpunkt kritischen Ressourcensituation, über eine plausible Terminplanung. Der Meilenstein «Systemintegrationstest abgeschlossen» ist auf Ende August 2024 terminiert, so dass danach das erste Referenzsystem auf die IKT-Plattform migriert werden kann. Die vorliegenden Informationen zeigen, dass verschiedene Herausforderungen im Projekt und dessen Umfeld die Zielerreichung negativ beeinflussen könnten:

- Aktuell fehlendes Knowhow und Ressourcen im Projekt und der Betreiberorganisation (FUB oder Kdo Cy);
- Unsicherheiten bei Mitarbeitenden der FUB und des Projektes aufgrund des anstehenden Transfers der FUB zum Kdo Cy (siehe Exkurs);
- Genehmigung von Changes, die den Projektumfang und -inhalt verändern.

Die Herausforderungen sind im Umfeld des Projektes bekannt und entsprechend adressiert. Um die kritische Situation bezüglich Ressourcen und finanziellen Mitteln zu stabilisieren, müssen wirksame Massnahmen ergriffen werden. Die notwendigen Entscheide werden von der Armeeführung im Oktober 2021 gefällt.

Die FUB im Wandel zum Kommando Cyber

Im Oktober 2020 hat der BR die Vernehmlassung zu diversen Änderungen des Militärgesetzes und der Organisation eröffnet. Insbesondere will er ein Kommando Cyber (Kdo Cy) schaffen und die Milizbestände in diesem Bereich ausbauen. Der Plan des Bundesrats sieht vor, dass die FUB auf Anfang 2024 zumindest teilweise in dieses Kdo überführt werden soll. Das Kdo Cy soll künftig die militärischen Schlüsselfähigkeiten in den Bereichen Lagebild, Cyberabwehr, IKT-Leistungen, Führungsunterstützung, Kryptologie und elektronische Kriegführung bereitstellen.

Gemäss dem genehmigten Teilprojektauftrag hat das Teilprojekt Gesamtplanung und Migration Referenzsysteme (MIGRA) (siehe Abbildung 2), zum Ziel, die Initialisierung der Migration sämtlicher Kernleistungen vorzunehmen und die Migration der Referenzsysteme durchzuführen. Im April 2021 werden 13 Referenzsysteme ausgewiesen. Das Teilprojekt MIGRA befindet sich aktuell in der Konzeptphase, die per April 2023 abgeschlossen werden soll. In dieser Konzeptphase werden für jedes Referenzsystem die Ist-Situation, Anforderungen und Lösungsvarianten für die Migration erhoben. Diese Arbeiten münden in einer Projektstudie pro Referenzsystem. Im Anschluss folgt pro Referenzsystem ein einzelnes Migrationsprojekt.

Neben den oben erwähnten Infrastrukturprojekten stehen auch Kundenprojekte in direkter Abhängigkeit. Dabei stellt das Programm «Air2030» welches die Überwachung und den Schutz des Luftraums sicherstellen soll, ein zentrales Vorhaben dar. Damit dieses Programm erfolgreich abgeschlossen werden kann, ist es unabdingbar, dass die Digitalisierungsplattform bis 2024 in Betrieb genommen werden kann.

Beurteilung

Die Ressourcen- und Knowhow-Situation und der anstehende organisatorische Transfer der FUB zum Kdo Cy stellen eine grosse Herausforderung dar. Fehlendes internes Wissen könnte zu längerfristigen Abhängigkeiten von externen Partnern führen. Ohne Entscheide der Armeeführung bezüglich Ressourcen und finanziellen Mitteln, sowie einer klaren Planung und Kommunikation des Transfers von der FUB zum Kdo Cy, könnte der ehrgeizige Terminplan und somit auch abhängige Projekte gefährdet werden.

Sollten die Referenzsysteme nicht ab Januar 2024 auf die Digitalisierungsplattform migriert werden können, besteht das Risiko, dass Alternativlösungen gesucht und umgesetzt werden müssen. Dies würde den zeitnahen Abbau der bestehenden RZ und Systemräume verzögern und weitere Betriebskosten verursachen. Der Weiterbetrieb könnte auch zu einer sinkenden Zuverlässigkeit der Systeme führen. Daher ist es erforderlich, dass die Plattformbetreiber die genauen Systemanforderungen bzw. -fähigkeiten der Plattform spezifizieren und diese den verschiedenen Projektstudien gegenübergestellt werden. Dabei ist sicherzustellen, dass die bestehenden Anwendungen laut gültigem Terminplan auf die standardisierte Plattform migriert werden können. Hierbei sind, im Rahmen einer Qualitätssicherung und Kontrolle der Terminplanung, der kritische Pfad, Risiken, Ressourcen und Kosten transparent, plausibel und konsolidiert darzulegen. Die Anforderungen an die Anwendungen sollen dabei bereits bei der Ausschreibung von Migrations- oder Beschaffungsprojekten definiert werden.

3 Aspekte der Bauvorhaben

3.1 Die Bauvorhaben der drei Rechenzentren sind gut strukturiert und dokumentiert

Pflichtenhefte liegen für alle drei Rechenzentren vor und beschreiben die wesentlichen Anforderungen in den Bereichen Leistung, Schutz gegen Waffenwirkung, Sicherheit, Verfügbarkeit und Infrastruktur. Basierend auf den Pflichtenheften wurden die Vorprojekte entwickelt. Etwaige Abweichungen zum Pflichtenheft sind im Abschlussbericht der Vorprojektphase festgehalten. Ab Stufe Bauprojekt bestand ein Change-Management-Prozess. Die Changes sind im Detail dokumentiert und bei den Projekten «FUNDAMENT» und «CAMPUS» vom PA unterzeichnet. Kosten-, Termin- und Qualitätsauswirkungen sind für die Changes ausgearbeitet, sowohl für Planungen als auch für die Ausführung. Beide Projekte verfügen über weniger als 50 Changes in einer Bandbreite zwischen 10 000 und 1.5 Millionen Franken. Gemessen am Kredit sind die Changes im tiefen einstelligen Prozent Bereich. Die Schnittstellen zwischen Bauprojekt und IKT-Projekt sind klar definiert und plausibel. Die Ausführungsstrategie der drei Rechenzentren ist konventionell mit einem Generalplaner (GP) und ausführenden Firmen, welche im direkten Vertragsverhältnis zur armasuisse stehen. Dies wurde gewählt, um die höchst mögliche qualitative Umsetzung der Anforderungen der Pflichtenhefte bei grösster möglicher vertraglicher Flexibilität zu gewährleisten.

Beim Projekt «FUNDAMENT» sind zwei Mängel aufgetreten, welche zu Verzögerung des Bauprojektes geführt haben. Die Mängelaufnahme, die Behebung und Aufarbeitung der Mangelentstehung sind gut dokumentiert.

Beurteilung

Die Erstellung und Fortschreibung der Pflichtenhefte im gesamten ist positiv zu werten. Die Anforderungen und Changes sind klar beschrieben und formal freigegeben. Bei «FUNDAMENT» und «CAMPUS» wird nicht von den definierten Standards laut Pflichtenheft abgewichen. So wurden teure bauherrenseitige Projektanpassungen mit Termin- und Kostenauswirkungen während der Projektlaufzeit vermieden. Dass die Pflichtenhefte bis Ende Vorprojekt gut definiert wurden, wird deutlich durch die geringe Anzahl von bauherrenseitigen Changes über die gesamte Projektlaufzeit. Hervorzuheben ist, dass bereits im Pflichtenheft eine klare Definition der Leistungsgrenze bestand zwischen Bau und IKT und diese auch in den Verträgen mit dem GP und im Projekt IKT stringent weiterverfolgt wurden. Im Terminplan sind die Meilensteine der Pflichtenhefte der drei Rechenzentren klar abgebildet. Die Ausführungsstrategie entspricht der Komplexität der Anforderungen der Pflichtenhefte. Die konventionelle Ausführungsstrategie im Gegensatz zur Beauftragung eines Totalunternehmers ist zielführend.

3.2 Die Projekte sind trotz Verzögerungen auf Kurs oder bereits abgeschlossen

Der ursprüngliche Übergabetermin für das RZ «FUNDAMENT» wurde laut Botschaft auf Mitte 2018 festgesetzt. Durch die zwei wesentlichen Schäden bei der Bodenplatte und dem Abgasstollen hat sich die Übergabe des RZ an die Betreiber auf Ende Dezember 2020 verschoben. Da die Entwicklung der IKT-Plattform verspätet ist, hat die Verzögerung des Bauprojekts keine weiteren Auswirkungen auf das Gesamtprojekt. Der Testbetrieb läuft seit Abschluss der integralen Tests Anfang 2020. Die integralen Tests konnten erfolgreich beendet werden und das Projekt «Optima» zur Optimierung der betrieblichen Prozesse wurde gestartet. Dies wird im 2022 abgeschlossen.

Das RZ «CAMPUS» wurde im Terminrahmen abgewickelt und Ende Februar 2020 dem Betreiber übergeben. Auch hier soll das Projekt «Optima» im 2022 die technische Gebäudeinfrastruktur verbessern und Mängel beheben. Da die Entwicklung der militärischen IKT-Plattform verzögert ist, wird ein grosser Teil des RZ nur gebäude- und sicherheitstechnisch betrieben. Zum Prüfzeitpunkt war der Aufbau der Testinfrastruktur für das Projekt «IKT A&I» in Umsetzung und die Migration bzw. der Aufbau der SAP S4HANA Infrastruktur in Planung. Im zivilen Teil des RZ wurde mit dem Aufbau und Betrieb der operativen Serveranlagen begonnen.

Wesentlich verzögert zur Basisterminplanung ist das Projekt RZ «KASTRO II». Dieses resultiert aus dem notwendigen Standortwechsel. Ende Mai 2021 wurde entschieden, den geplanten zivilen Nutzungsanteil aus dem «KASTRO II» Projekt herauszulösen. Definitive Aussagen über den Fertigstellungstermin liegen mit Ende des Vorprojekts Ende Q2 2022 vor.

Beurteilung

Die Verzögerungen von «FUNDAMENT» und «KASTRO II» haben keine Auswirkungen auf die redundante RZ-Strategie Bund. Die verspätete Entwicklung der IKT-Plattform kann mit bestehenden Rechenzentren überbrückt werden. Die bestehenden RZ sollten jedoch aus Sicht der EFK so rasch als möglich geräumt werden.

Einzig bei einer ausserordentlichen Lage mit Waffeneinsatz wäre die gewünschte Georedundanz nicht sichergestellt. In einem solchen Fall müsste der einsatzrelevante, militärische Teil des RZ «CAMPUS» gemäss den Genfer Konventionen[4] heruntergefahren werden. Es wird jedoch heute vom Betrieb bereits sichergestellt, dass solche Anwendungen nicht im RZ «CAMPUS» betrieben werden.

Beim RZ «FUNDAMENT» führten zwei wesentliche Schäden zu einer Verschiebung der Übergabe an den Betreiber. Der ursprüngliche Terminplan Bau 2018 laut Botschaft wurde um eineinhalb Jahre überschritten. Im Verhältnis zur Komplexität des Umbaus einer bestehenden unterirdischen Anlage, mit den hohen technischen Anforderungen und der langen Projektlaufzeit ist dieses jedoch verkraftbar und in entsprechenden Changes genehmigt. Trotz der Verzögerung konnte der Kreditrahmen eingehalten werden.

Die Einhaltung der Termine und Unterschreitung der Kosten bei «CAMPUS» ist positiv hervorzuheben.

[4] Genfer Abkommen über den Schutz von Zivilpersonen in Kriegszeiten vom 12. August 1949 (Stand am 18. Juli 2014)

3.3 Der Kreditrahmen bei «FUNDAMENT» und «CAMPUS» wird nicht überschritten

Der Kostenstand der drei RZ wird monatlich im Zusammenhang mit dem Projektstatusreport (PSR) von den Projektleitern an den Programmleiter «FITANIA» gemeldet. Der PA wird so auf dieser Basis monatlich über den Kostenstand informiert. Die Ist-, Obligo-[5] und Endkostenprognose der Kosten sind nachvollziehbar und die Kredite sind dargestellt. SAP[6] als Kostencontrolling Tool wird nicht umfänglich genutzt. Das Projektcontrolling erfolgt mit anderen Werkzeugen wie Messerli[7], welches vom GP gesteuert wird. Dafür ist ein monatlicher manueller Abgleich zwischen den Anwendungen notwendig.

Der Kredit für den Bau des RZ «FUNDAMENT» beträgt inklusive Reserve laut Botschaft 157 Millionen Franken. Laut Endkostenprognose kann das Budget eingehalten werden. Der Projektabschluss inkl. Kreditabrechnung ist im 2022 geplant. In der Endkostenprognose sind die Kosten für das Projekt «Optima» in Höhe von [redacted] enthalten. Hinzu kommen die gesprochenen Kredite für die Finanzierung der Schadensfälle von [redacted]. Bei den Mängeln handelt es sich um wesentliche, die Funktionsfähigkeit betreffende Bauteile, welche jedoch kostenmässig, gemessen an der Gesamtbausumme, weniger relevant sind. Die Zwischenfinanzierung der Schadensfälle erfolgt über einen gesonderten Kredit. Die armasuisse klärt zum Zeitpunkt der Prüfung die rechtliche und finanzielle Verantwortung für die Schadensfälle ab. Ein Vergleich mit den beteiligten Parteien und deren Versicherungen wird angestrebt, dabei geht es insbesondere um die «Ohnehin-Kosten»[8] des Schadens. Sollten sich aus den Schäden finanzielle Nachteile für den Bauherrn ergeben, so werden diese nicht dem Projekt belastet, sondern dem Schadenskredit laut Prozessbeschrieb. Ausserdem sind noch Nachforderungen des GP zu klären. Laut Schlussrechnung geht es um Forderungen in der Höhe von [redacted], welche seitens armasuisse bestritten werden. Der GP klagt die Summe aktuell nicht ein, aussergerichtliche Verhandlungen laufen. Nach Einschätzung der armasuisse ist die Forderung des GP unberechtigt. In der Endkostenprognose des Projektes gibt es für die Nachtragsforderungen keine Rückstellung. Wird ein Teil der Nachtragsforderungen valid, führt das zu einer Überschreitung des Kreditrahmens.

Der Kredit für das RZ «CAMPUS» beläuft sich laut Botschaft auf 136 Millionen Franken plus ca. 14 Millionen Franken Reserve. Laut Endkostenprognose schliesst das Projekt mit 115 Millionen Franken ab. In der Endkostenprognose sind die Kosten für das Projekt «Optima» in Höhe von [redacted] enthalten. Es gibt keine wesentlichen und pendenten Schadensfälle.

Das Projekt «KASTRO II» wird überarbeitet und befindet sich noch in der Vorprojektphase. Die Zusammenführung mit dem erneuerungsbedürftigen, zivilen RZ «PRIMUS» entfällt und das Projekt wird redimensioniert. Der Kostenvoranschlag ist geplant für das Ende der Vorprojektphase Ende Q2 2022.

---

5 Obligo wird im Finanzwesen für die Zahlungsverpflichtungen verwendet.

6 Das SAP-ERP-System, ist der Oberbegriff für die Anwendungs- und Systemmodule von SAP, mit denen Unternehmen ihre Geschäftsprozesse innerhalb eines einheitlichen Systems managen können

7 Softwarelösungen für die Baubranche

8 Als «Ohnehin-Kosten», auch «Sowieso-Kosten» genannt, werden die Kosten bezeichnet, welche bei ordentlicher Planung von Anfang an erkannt worden wären, aber eben unerkannt blieben. Sie fallen an, wenn der Bau korrekt erstellt werden soll. Sie entstehen regelmässig bei der Nachbesserung im Werkvertragsverhältnis, wenn der Unternehmer Leistungen erbringt, die bei ursprünglich mängelfreier Ausführung auch entstanden wären. Der Bauherr hat diese Kosten gegenüber dem Unternehmer zu tragen. Gegenüber dem Architekten sind «Ohnehin-Kosten» jedoch Mehrkosten aus falscher, da unvollständiger Planung. Kann dem Architekten Verschulden angelastet werden, so haftet er für Mehrkosten. (Quelle: weka.ch)

Beurteilung

Die Kostenkontrolle in SAP sollte gestärkt werden, da es momentan unmöglich ist via SAP einen Bericht zum Kostenstand zu generieren oder die Kosten mit den im PSR dargestellten Kosten zu vergleichen. Für das Projekt «KASTRO II» wäre es von Vorteil, dass SAP Controlling robuster aufzusetzen im Hinblick auf einen Projektstrukturplan (PSP) nach Baukostenplanstruktur (BKP) bis hin zu hinterlegten Abschreibungszeiträumen. Dadurch würde das Kostencontrolling der armasuisse gestärkt, die Schnittstellen zum GP reduziert und die Abhängigkeit vom GP verringert.

Positiv wird gesehen, dass der Kredit für das RZ «FUNDAMENT» der Botschaft inkl. 5 Prozent Sicherheit eingehalten wird. Das projektseitige Kostenmanagement ist im gesamten positiv zu sehen, da es sich um einen Prototyp im Vollschutz handelt, mit sehr hoher technischer Komplexität und vielen Schnittstellen. Hinzu kommt, dass ein Umbau und eine Umnutzung einer bestehenden Anlage ein hohes Risikopotential aufweisen. Die lange Laufzeit und die Teuerung erschweren eine exakte Endkostenprognose zum Zeitpunkt der Botschaft.

Ebenso wurden die zwei wesentlichen Schadensfälle technisch gut gelöst. Aufgrund der Komplexität der Schäden und unter Berücksichtigung der örtlichen Gegebenheiten, sowie der Tatsache, dass seitens des DTI-Schlüsselprojekts kein zeitlicher Druck bestand, erscheint die benötigte Zeit von ca. zwei Jahren akzeptabel. Die beim RZ «FUNDAMENT» aufgetretenen zwei wesentlichen Schäden sind bau- und nicht technikgetrieben. Die Schäden sind nicht der Projektausführungsstrategie geschuldet. Dies erstaunt umso mehr, als es sich beim GP um einen baugetriebenen Generalplaner handelt, dessen Kompetenz ursprünglich im Ingenieurbau zu finden ist. Die Auswahl des Generalplaners für das 3. RZ («KASTRO II») erfolgte unter Einbezug der «Lessons learnt» aus den Rechenzentren «FUNDAMENT» und «CAMPUS». Der gewählte Generalplaner ist technikgetrieben, sieht aber den ingenieurstechnischen Untertagebau als besondere Herausforderung an und stellt mit zwei Subplanern ein für das Vorprojekt nachvollziehbares Generalplaner Projektteam auf.

Auch wenn die Prozesse der armasuisse Immobilien die Zerstückelung der Gesamtprojektkosten in Botschaftskredit, Planungskredit, Schadensfallkredit und internes Engineering vorsehen, wäre es wünschenswert, diese konsolidiert darzustellen. Somit könnten Projekte besser miteinander verglichen und Gesamtkostenrechnungen erstellt werden.

Das projektseitige Kostenmanagement beim Bau des RZ «CAMPUS» ist im gesamten positiv zu sehen. «CAMPUS» weist weniger Komplexität, geringere technische Anforderungen und weniger Schnittstellen auf als «FUNDAMENT». Eine zusätzliche Anforderung war hier die Koordination für den zivil genutzten Teil der Anlage. Positiv wird auch gesehen, dass der vom Parlament gewährte Kredit um rund 10 Prozent unterschritten wird. Dieses ist zum einen Vergabeerfolgen geschuldet, zum anderen hat der Generalplaner zu hohe Sicherheitszuschläge in den Kostenvoranschlag eingesetzt. Eine Prüfung der Kostenschätzung des Generalplaners in Hinblick auf eine transparente Darstellung der Sicherheitszuschläge ist grundsätzlich als «Lessons learnt» zu sehen. Eine Gesamtkostenzusammenstellung wäre hier ebenfalls wünschenswert.

Es ist zielführend, dass armasuisse Immobilien und der Generalplaner eng zusammenarbeiten, um das Projekt «KASTRO II» bei gleichbleibender Leistung zu redimensionieren, nachdem der zivile Teil entfallen ist. Im Vorprojektstadium zum Zeitpunkt der Prüfung ist eine deutliche Volumenreduktion realistisch und wird vom Projektteam verfolgt. Aus diesem Grund sieht die EFK von einer Empfehlung ab. Es ist wichtig, dass die Kosten am Ende des

Vorprojektes (Q2 2022) plausibel und nachvollziehbar im Hinblick auf nachstehende Punkte aufgestellt werden:

1. Darstellung der «Worst case»-Szenarien (Einbezug in die Risikobetrachtung).
2. Darstellung der gesamten angelaufenen Kosten für «KASTRO II» und deren Verrechnung

3.4 Ein Risiko- und Qualitätsmanagement ist etabliert und nachvollziehbar aufgestellt

Gemäss Prozessanweisung ar Immo wird zur Sicherstellung des übergeordneten Total Quality Management (TQM) das Dokument Qualitätslenkungsplan (Q-Lenkungsplan) erstellt. In diesem werden das Projekt, die Grundlagen und die Ziele phasengerecht kurz umschrieben, zudem wird der Projektstand dokumentiert. Hauptthema ist das Risikomanagement (RM), in welchem die Risikobetrachtung sowie die Definition von Massnahmen zur Risikominimierung behandelt werden. In den vorliegenden Q-Lenkungsplänen der Rechenzentren «CAMPUS» und «FUNDAMENT» wurden über die Länge der Projektlaufzeit bis Übergabe an den Betreiber die Qualitätsanforderungen fortgeschrieben und nach den Prozessanweisungen erstellt. Für das RZ «KASTRO II» wurde im Vorprojekt ein Q-Lenkungsplan erstellt.

In Bezug auf das Qualitätsmanagement sind folgende Sitzungen etabliert: Es gibt monatliche Abstimmungen zum Q-Lenkungsplan in der Projektsitzung «Projektteam Bauherr» zur Gesamtbewertung der Kosten, Termine und zum Arbeitsstand. Die Fachteamsitzung TKQ (Termine Kosten Qualität) findet auf der Stufe Bauherr und Planungsteam statt. Der Q-Lenkungsplan wird an den PA versendet. Ebenso werden die Informationen aus dem Q-Lenkungsplan in einer kurzen Management Information im monatlichen PSR an den PA gespiegelt.

Beurteilung

Die Projektleiter halten sich an die Vorgaben der Prozessanweisung ar Immo über Risikomanagement. Risiken, wie der Terminverzug durch die Schäden werden transparent und zeitnah an die definierten Stellen gemäss Projektorganisation kommuniziert. Der Qualitäts-Lenkungsplan ist nachvollziehbar und wird regelmässig fortgeschrieben sowie an die vorgeschriebenen Stellen versandt.

3.5 Die Qualitätssicherung wesentlicher Anforderungen ist über alle Projektphasen hinweg zu stärken

Im Rahmen einer Qualitätssicherung wurden die unterschiedlichen Projektphasen bei «FUNDAMENT» und «CAMPUS» über interne Peer Reviews sichergestellt. Die EFK hat dieses anhand eines Fallbeispiels für die Nutzeranforderungen geprüft. Prüfungen durch Prüfingenieure gab es bisher nicht. Diese sind in den Prozessen der armasuisse oder der SIA nicht explizit vorgesehen. Aus den Qualitätsmanagement Dokumenten «FUNDAMENT» und «CAMPUS» ist nicht ersichtlich, wie die Qualitätssicherung für wesentliche Bestandteile des Pflichtenheftes wie z. B. TIER-Level[9], Lüftungsanforderungen, Schutz vor elektromagnetischen Impulsen (EMP) erfolgt. Bei «FUNDAMENT» kann zum Zeitpunkt der Übergabe des Bauprojekts keine

[9] Zur Klassifizierung von Rechenzentren wurde die TIER-Topologie Ende der 1990er Jahre vom Uptime Institut mit Sitz in den USA, weltweit als Standard eingeführt. Jedes «TIER» (Stufe) steht für einen bestimmten Rang, den das jeweilige Rechenzentrum bzw. dessen Subsysteme erfüllt. Die TIER-Topologie sieht insgesamt vier Stufen (TIER I bis TIER IV) vor, wobei TIER I die am wenigsten zuverlässige Umgebung ist und TIER IV als «hochverfügbar» eingestuft wird.

Evidenz vorgelegt werden, dass das nach Pflichtenheft geforderte TIER-Level erreicht wurde. Nach der Vorprojektphase wurde eine externe Überprüfung gemäss Anforderungen des Uptime Institutes über den Planungsstand zur Erreichung des geforderten TIER-Level erstellt. Diese besagt, dass für die Verbrennungsluft und Abgase der geforderte TIER-Level nicht erreicht wurde. Mit einer redundanten Luftfassung konnte der geforderte TIER-Level für die Verbrennungsluft erreicht werden. Die Abgasführung wurde mit baulichen Massnahmen maximal verbessert. Technisch wurde die geforderte Verfügbarkeit mit den Integralen Tests nachgewiesen und dokumentiert. Eine Dokumentation über organisatorische Massnahmen oder bauliche Anpassungen, um das geforderten TIER-Level zu erreichen, liegt in Form der Protokolle der integralen Tests vor. Nach Pflichtenheft wird bei «KASTRO II» auch eine hohe Verfügbarkeit gefordert. Da das Projekt sich in der Vorprojektphase befindet, liegt noch keine diesbezügliche Beurteilung vor.

Positiv wird gesehen, dass das Projekt «KASTRO II» bauherrenseitig Prüfingenieure verpflichtet hat, um einzelne Teile des Vorprojektes zu prüfen. Ein Prüfplan über den Einsatz von Prüfingenieuren über die gesamte Projektlaufzeit, gekoppelt an Meilensteine und wesentliche Bauteile oder Risiken, besteht seitens Bauherrn oder Generalplaner zum Prüfzeitpunkt noch nicht.

Beurteilung

Die Projektleiter halten sich an die Vorgaben der Prozessanweisung ar Immo über RM und TQM. Die Risiken sind nachvollziehbar im Q-Lenkungsplan in der Risikomatrix dargestellt. Für Projekte dieser Komplexität besteht noch Potential, um das Risiko- und Qualitätsmanagement zu optimieren. Im Q-Lenkungsplan sollten die Prozessdarstellung der Qualitätssicherungsschritte für Planung und Ausführung wesentlicher RZ-Anforderungen erfasst werden. Hier ist gemeint, dass besonders risikoreiche Bestandteile eines RZ wie z. B. eine Bodenplatte durch Prüfingenieure in den Schritten Planung, Ausschreibung und Ausführung qualitätsgesichert werden. Dies wurde mit dem Projektleiter und dem Generalplaner von «KASTRO II» besprochen. Es wurden Möglichkeiten diskutiert, wesentliche Risiken der Anforderungen in die Risikomatrix aufzunehmen und die Qualitätssicherung durch Prüfingenieure zukünftig beim Generalplaner oder Bauherren anzusiedeln.

Den Abweichungen im Bereich des geforderten TIER-Level im RZ «FUNDAMENT» wurde mit verschiedenen mitigierenden Massnahmen bzw. einer Notfallplanung soweit möglich entgegengewirkt. In den umfangreichen Abnahmetests wurde die erreichbare Verfügbarkeit akzeptiert. Da keine erneute unabhängige Beurteilung der Verfügbarkeitklasse vorgenommen wurde, liegt der EFK kein Nachweis für die Erfüllung sämtlicher Kriterien vor.

Empfehlung 1 (Priorität 1)

Die EFK empfiehlt der armasuisse, besonders risikoreiche oder betriebsrelevante Bestandteile des Projekts «KASTRO II» zu definieren und die geforderte Qualität in den Planungs-, Ausschreibungs- und Ausführungsphasen durch externe Prüfingenieure sichern zu lassen.

Die Empfehlung ist akzeptiert.

Stellungnahme armasuisse

Die Empfehlung der EFK wird durch die armasuisse akzeptiert.

Die bei den Immobilienvorhaben FUNDAMENT und CAMPUS gemachten Erfahrungen zeigten verschiedene, betriebsrelevante und auch risikobehaftete Teile auf. Diese Erfahrungen fliessen mittels eines strukturierten Verbesserungsprozess direkt ins Projekt KASTRO II ein. Die so

identifizierten Bestandteile und Planungen werden bereits aktuell laufend durch externe Stellen überprüft. Diese Überprüfungen werden auch mit dem Fortschreiten des Projektes in der Phase «Bauprojekt» sowie «Realisierung» weitergeführt.

Empfehlung 2 (Priorität 1)

Die EFK empfiehlt der armasuisse, eine Qualitätssicherung der TIER-Level Anforderung bei «KASTRO II» über alle Projektphasen nachvollziehbar und dokumentiert zu führen.

Die Empfehlung ist akzeptiert.

Stellungnahme armasuisse

Die Empfehlung der EFK wird durch die armasuisse akzeptiert.

Die Anforderungen an die Verfügbarkeit werden seit den ersten Planungstätigkeiten verifiziert und deren Erfüllungsgrad dokumentiert. Allfällige Verletzungen der Verfügbarkeitsanforderungen wie sie in den TIER-Leveln gefordert sind werden zeitnah bereinigt und in der Realisierungsphase umgesetzt.

4 Sicherheit und Betrieb der RZ «CAMPUS» und «FUNDAMENT»

4.1 Die Umsetzung der Sicherheitsanforderungen der Domotik weist noch Verbesserungspotential auf

Für beide Anlagen liegen die genehmigten Sicherheitsdokumente vor. Das Betriebshandbuch Domotik-Services gilt für beide Rechenzentren. Im Handbuch wird die Verfügbarkeit mittels fünf Verfügbarkeitsklassen definiert. Im Anschluss werden die IKT-Services RZ mit der geforderten Verfügbarkeit gelistet. Die EFK stellt hier eine Abweichung zwischen den Schutzbedarfsanalysen und dem Betriebshandbuch fest. Die Schutzbedarfsanalyse «FUNDAMENT» forderte eine Ausfalldauer von maximal acht Stunden und eine Servicezeit von 24/7. Für das RZ «CAMPUS» wird dieselbe Ausfalldauer jedoch eine Servicezeit von 11/5 erwartet. Die IKT-Services RZ sind jedoch gemäss Betriebshandbuch für eine Verfügbarkeit «Best Effort» ausgerichtet, dies entspricht der tiefsten Serviceklasse. In dieser Serviceklasse sind die Werte «Anzahl Ausfälle pro Messperiode», «Max. Serviceausfallzeit in Std. pro Ausfall» und «Reaktionszeiten» nicht definiert.

Für die beiden Rechenzentren wurden unterschiedliche Informationssicherheits- und Datenschutz-Konzepte (ISDS) erstellt. Beide ISDS-Konzepte wurden vom stellvertretenden Informatiksicherheitsbeauftragten (ISBO), dem Geschäftsprozessverantwortlichen und dem Auftraggeber unter Vorbehalt genehmigt. Der Vorbehalt lautet «Das ISDS Konzept wird unter der Bedingung freigegeben, dass die festgestellten Risiken durch Mitigation in einen tragbaren Bereich gebracht werden.»

Zum Prüfzeitpunkt werden die Empfehlungen zur Risikominderung noch umgesetzt. Die Umsetzung der 2-Faktor-Authentifizierung stellt sich dabei als grösste Herausforderung dar. Für die Administration der Domotik wird, entgegen den Anforderungen aus dem IKT-Grundschutz in der Bundesverwaltung, noch keine 2-Faktor-Authentifizierung eingesetzt. Die entsprechende Implementierung ist gemäss Projekt «RZ VBS/Bund 2020» noch in Umsetzung. Die korrekte Umsetzung der Massnahmen zur Risikominderung wird jeweils durch die FUB geprüft. Zu diesen Prüfungen werden entsprechende Protokolle erstellt. Die Risiken werden nach der Umsetzung der Massnahmen nochmals neu bewertet und im ISDS-Konzept dokumentiert. Die ISDS-Konzepte sollen bis Mitte November 2021 aktualisiert und neu genehmigt werden. Die Pendenzen aus den ISDS-Konzepten werden geführt und überwacht, jedoch sind bei den definierten Massnahmen keine verbindlichen Termine festgesetzt. Die Auflistung enthält auch eine Risikobehandlungsliste, welche alle Risiken der beiden Rechenzentren im Bereich Domotik aufzeigen. Nach Projektabschluss werden die Risiken den Fachbereichen der FUB und dem Chief Information Security Officer (CISO) FUB übergeben. Die Restrisiken sollen dann durch den CISO der Geschäftsleitung FUB zur Behandlung vorgelegt werden.

Im Juni 2020 führte die FUB ein DOMOTIK Security Assessment durch. Daraus resultierten zwölf Befunde, davon wurden sieben als «high» und einer als «moderate» eingestuft. Der CISO führt einen Statusbericht über die als «high» und «moderate» eingestuften Ergebnisse. Von den acht gelisteten Befunden sind zum Prüfzeitpunkt sechs erledigt. Die zwei noch offenen Massnahmen sollen per Ende 2022 respektive Ende 2023 erledigt werden. Eine Nachprüfung der bereits erledigten Massnahmen ist auf Ende Juni 2022 terminiert.

Beurteilung

Die Genehmigung der Schutzbedarfsanalyse erfolgte im Projektverlauf spät, insbesondere, weil die Anforderungen an Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit das Design der IKT-Sicherheitsarchitektur und die resultierenden Kosten massgeblich beeinflussen kann. Die festgestellte Differenz bezüglich Anforderungen und Umsetzung der Verfügbarkeit bei den IT-Services RZ ist überraschend. Dies ist ein Anzeichen, dass die Umsetzung der Sicherheitsanforderungen nicht durchgängig geprüft und dokumentiert wurden.

Eine nachweisbare zeitliche Planung, bis wann die Pendenzen aus den ISDS-Konzepten abgeschlossen sind liegt nicht vor. Die Begründung, dass Abhängigkeiten von externen Dienstleistern die Planung erschweren, ist nur bedingt nachvollziehbar. Ein externer Dienstleister kann zur Einhaltung von Terminen vertraglich verpflichtet werden. Es ist begrüssenswert, die Pendenzen zugleich mit der Überarbeitung der ISDS-Konzepte per Mitte November abzuschliessen.

Die FUB-Penetration Tests im Bereich Domotik sind positiv zu werten. Die Führung der Status erfolgt durch den CISO in einfacher und pragmatischer Form. Allerdings sollten die relativ langen Fristen von teilweise mehr als zwei Jahren bis zur Behebung von als «high» eingestuften Befunden verringert werden.

Empfehlung 3 (Priorität 1)

Die EFK empfiehlt der FUB, die Umsetzung der Pendenzen aus den ISDS-Konzepten zu terminieren und konsequent zu überwachen. Mit Abschluss der ISDS-Konzepte sind die noch offenen Pendenzen und Restrisiken ins RM zu überführen.

Die Empfehlung ist akzeptiert.

Stellungnahme FUB

Die Empfehlung der EFK wird durch die FUB akzeptiert.

Die Mitigation von Risiken und das Abarbeiten der dazu definierten Massnahmen wird laufend durchgeführt. Die Verbesserung der Termintreue und die konsequente Überwachung liegt auch im Fokus der FUB. Die bei Projektabschluss noch offenen Risiken werden ins ISMS der FUB übernommen. Sämtliche Risiken werden regelmässig überprüft und allfällige weitere Massnahmen definiert, terminiert und umgesetzt.

Empfehlung 4 (Priorität 1)

Die EFK empfiehlt der Gruppe Verteidigung, die Umsetzung und somit die Erfüllung der in der Schutzbedarfsanalyse gestellten Anforderungen hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit im Bereich Domotik zu validieren.

Die Empfehlung ist akzeptiert.

Stellungnahme Gruppe Verteidigung

Die Gruppe V akzeptiert die Empfehlung der EFK.

Die bei der Domotik gestellten Anforderungen an die Sicherheit werden geprüft und wo keine Ausnahmebewilligung vorliegt umgesetzt und die Umsetzung überprüft. Bei allfällig bestehenden Restrisiken wird vorgegangen wie in der Stellungnahme zur Empfehlung 3 beschrieben wurde.

4.2 Eine Test- und Integrationsumgebung für die Domotik fehlt

Im Betriebshandbuch Domotik-Services wird der Prozess Release Management für Domotik Systeme ausführlich beschrieben. Darin enthalten ist auch eine Sicherheitsprüfung jeglicher Software durch das Security Operation Center (SOC) der FUB. In einem weiteren Schritt wird die Installation auf der Integrationsumgebung beschrieben. Eine solche Umgebung ist für die Domotik-Plattform jedoch nicht vorhanden. Neue Software Versionen werden direkt auf der Produktionsumgebung eingespielt. Das Risiko ist dem PA bekannt und wurde anlässlich einer Projektausschusssitzung im Frühjahr 2020 protokollarisch erfasst. Das Risiko ist neben dem PA-Protokoll auch in den ISDS-Pendenzen aufgeführt. Als Grund für das Fehlen einer Integrationsplattform werden mangelnde finanzielle Mittel sowie fehlende Personalressourcen und der fehlende Auftrag ausgewiesen. Es ist vorgesehen mit dem Projekt «Domotik auf dem Führungsnetz für einsatzrelevante Standorte» eine Test- und Integrationsplattform für die Domotik zu realisieren. Dabei handelt es sich um ein Projekt aus dem Portfolio des Kdo Cy. Aufgrund der Priorisierung der Finanzmittel verzögert sich die Realisierung jedoch noch um mehrere Jahre.

Beurteilung

Die Domotik bildet einen grundlegenden Bestandteil für den sicheren Betrieb eines RZ. Software und auch Hardware direkt in die Produktionsumgebung des RZ-Verbundes einzuspielen, ohne vorher die Wechselwirkungen und das Zusammenspiel der einzelnen Soft- und Hardwareteile zu testen, ist riskant und sollte vermieden werden.

Empfehlung 5 (Priorität 1)

Die EFK empfiehlt der Gruppe Verteidigung, den Aufbau einer Integrations- oder Testumgebung für die Domotik zu prüfen und deren Realisierung zu priorisieren.

Die Empfehlung ist akzeptiert.

Stellungnahme Gruppe Verteidigung

Die Gruppe V ist mit der Empfehlung der EFK einverstanden.

Der Aufbau einer Test- und Integrationsumgebung für die Domotik Anwendungen und auch für die Domotik-Plattform ist auch aus Sicht der Gruppe V dringend nötig. Aufgrund der angespannten Ressourcensituation konnte diese Test- und Integrationsumgebung leider nicht mit den ersten beiden RZ aufgebaut werden.

Im Rahmen des bereits gestarteten Projekts DAFES (Domotik auf Führungsnetz und einsatzrelevanten Standorten) sollen die Domotik Infrastrukturen noch weiter vereinheitlicht werden und eine dazu gehörende Test- und Integrationsumgebung aufgebaut werden. Das Ziel der Gruppe V ist es, auch im Bereich Domotik eine hohe Standardisierung und Automatisierung zu erreichen. Dazu ist eine Test- und Integrationsumgebung zwingend nötig.

4.3 Die Architektur entspricht bewährten Standards

Die Architektur wurde basierend auf einem Gesamtkonzept Domotik für «CAMPUS» und «FUNDAMENT» konzipiert. Weiter besteht eine darauf basierende Lösungsarchitektur Netz-Infrastruktur Domotik. In den Dokumenten zur Systemarchitektur werden die unterschiedlichen verwendeten Zonen gemäss den Vorgaben des Bundes zur Netzwerksicherheit und die Anbindung der Domotik und des Campus-Local Area Network (Campus-LAN) an das

Fhr Netz CH beschrieben. Endbenutzer Systeme, die Automationsebene, die Domotik-Services und die IKT-Management-Services sowie die Administratoren Systeme werden in getrennten Zonen mit eigenen Vorgaben gruppiert.

Campus ist nicht gleich «CAMPUS»

Die Bezeichnung «CAMPUS» in Grossschrift bezeichnet den Namen des RZ in Frauenfeld. Hingegen bedeutet derselbe Begriff in Kleinschrift in der Netzwerkterminologie eine gängige Bezeichnung für eine Form von lokalen Netzwerken.

Ein Campus-LAN oder Campusnetz ist ein lokales Netz (LAN) oder eine Reihe miteinander verbundener LANs, die einem Unternehmen, einer Behörde, einer Universität oder einer ähnlichen Organisation dienen. In diesem Zusammenhang umfasst ein typischer Campus eine Reihe von Gebäuden in unmittelbarer Nähe. Die Endbenutzer in einem Campus-Netz können (im geografischen Sinne) weiter verstreut sein als in einem einzelnen LAN, aber sie sind in der Regel nicht so weit verstreut wie in einem Weitverkehrsnetz (WAN). Im vorliegenden Fall handelt es sich um lokale Netzwerke, welche auf einem abgesteckten militärischen Gelände wie z. B. einem RZ oder einem Flugplatz betrieben werden.

Das Zonenkonzept der Domotik sieht unterschiedliche Zonen vor. In der Managementzone befinden sich die IKT-Managementsysteme zur Überwachung der Domotik-Anwendungen und der Endbenutzerinfrastruktur. Der Zugang auf die Managementzone erfolgt über eine dedizierte Endbenutzerinfrastruktur in Bern. Der Zugriff zur Nutzung der Domomtiksysteme erfolgt standortgebunden ab Sicherheitsleitzentrale, geschützter Aussenstelle und dem geschützten Büro der Logistikbasis der Armee (LBA).

Die Domotik-Plattformen an den Standorten «FUNDAMENT» und «CAMPUS» werden über das Fhr Netz CH erschlossen, welches als reines Transportnetz verwendet wird. Die Verbindung zwischen den Rechenzentren im RZ-Verbund (Landesknoten) und weiteren Rechenzentren der FUB erfolgt über dedizierte VPN. Innerhalb des RZ existieren verschiedene LANs und Schutzzonen. Die Kommunikation zwischen externen Systemen und den IKT-Systemen der Domotik ist in der Systemarchitektur und in der Lösungsarchitektur vereinfacht dokumentiert.

Das Campus-LAN im RZ «CAMPUS» ist seitens FUB Betrieb abgenommen worden. Jedoch sind in den Abnahmeprotokollen nach wie vor pendente Mängel ausgewiesen. Die Mängel werden in einer Liste geführt, laufend behoben und anschliessend in der Liste aktualisiert. Im RZ «FUNDAMENT» ist seitens FUB Betrieb noch nichts abgenommen worden.

Wie auch bei den Domotik-Services (Kapitel 4.1) festgestellt wurde, existiert auch beim Service «RZ-Verbindung» eine Differenz zu den Anforderungen aus der Schutzbedarfsanalyse. In diesem Fall betrifft es die Servicezeit.

Der Zugriff auf die RZ-Infrastruktur erfolgt zurzeit über den «Netzperimeter Verteidigung» (NPV), es besteht noch kein lokaler Perimeter innerhalb der RZ. Dieser soll im Rahmen des Projekts Fhr Netz CH und dem Aufbau der neuen Digitalisierungsplattform realisiert werden. Für den lokalen Betrieb des RZ ist jedoch dieser Netzübergang nicht relevant.

Die betrieblichen Aspekte sind in drei Betriebshandbüchern niedergeschrieben. Die beiden Betriebshandbücher «RZ-FUNDAMENT» und «RZ-CAMPUS» sind freigegeben, während das Betriebshandbuch «Domotik-Services» noch nicht freigegeben ist. Im Bereich Domotik wurde erst die Feld- und Automationsebene dem Betrieb übergeben. Die Domotik IKT (Leit-ebene) Plattform ist aufgrund von Ressourcenproblemen noch nicht an den Betrieb übergeben worden. Dies ist per Ende 2021 geplant.

Beurteilung

Die gewählte Architektur für die internen Netze und die Verbindung der beiden Rechenzentren «FUNDAMENT» und «CAMPUS», sowie die RZ-Anbindung entsprechen einem bewährten Standard.

Das Netzwerk der Domotik ist gemäss den Vorgaben in Zonen unterteilt und die Inter-Kommunikation zwischen externen Systemen und den IKT-Systemen der Domotik ist dokumentiert. Die Freigabe der Systemarchitektur Domotik «FUNDAMENT» erfolgte im November 2018 und jene der Systemarchitektur Domotik «CAMPUS» im Mai 2019. Die fehlenden Definitionen oder Verweise auf später zu treffende Entscheide und die nicht in einer Version 1.0 vorliegende Lösungsarchitektur lassen den Schluss zu, dass die Systemarchitektur und Lösungsarchitektur nicht laufend, respektive konsequent nachgeführt wird.

Die Abnahme der Netzwerkanbindung in den RZ wird protokolliert. In den Protokollen sind die noch zu behebenden Mängel aufgeführt. Die Mängel werden laufend behoben und der Status nachgeführt. Zum Prüfzeitpunkt wird dies noch nicht einheitlich durchgeführt.

Das RZ «FUNDAMENT» ist dem Betrieb übergeben, jedoch sind die Verbindungen über das Fhr Netz CH zum RZ «CAMPUS», zur Domotik und zum CAMPUS-LAN noch nicht abgenommen. Bei einer Betriebsübergabe des RZ sind auch die Systeme abzunehmen, die unmittelbar für den Betrieb benötigt werden. Dazu gehört sicher auch die netzwerktechnische Anbindung die für den Betrieb der Domotik notwendig ist.

Die Architekturdokumente und Betriebshandbücher sind ausreichend und der Situation angepasst. Es gilt im zukünftigen Betrieb sicherzustellen, dass diese bei Veränderungen im Rahmen des Change-Managements nachgeführt werden.

Durch den noch nicht realisierten lokalen NPV im RZ «FUNDAMENT» besteht die Abhängigkeit zum heute vorhandenen Netzwerkperimeter V. Erst wenn lokale NPVs in den vollgeschützten RZ implementiert sind, besteht eine durchgängige hohe Sicherheit. Die Realisierung sollte zeitlich mit dem Aufbau der Digitalisierungsplattform abgestimmt werden.

Bevor IKT-Systeme in ein RZ installiert werden, muss das RZ betriebsbereit sein. Dies bedeutet, dass eine ordentliche Betriebsübergabe stattgefunden hat und somit keine Abhängigkeiten zu Projekten mehr besteht. Noch nicht an den Betrieb übergebene Teile der Infrastruktur, die noch vom Projektteam betrieben werden, erschweren den Betrieb und erhöhen das Risiko für Fehler.

Empfehlung 6 (Priorität 2)

Die EFK empfiehlt der Gruppe Verteidigung, die Dokumentation bestehend aus Systemarchitektur und Betriebshandbüchern im Rahmen der Betriebsübergabe der Domotik IKT-Plattform zu aktualisieren und erneut freizugeben. Zugleich soll das Netzwerk des Rechenzentrums «FUNDAMENT» durch die Betriebsorganisation der FUB abgenommen werden.

Die Empfehlung ist akzeptiert.

Stellungnahme Gruppe Verteidigung

Die Gruppe V ist mit der Empfehlung der EFK einverstanden.

Die Abnahme eines Werkes oder Systems durch die Betriebsorganisation der FUB ist der normale Ablauf der am Ende eines Projekts durchgeführt wird. Um eine Abnahme bzw. Betriebsübernahme machen zu können, ist es nötig, dass sowohl die Services betriebsbereit als auch

die Dokumentation nachgeführt ist. Leider konnte in der Vergangenheit aus Ressourcengründen nicht alle Dokumentation mit der geforderten Qualität erstellt werden. Der nun vorliegende Nachdokumentationsaufwand ist erkannt und wurde in Angriff genommen.

4.4 Im bewaffneten Konflikt ist die Geo-Redundanz nicht mehr gewährleistet

Im veröffentlichten Projektbericht VBS wird der Bau von drei geografisch getrennten und redundant betriebenen Rechenzentren als ein Teilprojekt von FITANIA genannt. Die Georedundanz soll auch in den drei definierten Lagen (normale, besondere und ausserordentliche Lage) bestehen. Im Nutzer-, Sicherheits- und Betriebskonzept «CAMPUS» wird als Ziel des VBS, welches mit RZ VBS/Bund 2020 erreicht werden soll, die Sicherstellung des Betriebs über alle Lagen, genannt. Das RZ «FUNDAMENT» mit Vollschutz wird in allen Lagen genutzt, während das RZ «CAMPUS» in der normalen, besonderen und ausserordentlichen Lage ohne bewaffneten Konflikt genutzt wird. In einer ausserordentlichen Lage mit bewaffnetem Konflikt wird der militärische Betrieb des zivilen RZ «CAMPUS» aus Sicherheitsgründen und in Einklang mit den Genfer Konventionen (siehe auch Kapitel 3.2) ausgesetzt. Damit soll vermieden werden, dass das RZ zu einem militärischen Ziel wird. Durch die Verzögerung beim Bau von «KASTRO II» besteht für die neue Digitalisierungsplattform in einer ausserordentlichen Lage mit bewaffnetem Konflikt bis zur geplanten Inbetriebnahme keine geschützte Georedundanz. Es wird in dieser Lage nur das RZ «FUNDAMENT» und die bis dahin noch bestehenden alten RZ betrieben.

Beurteilung

Durch die Georedundanz kann die Verfügbarkeit von IKT-Systemen bei einem Ausfall eines RZ aufrechterhalten werden. Werden die IKT-Systeme auch innerhalb des RZ «FUNDAMENT» redundant in unterschiedlichen Systemräumen betrieben, bleibt bei einem Ausfall von «CAMPUS» eine Redundanz innerhalb von «FUNDAMENT» bestehen. Nach Inbetriebnahme von «KASTRO II» soll die Georedundanz zwischen «FUNDAMENT» und «KASTRO II» implementiert werden.

5 Die Digitalisierungsplattform der Armee

«IKT A&I» ist ein Teilprojekt des Projekts «RZ VBS/Bund 2020». Im Projekt wird die IKT-Architektur für den Rechenzentren-Verbund und den automatisierten Betrieb der IKT auf der Basis virtualisierter Systeme entwickelt. Damit soll eine hohe Skalierbarkeit der Ressourcen sichergestellt werden. Die IKT-Architektur legt den Grundstein für eine Zusammenführung der heutigen dezentralen Systeme und RZ-Infrastrukturen. Die Strukturbereinigung erlaubt in Zukunft einen effizienten Betrieb und soll die komplette Funktionalität der IKT über alle Lagen gewährleisten.

5.1 Die Architektur entspricht etablierten Standards

Zum Zeitpunkt der Prüfung sind hauptsächlich Dokumentationen und Interviews die Quellen zur Überprüfung der Sachlage. Die zum Prüfzeitpunkt vorliegenden Dokumentationen sind auf einer Flughöhe, welche hauptsächlich die zu realisierende Architektur und die zu verwendenden technologischen Konzepte und Technologien aufführen, beschreiben und in Zusammenhang setzen. Die in den Dokumentationen aufgeführten Technologien und Konzepte entstammen grösstenteils aus der agilen Softwareentwicklung sowie den Konzepten von Infrastructure-as-Code (IaC)[10]. Die zu verwendenden Elemente sind herstellerspezifische «off the shelf»-Produkte oder stammen aus frei verfügbaren Open-Source-Projekten. Diese entsprechen dem aktuellen und etablierten Stand der Technik. Der Verbund der Elemente «Landes-, Regional- und Lokalknoten» baut zum jetzigen Stand des Projektes auf bereits vorhandenen, statischen Legacy-Systemen und -Technologien des Fhr Netz CH als Carrier auf. Das vorhandene Fhr Netz CH wird als reiner Carrier verstanden, wobei die FUB oder gegebenenfalls zukünftig das Kdo Cy entsprechende IKT-Service Leistungen zu erbringen hat. Die Recheneinheiten sollen als georedundante Verbunde betrieben werden können. Anhand der Selbstdeklarationen der Lieferanten können alle technischen Anforderungen aus dem Projektauftrag erfüllt werden. Offen steht dabei, ob die als «erfüllt» selbstdeklarierten Anforderungen im Sinne der Ausschreibung, und in Übereinkunft aller Stellen, zukünftig effektiv umgesetzt werden respektive umgesetzt werden können.

Für die Entwicklungs-, Test- und Integrationsumgebung liegen der EFK Schutzbedarfsanalyse, ISDS-Konzept und Umsetzung IKT-Grundschutz als Entwurf vor. Im ISDS-Konzept ist ein Risiko als hoch und fünf weitere Risiken als mittel ausgewiesen. In der Analyse der Umsetzung des IKT-Grundschutzes ist ersichtlich, dass aktuell neun IKT-Grundschutzmassnahmen noch nicht oder erst teilweise umgesetzt werden können.

Beurteilung

Die zur Beurteilung der Architektur zur Verfügung gestellten Dokumentationen sind vom November/Dezember 2020. Aus hoher Flughöhe sind in der Architekturdokumentation die Philosophie der Bereitstellung von IaC sowie auch die eingesetzten Technologien, Funktionen und Zusammenhänge klar erkennbar und entsprechen dem heutigen Stand der Technik. Im weiteren Projektverlauf sind insbesondere die Herausforderungen in der zukünftigen Anbindung des RZ-LAN an das Fhr Netz im Auge zu behalten, da Neues (aus dem Projekt

[10] Prozess zur Verwaltung und Bereitstellung von Computer-Rechenzentren über maschinenlesbare Definitionsdateien anstelle der physischen Hardwarekonfiguration oder interaktiver Konfigurationstools.

IKT A&I) mit dem Bestehenden (heutiges Fhr Netz) koexistieren muss. Die Teil-Projekte befinden sich zum Zeitpunkt der Prüfung noch in der Konzeptionsphase und können noch nicht abschliessend bewertet werden.

Der IKT-Grundschutz legt die minimalen organisatorischen, personellen und technischen Sicherheitsvorgaben im Bereich Informationssicherheit verbindlich fest. Die Einhaltung des IKT-Grundschutzes ist auch bei der Entwicklungs-, Test- und Integrationsumgebung sicherzustellen, insbesondere deshalb, weil die Integrationsumgebung gleich aufgebaut ist wie die Produktivumgebung, welche dann in den vollgeschützten Rechenzentren «FUNDAMENT» und «KASTRO II» zum Einsatz kommt und auf den einsatzrelevanten Systemen des VBS betrieben wird. Das Projekt hat die Wichtigkeit der Grundschutzmassnahmen erkannt und setzt die offenen Punkte laufend um. Es ist geplant, den Grundschutz vor Inbetriebnahme umzusetzen. Aus diesem Grund verzichtet die EFK hier auf eine Empfehlung.

5.2 Standardisierte Steuerung und Kontrolle der Datenflüsse

Zum Zeitpunkt der Prüfung wird das Fhr Netz CH durch die FUB als Standarddienstleistung aus dem IKT-Service-Katalog bereitgestellt, betrieben und gewartet. Die Anforderungen an physische Netzwerke und Verbindungen, die Netzwerklogik und entsprechende Berechtigungen werden jeweils über den Auftraggeber initiiert und mittels Bestellungen und Definition des Service Levels aus dem IKT-Service-Katalog der FUB bezogen.

Das Teilprojekt «Secure Data Interchange» bietet Lösungsansätze, welche die automatisierte Bereitstellung von IKT-Services und Sicherheitskomponenten ermöglichen soll. Mit diesen sollen die Steuerung und Kontrolle von Datenflüssen im Verbund sowie zu externen Stellen ermöglicht werden. Diese Lösungsansätze sollen komplementär zu den Sicherheitsmechanismen der Plattform IKT 4.0 ab Juli 2025 bereitstehen. Zum Zeitpunkt der Prüfung sind alle Übergänge über den Netzwerkperimeter V (NPV) angeschlossen.

Beurteilung

Aus technischer Sicht, ist die konzeptionelle Kombination der Ansätze erfolgsversprechend. Sofern das Zusammenspiel der Automatisierungsvorgänge der entsprechenden Komponenten zuverlässig konfiguriert werden kann, können manuelle, durch Personal verursachte Fehlkonfigurationen tendenziell vermindert werden. Anhand der zum Zeitpunkt der Prüfung verfügbaren Grundlagen können nur bedingte Aussagen zur Zuverlässigkeit, Verfügbarkeit und Integrität des Netzwerkes gemacht werden.

Es ist damit zu rechnen, dass der geplante Ersatz des NPV entsprechende Herausforderungen mit sich bringen könnte. Die im Projekt geplante Referenzarchitektur des Netzwerkes kann eine Veränderung des heutigen Netzwerkperimeters V (NPV) nach sich ziehen. Dies würde bedeuten, dass tendenziell ein massiver Umbau von bestehenden Dienstleistungen aus dem Service-Katalog erforderlich sein wird, um die Verbindungen zwischen den RZ stabil und sicher zu ermöglichen.

5.3 Das Management erfolgt über separate Netze

Aus den Dokumentationen ist ersichtlich, dass dedizierte Management-Netzwerke vorhanden sind. Einerseits sind physisch getrennte Netzwerke zur Steuerung von OOB[11]-Netzwerken und -Komponenten vorhanden. Andererseits können logisch-getrennte virtuelle private Kommunikationsnetze (VPN)[12] nach Bedarf konfiguriert werden. Die Authentifizierung für Remote Access auf Management-Konsolen erfolgt auf Netzwerkebene wahlweise über zwei Authentifizierungsdienste. Mittels unterschiedlicher Protokolle können entsprechend verschlüsselte Verbindungen aufgebaut werden, um den Schutz von Transport- und Kontrolldaten zu gewährleisten. Des Weiteren ist es möglich, Managementschnittstellen mittels sicherer Protokolle anzusteuern. Damit können Funktionen wie Monitoring, Logging und Reporting wahrgenommen werden.

Anhand der Dokumentationen ist ersichtlich, dass auch Protokolle zur Verwendung kommen, welche ohne weiteren Sicherungsmassnahmen mitgelesen oder verändert werden können. Die Massnahmen werden in einem Härtungs-Konzept beschrieben, in welchem dann auch die zu verwendenden Protokolle definiert werden sollten.

Beurteilung

Aus technischer Sicht sind in den Dokumentationen die notwendigen Komponenten und Protokolle vorhanden, um die Administration und den Betrieb in dedizierten Netzwerken auch aus der Ferne (Remote-Access) zu betreiben. Die physische Trennung von OOB-Netzwerken von Produktivnetzen entsprechen den marktüblichen Best-Practices. Ebenfalls sind Techniken und Protokolle dokumentiert, welche es ermöglichen, weitere logisch getrennte Netzwerke im Produktivnetz zu erstellen und zu betreiben.

5.4 Der Betrieb der Digitalisierungsplattform über alle Lagen ist mit möglichen Einschränkungen sichergestellt

Der Aufbau und Betrieb der komplexen Infrastrukturen und Orchestrierungswerkzeuge zum Management der unterschiedlichen Services in der Cloud erfordert vertieftes Expertenwissen. Dies wird von den Mitarbeitenden des Kdo Cy laufend aufgebaut. Zum Prüfzeitpunkt kann die Projektorganisation Kdo Cy nicht ausschliessen, dass für den Betrieb der Digitalisierungsplattform oder spezielle Interaktionen künftig externe Ressourcen beansprucht werden müssen. Dies wäre in der ausserordentlichen Lage mit Waffeneinwirkung möglicherweise nicht sichergestellt.

Beurteilung

Der Aufbau des Know-how für den Betrieb der Digitalisierungsplattform ist ein zentraler Aspekt und hat im Projekt Kdo Cy eine hohe Aufmerksamkeit. Der Einsatz von externen Ressourcen ist zwar in den meisten Lagen sichergestellt, könnte jedoch im Falle eines bewaffneten Konflikts nicht mehr möglich sein. Bei fehlendem externem Expertenwissen könnte auf komplexe Interaktionen im Gesamtsystem verzichtet werden, ohne dabei den Betrieb zu gefährden. Das Kdo Cy muss den grundlegenden Betrieb jedoch autonom sicherstellen können.

[11] Out of Band, physikalisch getrennte Anbindung zur Steuerung von Netzwerkhardware
[12] Statische und Dynamische VPNs (FlexVPN)

6 Auslastung der Rechenzentren

Die Leistungserbringer (LE) der BV betreiben heute ihre RZ an zahlreichen Standorten in der Schweiz. Die Konzeption widerspiegelt die historische Entwicklung der aktuellen IKT-Landschaft. Gemäss IKT-Strategie des Bundes für die Jahre 2012 bis 2015 und Masterplan wurden die LE beauftragt, ein departementsübergreifendes Datacenter-Konzept zu erarbeiten, um eine Konsolidierung der vorhandenen RZ zu erreichen. Das Konzept Rechenzentren-Verbund entstand aus der strategischen Stossrichtung vier.

Betriebsmodell RZ-Verbund 2020

Mit der Verabschiedung des Konzepts für den RZ-Verbund hat der Bundesrat im Juli 2014 das EFD beauftragt, das Betriebsmodell für den gesamten RZ-Verbund zu erarbeiten. Der Bundesrat hat dieses «Betriebsmodell Rechenzentren-Verbund Zielbild 2020» im Jahr 2017 verabschiedet und die internen Leistungserbringer beauftragt, dieses bis 2020 umzusetzen. Es regelt, welche bundesinternen IKT-Leistungserbringer künftig welche IKT-Infrastrukturdienste wie Hardware, Betriebssysteme und Speicher im RZ-Verbund erbringen, so dass Synergien optimal genutzt werden. Das Betriebsmodell gibt zudem vor, dass nebst den vier RZ des Verbundes keine weiteren Rechenzentren mehr gebaut, erweitert oder modernisiert werden dürfen.

6.1 Der Bezug des RZ «Campus» schreitet voran, räumliche Reserven sind vorhanden

Das RZ «CAMPUS» ist seit Anfang 2021 im Betrieb. Bei allen vorgesehenen LE laufen Projekte für die schrittweise Bestückung der RZ-Flächen. Während die FUB dort die neue Digitalisierungsplattform entwickelt, ist das BIT bereits produktiv in der Anlage vertreten. Seit Januar 2021 betreibt das BIT erste Infrastruktur- und Basisdienste im neuen Rechenzentrum wie beispielsweise Zugangssysteme und erste Netzwerkkomponenten. Erste Infrastrukturen und Services aus dem Programm SUPERB (S4/Hana-Plattform), sowie die neuen Oracle- und Teradata-Plattformen und Unified Communication & Collaboration (UCC) werden ebenfalls bereits produktiv im neuen Rechenzentrum betrieben. Die Aufbauarbeiten im RZ-CAMPUS und RZ-PRIMUS schritten in den letzten Monaten nach Plan voran. Die flächenmässige Auslastung der zivilen Nutzer liegt aktuell bei 20 Prozent und für die Planungen der nächsten Jahre geht das BIT von einer Belegung von ca. 50 Prozent aus. Somit sind entsprechende Reserven für die Integration weiterer Systeme aus der Konsolidierung der dezentralen RZ vorhanden. Das Konzept des RZ beinhaltet einen modularen Ausbau. Sobald sich abzeichnet, dass der bestehende Bau nicht mehr ausreicht, können weitere Module angebaut werden.

Der Einbau der IKT-Systeme für die Digitalisierungsplattform der Armee im RZ «FUNDAMENT» soll ab 2023 erfolgen und 2024 in den Betrieb gehen. In diesem RZ ist die Hälfte der zur Verfügung stehende Fläche voll ausgebaut, die andere Hälfte ist als Reserve vorgesehen und kann während dem Betrieb des RZ ausgebaut werden.

Gemäss einer Umfrage des Bereichs DTI bei den Departementen, sind im zivilen Bereich der BV heute noch 25 RZ in Betrieb. Ein Ziel der Umfrage war die Klärung des Bedarfs für eine Integration in den RZ-Verbund. Die Ergebnisse zeigen einen klaren Bedarf an RZ-Fläche. Die erfassten RZ und Systemräume sind bis auf eine Ausnahme in Bundesbesitz und werden mehrheitlich durch die LE selbst betrieben. Militärische und klassifizierte RZ und Serverräume wurden in der Umfrage des Bereichs DTI nicht erfasst, da Informationen über Kapazitätsanforderungen klassifiziert sind.

Beurteilung

Um die kostspieligen Infrastrukturen auch sinnvoll nutzen zu können, ist es wichtig, die laufenden und geplanten Migrationsprojekte mit Hochdruck weiter zu verfolgen. Nur so können alte Systemräume und RZ zeitnah abgebaut werden und damit Betriebskosten gespart und eine bessere Qualität und Zukunftsfähigkeit der IKT-Leistungserbringung erreicht werden. Die Bestrebungen des Bereichs DTI zur Konsolidierung und Verschiebung der verschiedenen Systeme in die RZ des RZ-Verbundes ist zielführend. Nur durch ein konsequentes Festhalten an der Strategie können die Ziele und Vorteile des RZ-Verbundes auch erreicht bzw. genutzt werden.

Auf Basis der strategischen Initiative SI-4 «Hybrid Multi-Cloud» wurde durch eine externe Firma eine Studie zur künftigen Nutzung der RZ erarbeitet. Weiter wurden ein strategisches Portfolio zu Zielplattformen und Infrastrukturen sowie ein Entscheidungsmodell zur Beurteilung der Anwendungen und Zielarchitekturen erarbeitet. Die Ergebnisse sollen direkt in die überarbeitete RZ-Strategie einfliessen.

6.2 Ein neues RZ trotz RZ-Verbund Strategie?

Noch vor Inkrafttreten der IKT-Strategie des Bundes 2012 bis 2015 wurde in den Jahren 2008 bis 2016 der Systemraum im Campus G1 (Guisanplatz 1) von fedpol im Rahmen der Bau Projektierung mit dem Bundesamt für Bauten und Logistik (BBL) geplant und per 2018 fertiggestellt. Die Dimensionierung und Ausstattung wurde unter Berücksichtigung der besonderen Anforderungen (Schutzniveau und Verfügbarkeit) insbesondere auch im Kontext der Einsatz- und Alarmzentrale, der Anforderungen der Bundes Kriminalpolizei (BKP) und der Nationalen Alarmzentrale (NAZ) gewählt. Die Zusammenführung von mehreren Standorten des fedpol im G1 sowie die Bedürfnisse aller Arealnutzer, führten zur heutigen Infrastruktur im Systemraum G1.

Ein vom ISB (heute DTI) bewilligter Ausnahmeantrag (P035) legitimiert fedpol zum Betrieb des RZ inklusive den Fachanwendungen. Die Ausnahmen sind jedoch teilweise zeitlich limitiert. Aus diesem Grund hat das fedpol bereits Massnahmen zur Integration seiner Lösung mit dem ISC-EJPD eingeleitet. So können bis anhin selbst betriebene Fachanwendungen jeweils stückweise in den Betrieb zum ISC-EJPD überführt werden. In enger Zusammenarbeit mit dem ISC-EJPD wurde eine Lösung zur weiteren Synergienutzung innerhalb des EJPD erarbeitet: Das RZ G1 soll für fedpol künftig in der Verantwortung des ISC-EJPD betrieben und gemäss RZ-Strategie Bund eingebunden werden. Dadurch kann das RZ an der Güterstrasse aufgelöst werden, dessen Mietvertrag per Ende 2024 ausläuft. Dadurch entfallen diese Mietkosten ab 2025.

Um die Schengen-Anforderungen an die Höchstverfügbarkeit abdecken zu können, basiert die RZ-Strategie des EJPD auf einem Regionen-Konzept. Auf Grund der langen Latenzzeiten war das RZ «CAMPUS» als alleiniger Redundanzstandort keine Option. Deshalb werden an beiden Standorten die Anwendungen redundant aufgebaut, wodurch bei einem Ausfall des Standortes Bern, der Weiterbetrieb in Frauenfeld sichergestellt ist. Durch diese Architektur werden eine sehr hohe Verfügbarkeit und die Georedundanz sichergestellt. Mit den zwei RZ «PRIMUS» und G1 in der Region Bern, kann die Anforderung an die Höchstverfügbarkeit sichergestellt werden. Um die Georedundanz sicherzustellen, wird die Umgebung auch im «CAMPUS» Frauenfeld am selben Standort physisch redundant aufgebaut.

Im Jahr 2020 schätzte ein akkreditierter TIER-Designer die Verfügbarkeitsklasse des RZ G1 nach dem Standard des Uptime Institute ein. In seinem Bericht kam er zum Schluss, dass die

Gebäudetechnik die angestrebte Verfügbarkeitsklasse nach den Kriterien des Uptime Institute nicht vollständig erreicht. In Bezug auf die Verfügbarkeitsanforderungen, welche sich inhaltlich aus den Anforderungen seitens der Schengen Systeme ableiten lassen, sind zusätzlich zu den vollständig redundanten Leistungskomponenten, alle kritischen Komponenten über mehrere, voneinander unabhängigen Versorgungspfade zu erschliessen. Dies ist heute in den Bereichen der Kälte- und Energieversorgung jedoch nicht vollständig der Fall.

Beurteilung

Die Begründung für den Bau des RZ am Guisanplatz 1 kann nachvollzogen werden. Die künftigen Anforderungen an die hohe Verfügbarkeit konnte durch die geografische Trennung nicht vollumfänglich abgedeckt werden. Die heutige Konfiguration stellt auch den Betrieb bei einem Ausfall des Standortes Bern sicher.

Für den Betrieb der bisherigen Anwendungen war die maximale Verfügbarkeit der RZ-Infrastruktur ausreichend. Künftig mit der Übergabe des Betriebs an das ISC-EJPD, kann ein Ausfall der zentralen Versorgungselemente zu einem Ausfall der Systeme führen und sollte, soweit technisch möglich, verhindert werden. Inwiefern diese Anpassungen nach der Inbetriebnahme bzw. nach dem Abschluss des Bauprojektes noch nachgerüstet werden können, sollte durch das fedpol geklärt werden. Allenfalls besteht auch die Möglichkeit, im Rahmen der Erweiterungsbauten am G1 gewisse Nachrüstungen vorzunehmen. Hierfür könnte eine TIER-Gap-Analyse (TGA) Aufschluss geben.

Eine Ausnahmegenehmigung des Informatiksteuerungsorgans des Bundes (ISB) (heute DTI) liegt vor. Die Nutzung von Synergien mit anderen VE und die geplante Überführung des Betriebs in das ISC-EJPD ist zielführend. In der Anforderung «Anf2019-066» aus dem Jahr 2019 sah das damalige Informatiksteuerungsorgan des Bundes (ISB) vor, das RZ G1 in den «RZ-Verbund der zentralen Bundesverwaltung» als zusätzliches RZ einzubinden. Die überarbeitete Strategie sollte bis Ende Juni 2020 zum Beschluss vorgelegt werden.

Empfehlung 7 (Priorität 2)

Die EFK empfiehlt dem Bereich DTI der BK, die Überarbeitung der Strategie «RZ-Verbund der zentralen Bundesverwaltung» zu priorisieren und zeitnah zu verabschieden.

Die Empfehlung ist akzeptiert.

Stellungnahme Bereich DTI der Bundeskanzlei

Die Strategie «RZ-Verbund der zentralen Bundesverwaltung» ist in der Überarbeitung im Bereich DTI der BK. Das Dokument wird im Juni fertiggestellt und danach in den Gremien (FA, IBK, LT-DTI, GL BK, DRB, GSK) vorgestellt. BK Beschluss ist auf Ende 2022 geplant.

Empfehlung 8 (Priorität 1)

Die EFK empfiehlt dem fedpol, das RZ G1 einer TIER-Gap-Analyse zu unterziehen. Die Ergebnisse sollten als Grundlage für die Ausarbeitung einer Machbarkeitsstudie zur Erhöhung der Verfügbarkeit des Rechenzentrums G1 dienen. Dabei sollen unter Beachtung der Kosten und des Nutzens auch alternative Lösungen geprüft werden.

Die Empfehlung ist akzeptiert.

Stellungnahme fedpol

fedpol ist mit der Empfehlung einverstanden und wird in Zusammenarbeit mit dem ISC-EJPD eine entsprechende GAP-Analyse für das RZ-G1 vornehmen.

Anhang 1: Rechtsgrundlagen

Rechtstexte
Bundesgesetz über die Eidgenössische Finanzkontrolle (Finanzkontrollgesetz, FKG) vom 28. Juni 1967 (Stand am 1. Januar 2018), SR 614.0
Bundesgesetz über die Rüstungsunternehmen des Bundes (BGRB) vom 10. Oktober 1997 (Stand am 1. Januar 2012), SR 934.21
Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV), vom 27. Mai 2020 (Stand am 1. April 2021), SR 120.73
Verordnung über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV) vom 4. Juli 2007 (Stand am 1. Januar 2018), SR 510.411
Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992 (Stand am 1. Januar 2014) SR 235.1
Verordnung zum Bundesgesetz über den Datenschutz (VDSG) vom 14. Juni 1993 (Stand am 16. Oktober 2012) SR 235.11
Verordnung über das Geheimschutzverfahren bei Aufträgen mit militärisch klassifiziertem Inhalt (Geheimschutzverordnung) vom 29. August 1990 (Stand am 1. Januar 1991) SR 510.413
Botschaften
14.030 – Botschaft über die Beschaffung und die Ausserdienststellung von Rüstungsmaterial 2014 (Programm zur Beschaffung und Ausserdienststellung von Rüstungsmaterial 2014) vom 7. März 2014, BBI 2014 2745
16.026 – Botschaft über den Zahlungsrahmen der Armee 2017–2020, das Rüstungsprogramm 2016 und das Immobilienprogramm VBS 2016 (Armeebotschaft 2016) vom 24. Februar 2016, BBI 2016 1573
17.026 – Botschaft zum Bundesbeschluss über die Migration und den Umzug ins Rechenzentrum «CAMPUS» (Vorhaben RZMig2020) vom 22. Februar 2017, BBI 2017 2251
17.027 – Armeebotschaft 2017 vom 22. Februar 2017, BBI 2017 2761
21.023 – Armeebotschaft 2021 vom 17. Februar 2021, BBI 2021 372

Anhang 2: Abkürzungen

ar Immo	armasuisse Immobilien
armasuisse	Bundesamt für Rüstung
A Stab	Armeestab
BABS	Bundesamt für Bevölkerungsschutz
BBL	Bundesamt für Bauten und Logistik
BIT	Bundesamt für Informatik und Telekommunikation
BKP	Baukostenplan
BKP	Bundeskriminalpolizei
BR	Bundesrat
BV	Bundesverwaltung
CdA	Chef der Armee
CISO	Chief Information Security Officer
DC	Data-Center
DTI	Digitale Transformation und IKT-Lenkung
EFK	Eidgenössische Finanzkontrolle
EMP	Elektromagnetischer Impuls (electromagnetic pulse)
fedpol	Bundesamt für Polizei
Fhr Netz CH	Führungsnetz Schweiz (siehe Glossar)
FUB	Führungsunterstützungsbasis
G1	Guisanplatz 1
GP	Generalplaner
IaC	Infrastructure as Code (siehe Glossar)
IKT	Informatik- und Kommunikationstechnik
IKT A&I	(IKT) Architektur und Infrastruktur

ISB	Informatiksteuerungsorgan des Bundes (heute DTI)
ISBO	Informatiksicherheitsbeauftragte(r) einer Verwaltungseinheit
ISC-EJPD	Informatik Service Center des Eidgenössischen Justiz- und Polizeidepartements
ISDS	Informationssicherheits- und Datenschutz-Konzept
Kdo Cy	Kommando Cyber
LAN	Local Area Network (lokales oder örtliches Netzwerk)
LBA	Logistikbasis der Armee
LE	Leistungserbringer
NAZ	Nationale Alarmzentrale
NPV	Netzwerkperimeter Verteidigung
PA	Projektausschuss
PSP	Projektstrukturplan
PSR	Projektstatusreport
OBB	Out of Band (siehe Glossar)
RM	Risikomanagement
RZ	Rechenzentrum
SDI	Secure Data Interchange
SOC	Security Operation Center
TGA	TIER-Gap-Analyse
TQM	Total Quality Management
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
VE	Verwaltungseinheit(en)
VPN	Virtual Private Network

Anhang 3: Glossar

2-Faktor-Authentifizierung	Bezeichnet den Identitätsnachweis eines Nutzers mittels einer Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (wissen und haben).
Programm «Air2030»	Das Programm Air2030 besteht aus vier Projekten: *NKF*: Neues Kampfflugzeug *Bodluv*: Bodengestütztes Luftverteidigungssystem grösserer Reichweite *C2Air*: Erneuerung des Führungs- und Kommunikationssystems des Luftraumüberwachungs- und Einsatzleitsystems Florako (mit Armeebotschaft 2020 bewilligt) *Radar*: Erneuerung der Sensorsysteme des Luftraumüberwachungs- und Einsatzleitsystems Florako (Werterhalt Flores-Primärradare mit Armeebotschaft 2016 sowie mit Zusatzkredit in Armeebotschaft 2018 bewilligt, Werterhalt und Fähigkeitserweiterung Flores-Sekundärradare mit Armeebotschaft 2018 bewilligt)
Ausserordentliche Lage	Situation, in der in zahlreichen Bereichen und Sektoren normale Verwaltungsabläufe nicht genügen, um die Probleme und Herausforderungen zu bewältigen, die das ganze Land schwer in Mitleidenschaft ziehen, oder bei kriegerischen Ereignissen. (Definition Reglement 52.055 d)
Besondere Lage	Situation, in der gewisse Staatsaufgaben mit den normalen Verwaltungsabläufen nicht mehr bewältigt werden können. Die sektoriell betroffene Regierungstätigkeit verlangt in der Regel eine rasche Konzentration der Mittel und Straffung der Verfahren. (Definition Reglement 52.055 d)
Domotik	Bezeichnung der Einrichtungen, Software und Dienstleistungen für automatische Steuerung und Regelung, Überwachung und Optimierung von Gebäuden und technischen Steuerungen.
Führungsnetz Schweiz	Das Führungsnetz Schweiz ist ein standortgebundenes, fixes Transportnetz auf der Basis von Glasfaserkabeln und Richtfunk-Verbindungen. Basis für das Führungsnetz bildet ein bestehendes Kern-Netz, das bereits weite Teil der Schweiz erschliesst. Um die Verfügbarkeit hoch zu halten, werden verschiedene Verbindungen redundant aufgebaut. Im Endausbau wird das Netz eine Länge von knapp 3000 Kilometern und rund 300 Standorte umfassen. (Quelle www.vtg.admin.ch)

HERMES	eCH-0054: HERMES Projektmanagement-Methode HERMES ist die Projektmanagement-Methode für Informatik, Dienstleistung, Service und Geschäftsorganisationen und wurde von der schweizerischen Bundesverwaltung entwickelt. Die Methode steht als offener Standard vom Verein eCH allen zur Verfügung.
Hybrid Multi-Cloud (der Bundesverwaltung)	Der Begriff Multi-Cloud beschreibt die Verbindung mehrerer Cloud-Dienstleistungen verschiedener Private- und Public-Cloud-Anbieter zu einer oder mehreren gemeinsamen Clouds, um von den Vorteilen (z. B. Portabilität und Herstellerunabhängigkeit) mehrerer Cloud-Anbieter zu profitieren. Hybrid Multi-Cloud der Bundesverwaltung bezeichnet den Ansatz, die Cloud-Dienstleistungen der eigenen Leistungserbringer mit jenen mehrerer Public Cloud-Anbieter als abstrahierte IT-Infrastruktur- und Plattformdienste für die Schweizer Bundesverwaltung zur Verfügung zu stellen. (Definition: Cloud-Strategie der Bundesverwaltung, 2020)
Infrastructure as Code	Prozess der Verwaltung und Bereitstellung von Computer-Rechenzentren über maschinenlesbare Definitionsdateien anstelle der physischen Hardwarekonfiguration oder interaktiver Konfigurationstools.
Informationssicherheits- und Datenschutz Konzept	Das ISDS-Konzept bildet die Grundlage für die Festlegung der Massnahmen für die Informationssicherheit und den Datenschutz. Es zeigt die Restrisiken auf, die mit dem Betrieb des IT-Systems und der Organisation verbunden sind.
ISO/IEC 27001:2013	Die internationale Norm ISO/IEC 27001 definiert Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems (ISMS).
Legacy-System	Auch «Altsystem»: Bezeichnet in der Informatik eine etablierte, historisch gewachsene Anwendung oder System.
Normale Lage	Situation, in der ordentliche Verwaltungsabläufe zur Bewältigung der anstehenden Probleme und Herausforderungen ausreichen. (Definition Reglement 52.055 d)
«off the shelf»-Produkte	Seriengefertigte Produkte aus dem Elektronik- oder Softwaresektor, die in großer Stückzahl völlig gleichartig aufgebaut und verkauft werden.
Out of Band	Bezeichnet die Daten, welche ausserhalb der Hauptkommunikationsform übermittelt werden.

P035 – Prozess	Die IKT-Vorgabe regelt den Umgang mit Anforderungen und Vorgaben zur Bundesinformatik gemäss Ziffer 4 der Weisungen des EFD vom 19. Februar 2013 zur Umsetzung der Bundesinformatikverordnung (WUBinfV) sowie gemäss P000 – Informatikprozesse in der Bundesverwaltung.
Q-Lenkungsplan	Der Q-Lenkungsplan ist ein Teilprozess des Qualitätsmanagements (QM), der auf die Erfüllung von Qualitätsanforderungen ausgerichtet ist. QM ist der Hauptprozess, der auf die Abstimmung der Tätigkeiten zum Leiten und Lenken der Produkte/Systeme in der (Initialisierungsphase) Konzeptphase, Realisierungsphase, Einführungsphase, Nutzung und Ausserdienststellung bezüglich Qualität ausgerichtet ist. Zum QM gehören ebenfalls die Teilprozesse: Qualitätsplanung (QP), Qualitäts-Sicherung (QS), Qualitäts-Controlling (QC). Gemäss Prozessanweisung ar Immo wird zur Sicherstellung des übergeordneten Total Quality Management (TQM) das Dokument Q-Lenkungsplan erstellt. Im Q-Lenkungsplan werden das Projekt, die Grundlagen und die Ziele phasengerecht kurz umschrieben, zudem wird der Projektstand dokumentiert. Hauptthema ist das Risikomanagement, in welchem die Risikobetrachtung und -Bewertung sowie die Definierung von Massnahmen zur Risikominimierung behandelt wird. (Definition armasuisse: «VA (Verfahrensanweisung) Qualitätsmanagement» Dokument ID 1000 vom 21.08.2020)
TIER	Zur Klassifizierung von Rechenzentren wurde die TIER-Topologie Ende der 1990er Jahre vom Uptime Institut mit Sitz in den USA, weltweit als Standard eingeführt. Jedes «TIER» (Stufe) steht für einen bestimmten Rang, den das jeweilige Rechenzentrum bzw. dessen Subsysteme erfüllt. Die TIER-Topologie sieht insgesamt vier Stufen (TIER I bis TIER IV) vor, wobei TIER I die am wenigsten zuverlässige Umgebung ist und TIER IV als «hochverfügbar» eingestuft wird.

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).

Anhang 4: Follow-up der offenen Empfehlungen

Nr.	Massnahme	Status und Rückmeldungen der Geprüften	Beurteilung
15511.002	Soll-Frist: 31.12.2017, Nachfrist: 30.11.2020 Die EFK empfiehlt dem VBS, die Zentralisierung und Definition der Systeme für «FUNDAMENT» und «KASTRO II» mit hoher Priorität voranzutreiben um die Betreibbarkeit zu bestätigen. Dazu muss auch der Personalkörper für den Betrieb in allen Lagen ermittelt und gesichert werden.	Stand 04.11.2020: Die Definition der auf den militärischen RZ-Verbund zu migrierenden Systemen ist grösstenteils abgeschlossen. Die Anwendungen wurden gemäss ihrer Relevanz für den Einsatz der Armee beurteilt und in entsprechende Gruppen eingeteilt. Die daraus resultierende Liste der «Kernsysteme/-anwendungen» ist die Grundlage für die noch laufende Migrationsplanung. Die für den Betrieb nötigen Personalressourcen wurden im 2017 erstmals abgeschätzt. Der Personalkörper um die Immobilien zu betreiben ist fixiert. Die Personen für diese Aufgaben sind in «CAMPUS» für den Betrieb verantwortlich und in «FUNDAMENT» übernehmen sie voraussichtlich Ende 2020 ihre Betriebsverantwortung. Der Aufwand für den Betrieb der IKT Plattform sowie der Anwendungen kann heute noch nicht abschliessend abgeschätzt werden. Der Bedarf wird sich mit der fortlaufenden Planung sowie der eigentlichen Migration von Anwendungen und Diensten konkretisieren. Das Betriebspersonal für Plattform und Anwendungen sollte jedoch die Anzahl der heute verfügbaren Vollzeitstellen für die gleichartigen Aufgaben nicht übersteigen. Das Thema Ressourcen ist in der FUB ein Fokuspunkt und wird mit grosser Aufmerksamkeit, auch auf der Stufe V und VBS verfolgt. Dementsprechend beantragt das VBS, diese Empfehlung zu schliessen und die Verfolgung der Fortschritte und die Sicherstellung der Betreibbarkeit der Linie zu übertragen.	Stand Dezember 2021 Die zu migrierenden Systeme sind bekannt und werden im Rahmen des Teilprojektes MIGRA für die Verschiebung auf die Digitalisierungsplattform der Armee vorbereitet. Die ersten Anwendungen sollen 2024 auf der neuen Infrastruktur des RZ «FUNDAMENT» in Betrieb genommen werden. Beide Rechenzentren sind seit 2020 bzw. 2021 in Betrieb und die Organisation ist inzwischen eingespielt. Die Ressourcen für den Betrieb der Anlagen und der Domotik genügen den betrieblichen Anforderungen in allen Lagen. Der Betrieb der IKT-Systeme kann mit gewissen Einschränkungen über alle Lagen gewährleistet werden (siehe Kapitel 5.4). Die Empfehlung kann geschlossen werden.

Nr.	Massnahme	Status und Rückmeldungen der Geprüften	Beurteilung
17410.005	Soll-Frist: 31.12.2018, Nachfrist: 30.06.2020 Die EFK empfiehlt der Gruppe Verteidigung, das Migrationsprojekt und damit die Themen technische Zielarchitektur FUB, Ermittlung der aus dem Entflechtungsentscheid resultierenden Mengen und Abstimmung dieser mit dem BIT sowie den Wissenstransfer des Gesamtprojektleiters ins RZ VBS/Bund 2020 schnellstmöglich voranzutreiben und mit dem nächsten IKT SPP-Reporting (Sommer 2018) den Stand der einzelnen Aufgaben explizit auszuweisen.	Stand am 04.11.2020: Im Rahmen des Migrationsprojekts innerhalb des Projekts RZ VBS/Bund 2020 wurden sämtliche zu migrierenden Anwendungen und Systeme analysiert. Die zu migrierenden Systeme wurden in Abstimmung mit dem A Stab, den betroffenen Nutzerorganisationen und unter Berücksichtigung des Entflechtungsentscheids festgelegt. Die Anwendungen wurden entsprechend ihrer Komplexität in verschiedene Klassen eingeteilt. Die weitere Bearbeitung und die Initialisierung der Migration jeder einzelnen Anwendung wird in Kürze starten. Auch konnte zwischenzeitlich die technische Zielarchitektur festgelegt werden. Die im Projekt RZ VBS/Bund 2020, IKT Architektur und Infrastruktur nötigen Anpassungen wurden formuliert und werden voraussichtlich im Herbst 2020 im Rahmen eines Changes des Projekts bewilligt und anschliessend mit dem Lieferanten Swisscom umgesetzt. Die Projektleitung des Gesamtprojekts ist stabil. Nebst dem Gesamt PL steht eine interne Person als PL Stv zur Verfügung welche das Wissen des Gesamt PLs bezüglich des Projekts zu sehr grossen Teilen auch hat.	Stand Dezember 2021 Die zu migrierenden Systeme sind bekannt und werden im Rahmen des Teilprojektes MIGRA für die Verschiebung auf die Digitalisierungsplattform der Armee vorbereitet. Die ersten Anwendungen sollen 2024 produktiv auf der neuen Infrastruktur des RZ «FUNDAMENT» in Betrieb genommen werden. Die Konzepte zur Zielarchitektur sind erstellt und die Umgebung wird seit September 2021 im RZ «CAMPUS» aufgebaut und entwickelt (siehe Kapitel 5). Die Projektorganisation ist nach HERMES aufgebaut und der Wissenstransfer findet auf verschiedenen Stufen statt (siehe Kapitel 2.1). Die Empfehlung kann geschlossen werden.

Nr.	Massnahme	Status und Rückmeldungen der Geprüften	Beurteilung
18491.001	Soll-Frist: 30.06.2020, Nachfrist: 31.07.2021 Die EFK empfiehlt dem ISB, in Zusammenarbeit mit dem ISC-EJPD, dem BIT und der FUB, dafür zu sorgen, dass die Rechenzentren der zentralen Bundesverwaltung und der dezentralen Bundesverwaltung sowie weiterer Behörden – soweit wirtschaftlich – gemäss Konzept «S04 – Datacenter-Verbund» in den RZ-Verbund migriert werden.	Bemerkung zur Nachfrist: Im Rahmen der strategischen Initiative SI-4 ”Hybrid Multi-Cloud” wird die Strategie RZ-Verbund bis Mitte 2021 erarbeitet. Dazu gehört auch das Self-Assessment, ob RZ-Flächen (1:1-Umzug von Racks, HW) in die zentralen RZ migriert werden können. Dazu wurde ein Unterstützungsauftrag an eine externe Firma erteilt. Die Ergebnisse werden in die RZ-Strategie mit einfliessen. Zudem wird in der SI-4 auch ein strategisches Portfolio zu Zielplattformen/-Infrastrukturen (-Services) angegangen und ein Entscheidmodell erstellt zur Beurteilung, welche (Arten von) Anwendungen basierend auf welchen Zielarchitekturen auf welche Zielplattformen/Infrastrukturen abgestützt werden können. Dies dient als Alternative für einen 1:1-Umzug von Racks oder HW.	Stand Dezember 2021 Das Konzept «Rechenzentren-Verbund für die zentrale Bundesverwaltung» stammt aus dem Jahre 2014. In den letzten fünf Jahren gab es neue Erkenntnisse, was den prognostizierten Bedarf an RZ-Leistungen und die RZ-Architekturen betrifft. Zudem muss berücksichtigt werden, dass mit dem Bezug von Diensten aus der öffentlichen Cloud und /oder mit einem strategischen Outsourcing weniger RZ-Leistungen aus bundeseigenen RZ bereitgestellt werden müsste und ein Leerstand in den bundeseigenen RZ zu vermeiden ist. Das aktuelle Konzept fokussiert sich primär auf die Anforderungen der departementalen IKT-Leistungserbringer. Das neue Konzept wird die Anforderungen der weiteren IKT-Leistungserbringer der zentralen Bundesverwaltung und deren allfälligen Rechenzentren/Serverräume mitberücksichtigen. Gemäss einer Umfrage der DTI bei den Departementen sind im zivilen Bereich der BV heute noch 25 RZ in Betrieb. Ein Ziel der Umfrage war die Klärung des Bedarfs für eine Integration in den RZ-Verbund (siehe Kapitel 6). Die überarbeitete RZ-Strategie liegt vor, ist jedoch zum Prüfzeitpunkt noch nicht verabschiedet. Die Empfehlung kann geschlossen werden.