INFORMATIKPROJEKTE

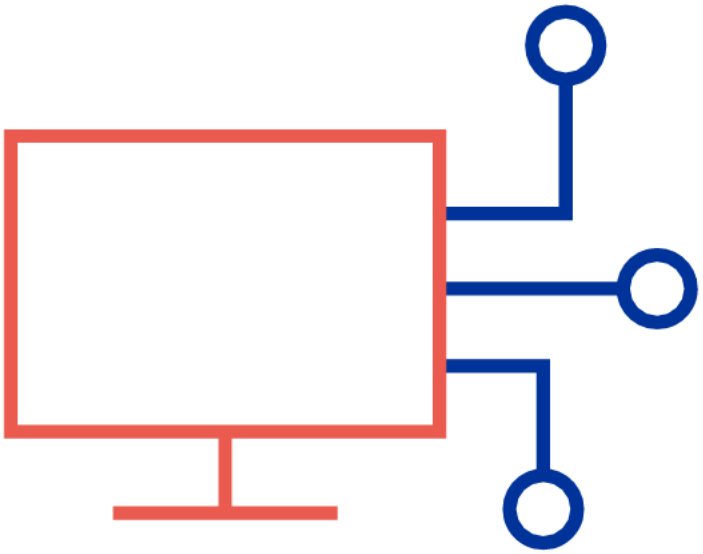
Prüfung der Sicherheit der Secure Private Cloud

Informatik Service Center des Eidgenössischen Justiz- und Polizeidepartements

EFK-24110

VERSION INKL. STELLUNGNAHMEN

08.01.2025



EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
CONTROLLA FEDERALA DA FINANZAS
SWISS FEDERAL AUDIT OFFICE

DOKUMENTINFORMATION

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	485.24110
ZUSÄTZLICHE INFORMATIONEN COMPLÉMENT D'INFORMATIONS INFORMAZIONI COMPLEMENTARI ADDITIONAL INFORMATION	www.efk.admin.ch info@efk.admin.ch + 41 58 463 11 11
ABDRUCK REPRODUCTION RIPRODUZIONE REPRINT	Gestattet (mit Quellenvermerk) Autorisée (merci de mentionner la source) Autorizzata (indicare la fonte) Authorized (please mention source)

PRIORITÄTEN DER EMPFEHLUNGEN

Die Eidgenössische Finanzkontrolle priorisiert ihre Empfehlungen auf der Grundlage definierter Risiken: 1 = hoch, 2 = mittel, 3 = gering.
Als Risiken gelten beispielsweise unrentable Projekte, Verstösse gegen die Legalität oder Ordnungsmässigkeit, Haftungsfälle oder Reputationsschäden. Damit werden die Auswirkungen und die Wahrscheinlichkeit des Eintretens beurteilt. Diese Beurteilung richtet sich nach dem konkreten Prüfungsgegenstand (relativ) und nicht nach der Relevanz für die Bundesverwaltung als Ganzes (absolut).

INHALTSVERZEICHNIS

Das Wesentliche in Kürze **4**

1 Auftrag und Vorgehen **7**
1.1 Ausgangslage 7
1.2 Prüfungsziel und-fragen 7
1.3 Prüfungsumfang und-grundsätze 7
1.4 Unterlagen und Auskunftserteilung 7
1.5 Schlussbesprechung 7

2 Secure Private Cloud des ISC-EJPD **9**
2.1 Anforderungen der Cloud Stufe IV müssen erst erarbeitet werden 10
2.2 Die SPC wurde für einen sicheren Betrieb konzipiert 11
2.3 Eine hohe Verfügbarkeit der Daten ist durch geeignete Massnahmen adressiert 12
2.4 Die Kontrolle der Vorgaben sollte verbessert werden 13
2.5 Voraussetzungen zum Betrieb von externen Fachanwendungen müssen geschärft werden 14
2.6 Security Monitoring sollte zentral aufgesetzt werden 14
2.7 Die IT-Security Auditplanung sollte verfeinert werden 15
2.8 Das Lifecycle Management wird konsequent umgesetzt 16

3 Umsetzung früherer Empfehlung **17**
3.1 Das Dokument «Bewältigung von Cybervorfällen im EJPD» wurde erstellt 17

Anhang 1 – Rechtsgrundlagen und Rechtstexte 18
Anhang 2 – Abkürzungen 19
Anhang 3 – Glossar 20
Anhang 4 – Cloud-Stufen der Bundesverwaltung 22

PRÜFUNG

Prüfung der Sicherheit der Secure Private Cloud

Informatik Service Center des Eidgenössischen Justiz- und Polizeidepartements

DAS WESENTLICHE IN KÜRZE

Die Bundesverwaltung betreibt ihre Anwendungen in eigenen Rechenzentren, in Private Clouds und in Public Clouds von mehreren Anbietern. Mit der Cloud Strategie Bund hat der Bundesrat im 2020 ein Cloud-Stufen-Modell[1] beschlossen, welches vier Sicherheitsstufen definiert. Das Informatik Service Center des Eidgenössischen Justiz- und Polizeidepartements (ISC-EJPD) betreibt eine Secure Private Cloud (SPC), die gemäss dieser Cloud-Strategie eine Cloud der Stufe IV «Bundeseigene Private Cloud+» darstellt. Bisher steht diese Cloud den Ämtern des EJPD zur Verfügung. Im Rahmen der Weiterentwicklung der Cloud-Strategie ist geplant, diese auch für weitere Kunden innerhalb des Bundes zugänglich zu machen. Die Cloud Leistungen werden als Plattform-as-a-Service (PaaS) angeboten.

Die vorliegende Prüfung soll klären, ob die SPC als Plattform sicher und zuverlässig betrieben wird. Dabei liegt der Fokus insbesondere auf der Sicherheit der Plattformdienstleistungen. Zudem soll überprüft werden, ob die SPC die Vorgaben des Bereichs Digitale Transformation und IKT-Lenkung (DTI) der Bundeskanzlei erfüllt.

Die Anforderungen müssen durch den Bereich DTI erst noch erstellt werden. Daher kann das ISC-EJPD diese formell nicht erfüllen. Die SPC wurde jedoch so konzipiert, dass sie für Fachanwendungen mit erhöhten Schutzanforderungen geeignet ist. Im Rahmen der Prüfung hat sich Verbesserungspotential im Bereich Vorgaben, Security Monitoring sowie der Planung von IT-Audits ergeben.

Anforderungen des DTI müssen präzisiert werden

Der Bereich DTI hat im Dezember 2020 die aktuelle Cloud-Strategie der Bundesverwaltung veröffentlicht, welche die Vision und Ziele der Cloud-Nutzung bis 2025 festlegt. Eine Weisung zu den Cloud-Prinzipien trat im Oktober 2023 in Kraft und führt ein Modell der Cloud-Stufen der Bundesverwaltung ein.

Die DTI-Dokumente legen aus Sicht der Leistungsbezüger (LB) fest, welche Anwendungsfälle durch die verschiedenen Stufen abgedeckt werden sollten. Dies insbesondere in Bezug auf Datenklassifizierung, Datenschutz und digitale Souveränität der Schweiz. Es fehlen detaillierte Vorgaben zu den Sicherheitsmerkmalen für die verschiedenen Cloud-Stufen. Im Rahmen der Vorbereitungsarbeiten zum Aufbau der Swiss Government Cloud hat der Bereich DTI vom Bundesrat einen Auftrag zur Präzisierung dieses Cloud Stufenmodells bis Ende 2024 erhalten. Die Umsetzung des Auftrags ist noch offen. Die technische Umsetzung muss danach durch das SEPOS in Zusammenarbeit mit DTI und den Leistungserbringern (LE) verifiziert und allenfalls konkretisiert werden.

Die SPC wurde sicher konzipiert

Unabhängig von den fehlenden Vorgaben für die Cloud Stufe wurde die SPC mit einem Fokus auf den Betrieb für sicherheitskritische und hochverfügbare Fachanwendungen konzipiert und aufgebaut. Sie deckt den IKT-Grundschutz des Bundes sowie die bisher vom EJPD festgelegten und angewandten weitergehenden IT-Sicherheitsanforderungen für den Betrieb solcher Anwendungen ab.

Eine hohe Verfügbarkeit wird insbesondere mit Redundanz innerhalb der Rechenzentren sowie dem Aufbau weiterer Standorte in verschiedenen Regionen sichergestellt. Die rasche Wiederherstellung von

[1] Siehe Anhang 4

Fachanwendungen respektive der Plattform wird durch die gewählte Architektur und Virtualisierung erleichtert. Sie wird aber auch mittels Tests geübt.

Zudem wird dem Lifecycle erhöhte Beachtung geschenkt und die Plattform sowie die Anwendungen werden auf einem aktuellen Stand gehalten.

Vorgaben an die Bezüger von Plattformleistungen sollen geschärft und deren Umsetzung kontrolliert werden

Die Verantwortung für die IT-Sicherheit (Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit) wird bei cloudbasierten Anwendungen zwischen Leistungserbringer (LE) und LB geteilt. Das ISC-EJPD hat Vorgaben erstellt, welche eine Fachanwendung erfüllen muss, damit sie auf der SPC betrieben werden kann. Die Umsetzung dieser Vorgaben durch die LB sollten soweit möglich überprüft und durchgesetzt werden.

Damit die Sicherheit der SPC nicht durch weitere Kunden des Bundes gefährdet wird, müssen weitere Implementierungsdetails definiert und die Rolle des Cloud Service Brokers, resp. des Integrators, geschärft werden. Um die technische Sicherheit zu gewährleisten werden bereits unterschiedliche Massnahmen umgesetzt (z.B. logische Isolierung, Hardwaretrennung usw.).

Security Monitoring sollte zentralisiert und die Auditplanung verfeinert werden

Zum Prüfzeitpunkt werden Logging- und Überwachungsdaten der Plattform gesammelt. Diese sind für die verschiedenen Teams im ISC-EJPD für Auswertungen zugänglich. Für Betrieb und Fehlersuche reicht dies aus. Sicherheitsrelevante Informationen werden teilweise an eine zentrale Datenbank weitergeleitet. Es fehlt jedoch ein übergeordnetes Konzept um den vollen Nutzen aus den vorhandenen Daten zu ziehen. Das ISC-EJPD hat dies erkannt und ist daran ein Security Operations Center zu konzipieren, welches diese Aufgabe umsetzen kann.

Externe Tests der IT-Sicherheit werden für die SPC und ihre Umsysteme durchgeführt. Mit einem übergeordneten Audit Konzept sollten diese Tests besser aufeinander abgestimmt und damit deren Nutzen vergrössert werden.

Empfehlung zur besseren Bewältigung von Cybervorfällen wurde umgesetzt

Im Rahmen dieser Prüfung wurde die Umsetzung einer Empfehlung aus einem früheren Bericht[1] geprüft. Das ISC-EJPD hat ein Dokument zur «Bewältigung von Cybervorfällen im EJPD (Zusammenarbeit zwischen LE und LB)» erstellt. Dieses wurde den LB zur Verfügung gestellt.

[1] «Prüfung Sicherheit der Datenbank INFOSTAR» (PA 21135) auf der Webseite der EFK abrufbar

GENERELLE STELLUNGNAHME DES ISC-EJPD

Das ISC-EJPD bedankt sich bei der Eidgenössischen Finanzkontrolle für die konstruktive und zielführende Durchführung der Prüfung, welche die Wichtigkeit des Themas aufzeigt und die damit verbundenen Herausforderungen ausgewogen darlegt. Das ISC-EJPD nimmt die positive Würdigung der Secure Private Cloud EJPD dankend zur Kenntnis und ist mit den Empfehlungen einverstanden.

GENERELLE STELLUNGNAHME DER BUNDESKANZLEI BEREICH DIGITALE TRANSFORMATION UND IKT-LENKUNG

Die Bundeskanzlei dankt der EFK für die Gelegenheit zur Stellungnahme. Der Bundesratsauftrag zur Präzisierung des Cloud-Stufenmodells ist bearbeitet worden. Das präzisierte Cloud-Stufenmodell bietet die Grundlage für eine Definition genereller Sicherheitsmerkmale für die Cloud-Stufen (Empfehlung 1). Der Bereich DTI der Bundeskanzlei bietet zudem Unterstützung bei der Ausarbeitung der Sicherheitsanforderungen für die Cloud-Stufen unter Federführung des SEPOS (Empfehlung 2).

GENERELLE STELLUNGNAHME STAATSSEKRETARIAT FÜR SICHERHEITSPOLITIK

Das SEPOS begrüsst die Prüfungsinitiative der EFK, die vorgeschlagene Vorgehensweise sowie die Feststellungen, die im Rahmen der Prüfung gemacht wurden.

Insbesondere die Feststellung zum Verbesserungspotenzial im Bereich Vorgaben wurde zur Kenntnis genommen. Das SEPOS wird mit den in diesem Jahr geplanten neuen Bearbeitungsvorschriften zur Klassifizierung einen wesentlichen Beitrag zur Optimierung in diesem Bereich leisten.

Da die Secure Private Cloud (SPC) speziell für Fachanwendungen mit erhöhten Schutzanforderungen konzipiert ist, werden die Zertifizierungsvorgaben des SEPOS zu sensitiven IKT-Mitteln künftig weitere Klarheit und Orientierung schaffen. Dies wird die Anforderungen für Anwendungen und Systeme mit hohen Sicherheitsstandards präzisieren und deren Umsetzung fördern.

Positiv hervorzuheben und als unumgängliche Anforderung zu bestätigen ist die Prüfungsfeststellung, dass der IT-Grundschutz konsequent eingehalten werden muss. Dieser stellt eine wesentliche Grundlage für die Sicherheit und den Schutz der sensiblen Daten sowie der Fachanwendungen dar.

Um offene Punkte (Cloud-Stufen, Krypto) zu klären oder vertiefend auszuarbeiten, bietet das SEPOS jederzeit das Gespräch an. Wir freuen uns auf eine konstruktive Zusammenarbeit und den weiteren Austausch zu den genannten Themen.

1 AUFTRAG UND VORGEHEN

1.1 Ausgangslage

Der Bundesrat hat eine Cloud-Strategie verabschiedet, welche bezüglich IT-Sicherheit vier Stufen definiert. In diesem Umfeld betreibt das Informatik Service Center des Eidgenössischen Justiz- und Polizeidepartements (ISC-EJPD) eine Secure Private Cloud (SPC) welche gemäss der Cloud-Strategie in die Stufe IV «Bundeseigene Private Cloud+» fällt. Der aktuelle Fokus der SPC liegt grundsätzlich bei den Leistungsbezügern des EJPD. Die SPC steht heute bereits für Pilotprojekte unterschiedlicher Ämter auch ausserhalb des EJPD zur Verfügung (ein Pilotprojekt wurde bereits produktiv realisiert). Mit der Weiterentwicklung der Cloud-Strategie ist angedacht, diese Stufe IV Cloud für weitere Kunden im Bund zur Verfügung zu stellen. Die Cloud wird im Modell Platform-as-a-Service (PaaS) angeboten. Mit der Prüfung soll beurteilt werden, ob die SPC als Plattform zuverlässig und sicher ist. Zudem soll überprüft werden ob die SPC die Anforderungen des Bereichs Digitale Transformation und IKT-Lenkung (DTI) der Bundeskanzlei erfüllt.

1.2 Prüfungsziel und -fragen

Ziel der Prüfung war die Beurteilung, ob die Secure Private Cloud vom ISC-EJPD sicher und zuverlässig betrieben wird

Die Prüffragen lauten:

1. Ist der Betrieb der Secure Cloud sicher und erfüllt die Anforderungen der Cloud Stufe IV des DTI-Modells?
2. Hat das ISC-EJPD Massnahmen ergriffen, um den technologischen Life-Cycle zu managen?
3. Sind die Strukturen geeignet um Fachanwendungen ausserhalb des EJPD auf der Secure Cloud sicher zu betreiben?

Daneben wurde die Umsetzung einer Empfehlung nachgeprüft, welche die EFK im 2021 ausgesprochen hatte (21135.004[1]).

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Christian Brunner (Revisionsleitung), André Stauffer und mit Unterstützung einer externen Firma vom 29. Juli bis 23. August 2024 durchgeführt. Sie erfolgte unter der Federführung von Bernhard Hamberger. Der vorliegende Bericht berücksichtigt nicht die weitere Entwicklung nach der Prüfungsdurchführung.

1.4 Unterlagen und Auskunftserteilung

Die notwendigen Auskünfte wurden der EFK von allen Beteiligten umfassend und zuvorkommend erteilt. Die gewünschten Unterlagen sowie die benötigte Infrastruktur standen dem Prüfteam vollumfänglich zur Verfügung.

1.5 Schlussbesprechung

Die Schlussbesprechung fand am 19. November 2024 statt. Teilgenommen haben seitens ISC-EJPD der Leiter Informatik Service Center, der AL Technologie, der Stv. AL T/BL A/Senior ICT Architekt, der AL Betrieb und Support, der BL Cloud-Plattformen und der Senior ICT-Sicherheitsbeauftragte, seitens DTI der Leiter AI Stv.- Leiter TI und ein Unternehmensarchitekt und seitens SEPOS die Chefin Fachstelle des Bundes für

[1] «Prüfung der Sicherheit der Datenbank INFOSTAR» (PA 21135), verfügbar auf der Webseite der EFK.

Informationssicherheit. Von der EFK haben der Fachbereichsleiter sowie der Revisionsleiter teilgenommen.

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

EIDGENÖSSISCHE FINANZKONTROLLE

[redacted]

[redacted]

Fachbereichsleiter

Prüfungsexperte

2 SECURE PRIVATE CLOUD DES ISC-EJPD

Die SPC wurde entwickelt um für sicherheitskritische und hochverfügbare Fachanwendungen eine zukunftsgerichtete Plattform bereitzustellen. Die Plattform basiert auf dem Open-Source System Kubernetes. Dieses System unterstützt die automatische Bereitstellung, Verwaltung und Skalierung von Anwendungen in sogenannten Containern, einer Art standardisierter, ausführbarer Software-Behälter. Die SPC ist für Fachanwendungen konzipiert, die nach modernen Cloud-Standards entwickelt werden und in einer hochsicheren Umgebung laufen müssen.

Das ISC-EJPD stellt mit der SPC den Nutzern aus dem Bundes- und bundesnahen Umfeld eine Gesamtlösung als Plattform zur Verfügung, die auf einer Reihe von aufeinander aufbauenden Softwarekomponenten, basiert (siehe grüne Bereiche in Abbildung 1). Die Plattform ist hochautomatisiert und bietet einen hohen Sicherheitsstandard. Für die Verwaltung der Zugriffsrechte und Benutzerkonten nutzt die Plattform das etablierte Single-Sign-On (SSO)-Portal des EJPD. Dieses bietet nicht nur sicheren Zugang, sondern auch umfassende Möglichkeiten der Steuerung der Identitätsverwaltung und des Zugriffs auf Fachanwendungen.

Neben der Kubernetes-Plattform, dem SSO-Portal, sowie einer Container-Registrierung, werden verschiedene Zusatzdienste angeboten (siehe Abbildung 2). Diese Services können von den Nutzern flexibel verwaltet und bei Bedarf dynamisch angepasst werden.

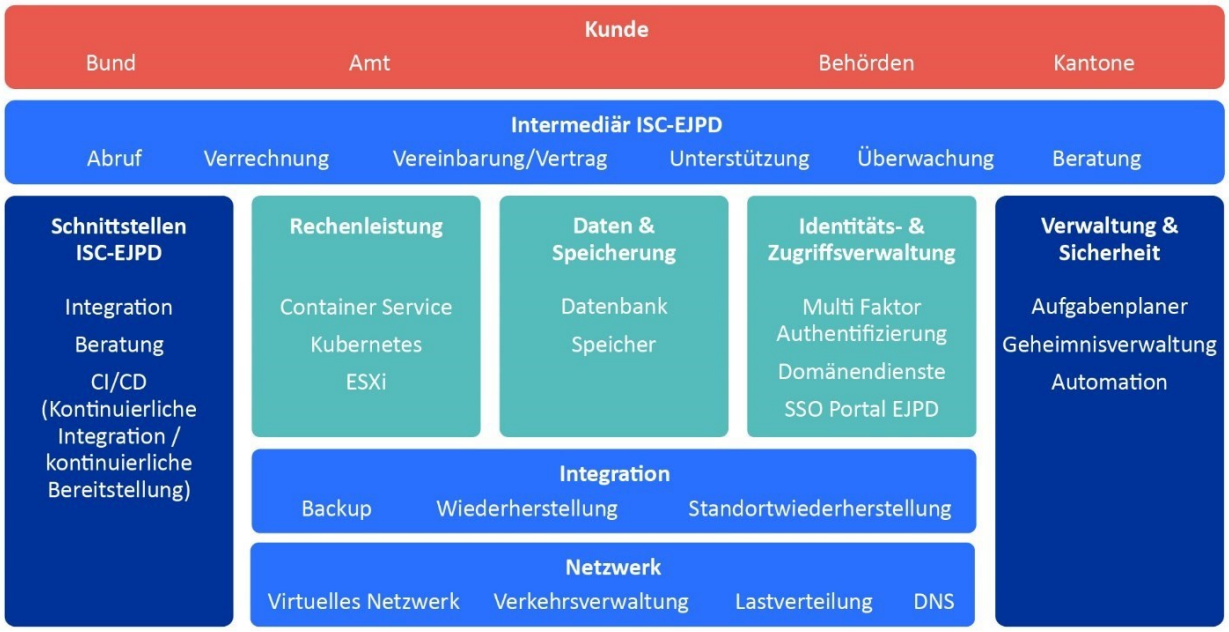


Abbildung 1 Big Picture – Secure Private Cloud, Quelle: ISC-EJPD, Darstellung EFK

Abbildung 2 Serviceoptionen der Secure Private Cloud Plattform, Quelle: ISC-EJPD, Darstellung EFK

2.1 Anforderungen der Cloud Stufe IV müssen erst erarbeitet werden

Der Bereich DTI hat die aktuell gültige Cloud-Strategie im Dezember 2020 veröffentlicht. Das Dokument beschreibt die Vision und das Zielbild der Cloud-Nutzung in der Bundesverwaltung bis 2025. Eine Weisung zu den Cloud-Prinzipien der Bundesverwaltung wurde im Oktober 2023 in Kraft gesetzt. Sie hat Governance Themen im Fokus und zum Ziel, eine Nutzung der Cloud-Dienste nach einheitlichen Prinzipien zu fördern, eine Hilfestellung bei der Wahl der Cloud-Modelle zu bieten und einheitliche Prinzipien für die Arbeit der Cloud Service Broker (CSB) zu definieren. Ein Modell der Cloud-Stufen wird vorgeschlagen, wobei eine Stufe IV «Bundeseigene Private Cloud+» eingeführt wird. Als Beispiel für diese Stufe wird die SPC des ISC-EJPD aufgeführt.

Die Dokumente des Bereichs DTI beschreiben aus Sicht der Leistungsbezüger (LB), welche Use-Cases bzgl. Datenklassifizierung, Datenschutz und der digitalen Souveränität der Schweiz durch die verschiedenen Stufen abgedeckt werden sollen. Es fehlen Dokumente, welche die konkreten Sicherheitsanforderungen an die verschiedenen Plattformen festlegen.

Im Rahmen der Vorbereitungsarbeiten zum Aufbau der Swiss Government Cloud hat der Bereich DTI einen Auftrag des Bundesrates erhalten, die Abgrenzung der Cloud-Stufen I-IV zu konkretisieren. Zur Zeit der Prüfung bestand beim Bereich DTI erst ein Auftrag zur Etablierung der Abgrenzung der Cloud-Stufen III und IV. Die Details der konkreten Planungselemente sind jedoch noch nicht definiert und keine für die Umsetzung oder Erarbeitung verantwortliche Person bestimmt. Ab September 2024 sollen sich zwei Personen darum kümmern. Der Endtermin für den Auftrag wurde auf Ende 2024 festgelegt.

BEURTEILUNG

Die Definition der Sicherheitsmerkmale der entsprechenden Cloud-Stufen fehlt. Somit besteht das Risiko, dass die Cloud-Stufen, insb. die Stufen III und IV, schlecht abgegrenzt sind und dass die Plattformen teilweise redundante Services anbieten oder dass Lücken zwischen den Cloud-Stufen entstehen.

Der Bereich DTI hat die Problematik erkannt. Aufgrund der vorgesehenen Aktivitäten im Rahmen des BR-Auftrags zur Abgrenzung der Cloud-Stufen erwartet die EFK, dass Sicherheitsanforderungen an die verschiedenen Stufen konkret definiert und deren Umsetzung anschliessend kontrolliert werden.

EMPFEHLUNG 1 — PRIORITÄT 1

Die EFK empfiehlt dem Bereich DTI in Zusammenarbeit mit den Leistungserbringern die relevanten generellen Sicherheitsmerkmale für die Cloud Stufen verbindlich zu definieren.

STELLUNGNAHME DES BEREICHS DTI

Die Empfehlung ist akzeptiert.

Im Rahmen des Bundesratsauftrags zur Präzisierung des Cloud-Stufenmodells wurden die Grundlagen für die Sicherheitsmerkmale der verschiedenen Cloud Stufen gelegt und es erfolgte die genauere Abgrenzung der Stufen III und IV auch anhand wesentlicher Sicherheitsaspekte. Insbesondere für die Stufe IV wurden Anforderungen bezüglich Datenzugriff (Sicherheitsstufe 4), Hardware (dedizierte Serverzone) sowie Zutrittsberechtigungen erfasst. Die verbindliche Vorgabe für alle Stufen I-IV wird mit der Abnahme der Cloud Prinzipien veröffentlicht.

EMPFEHLUNG 2 — PRIORITÄT 1

Die EFK empfiehlt dem SEPOS in Zusammenarbeit mit dem Bereich DTI sowie den Leistungserbringern die Details zur Umsetzung der Sicherheitsanforderungen für die Cloud Stufen zu definieren.

STELLUNGNAHME DES SEPOS

Die Empfehlung ist akzeptiert.

voir prise de position générale

2.2 Die SPC wurde für einen sicheren Betrieb konzipiert

Die SPC ist für das EJPD eine strategisch wichtige Betriebsplattform, welche nur unter Einhaltung der Vorgaben des ISC-EJPD genutzt werden darf. Sie folgt dem Cloud-native Ansatz und hat den Anspruch einerseits den IKT-Grundschutz des Bundes aber auch die bisher angewandten weitergehenden IT-Sicherheitsanforderungen für den Betrieb sicherheitskritischer und hochverfügbarer Fachanwendungen abzudecken. Darüber hinaus soll sie weiteren erhöhten Sicherheitsanforderungen (z. B. CIS-Kubernetes Benchmark[1]) gerecht werden und Anwendungen, wo erforderlich, mit einer Verfügbarkeit von 99,8% bereitstellen. Mit zwei zusätzlichen Standorten und der Einführung eines Zonenkonzepts soll bis Ende 2025 eine Verfügbarkeit von 99.98% möglich werden. Die von den SLAs geforderte Verfügbarkeit wird gemessen und konnte bisher immer eingehalten werden.

Technologisch basiert die SPC auf Kubernetes, welches durch eine Kubernetes-Management-Lösung von VMware orchestriert und administriert wird. Die Plattform wird auf virtualisierter Infrastruktur betrieben und nutzt die verfügbaren Netzwerkvirtualisierungs-, Skalierungs-, Loadbalancing- sowie Backup- und Restore (Snapshots) Mechanismen.

Die LB können ihre Anwendungen über ein von der Plattform bereitgestelltes Self-Service-Portal verwalten und administrieren. Wo möglich wird auf den GitOps und Infrastructure-as-Code (IaC)-Ansatz gesetzt, um Applikationen sowie auch Infrastruktur automatisiert zu konfigurieren und zu provisionieren.

Es werden primär Linux Betriebssysteme unterstützt und mittels unterschiedlicher Methoden ausgerollt. Die Container-Images der Applikationen werden in einer redundanten Image Bibliothek verwaltet.

Security hat einen hohen Stellenwert und ist nach dem Defense in Depth Prinzip umgesetzt. Die Ansätze von Perimeterschutz und Mikrosegmentierung werden in einem dreistufigen Firewall-Konzept

[1] https://www.cisecurity.org/benchmark/kubernetes

kombiniert. Jede Fachanwendung wird in einem eigenen, isolierten Bereich betrieben. Die Separierung der Bereiche erfolgt durch software-definierte Firewall-Mechanismen.

Um Fachapplikationen mit unterschiedlichen Anforderungen, Integrationsstufen und/oder Verantwortungsbereichen weiter zu trennen, werden diese in abgeschotteten Umgebungen, sogenannten Tenants, betrieben, welche auf dedizierter, physisch getrennter Hardware realisiert werden.

BEURTEILUNG

Die SPC wurde mit moderner Technologie und nach zweckmässigen Security-Grundsätzen konzipiert. Die konsequente Hardwaretrennung der Tenants und die klaren technischen, architektonischen und organisatorischen Vorgaben sind grosse Stärken der Lösung.

Mit dem CIS Kubernetes Benchmark wird ein etabliertes und zweckmässiges Security Framework zur Härtung der Plattforminfrastruktur verwendet. Die implementierten Security-Mechanismen erscheinen insgesamt gut gewählt und implementiert und sorgen für ein Schutzniveau, das den Anforderungen der heutigen sicherheitskritischen und hochverfügbaren Fachanwendungen gerecht wird.

Die durch die SLA zugesicherte Verfügbarkeit der Plattform war in der Vergangenheit gegeben und wird weiter ausgebaut.

2.3 Eine hohe Verfügbarkeit der Daten ist durch geeignete Massnahmen adressiert

Für die Datenhaltung bietet das ISC-EJPD Datenbanken als Managed Service an, welche von den LB benutzt werden können. Die Redundanz der Applikationen ist (wo entsprechend bestellt) durch das standort-redundante Linienkonzept implementiert. Hierbei erfolgt ein transparentes Loadbalancing zwischen mehreren Rechenzentren. Fachanwendungen werden dementsprechend standort-redundant in separaten Kubernetes-Clustern betrieben. Die Datenbestände werden separat zwischen den Standorten repliziert, wodurch sich im Fall eines Failovers ein kleines Zeitfenster möglichen Datenverlusts ergibt, welches im Service Level Agreement (SLA) ausgewiesen wird.

Für Backup und Restore der einzelnen Plattform-Komponenten gelten unterschiedliche Zuständigkeiten. Allfällig benötigte Restores können vom Cloud Plattformen Team selbständig erfolgen, wenn der gewünschte Recovery-Zeitpunkt nicht länger als 5 Tage in der Vergangenheit liegt (Snapshots). Backups erfolgen im Mehrgenerationenprinzip und werden ausgelagert. Restoretests der Plattformkomponenten werden seit kurzem regelmässig durchgeführt und dokumentiert. Im Rahmen des Projekts RZ-Umzug Bern wurden vollumfängliche Verfügbarkeitstests bis zur Stufe Produktion durchgeführt. Weiter wird auch beim Neubau der Infrastruktur in den zusätzlichen Standorten (Frauenfeld), die Wiederherstellung der gesamten Plattform sowie von definierten Fachanwendungen von Grund auf getestet.

Die Infrastruktur der Plattform kann mit einem IaC Ansatz automatisiert ausgerollt werden, sofern die erforderlichen Grundsysteme verfügbar sind. Im Fehlerfall kann daher zu weiten Teilen auf ein Restore der entsprechenden Komponenten verzichtet werden und stattdessen die betroffene Komponente mittels IaC neu gebaut und ausgerollt werden.

BEURTEILUNG

Im Fehlerfall können virtuelle Maschinen entweder ab Snapshots komplett wiederhergestellt oder Komponenten via IaC neu gebaut und ausgerollt werden. Dies ist ein übliches und zweckmässiges Vorgehen. Da die Zuständigkeiten für Backup und Restore verteilt sind, sollte die Wiederherstellung kritischer Komponenten der Plattform regelmässig und bereichsübergreifend geübt werden.

Es ist zielführend Gelegenheiten wie Umzüge oder der Aufbau der Plattform in weiteren Rechenzentren zu nutzen um den gewählten Backup- und Recovery Ansatz zu üben. Da das ISC-EJPD daran ist die Restore Tests zu erweitern und zu dokumentieren verzichtet die EFK auf eine Empfehlung.

2.4 Die Kontrolle der Vorgaben sollte verbessert werden

Die Verantwortung für die Sicherheit (Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit) wird zwischen Leistungserbringer (LE) und LB geteilt. Die Aufteilung der Verantwortlichkeiten zwischen LB und LE ist durch Vorgaben und Empfehlungen des ISC-EJPD technisch, organisatorisch und architektonisch geregelt. Die Systemarchitektur und architektonische Abweichungen werden heute vom Architektur Board ISC-EJPD (ABI) und dem Architektur Board Departement EJPD (ABD) geprüft, bewertet und bewilligt, dies für den heutigen Workload welcher auf der SPC betrieben wird. Wo möglich, werden die Vorgaben technisch und organisatorisch durchgesetzt.

Bei Abweichungen von Vorgaben oder Manipulationen an der Konfiguration wird der Bereich Cloud Plattformen in definierten Fällen alarmiert. Die Umsetzung der Vorgaben kann aufgrund der Architektur und der geteilten Verantwortung vom ISC-EJPD nicht in allen Fällen überprüft werden. Grund dafür ist, dass der LE keinen Einblick in die in den Containern laufenden Fachanwendungen, den sogenannten Workloads der LB hat, oder entsprechende Werkzeuge noch nicht vorhanden sind. Über den aktuellen Stand hinausgehende Prüfungen (z.B. kontinuierliche Analyse der auf der Plattform ausgerollten Images) werden täglich auf Schwachstellen geprüft und im Self-Service Portal rapportiert.

BEURTEILUNG

Die Einhaltung der Vorgaben und Empfehlungen des ISC-EJPD durch die LB ist wichtig für den sicheren Betrieb der Plattform. So kann eine Schwachstelle in einer Workload zum Risiko für die ganze Plattform oder einer Fachanwendung werden. Um dieses Risiko zu mitigieren, werden unterschiedliche Massnahmen auf der Plattform angewendet (z.B. Isolierung auf unterschiedlichen Stufen, Einschränkung der Berechtigungen usw.). Eine systematische und regelmässige Auswertung der Einhaltung der Vorgaben ist ein Instrument, um die LB zu steuern und die durch Abweichungen entstehenden Risiken besser zu verstehen und zu mitigieren.

Aufgrund der gewählten Architektur bzw. Technologie kann die Einhaltung gewisser Vorgaben, insbesondere organisatorischer und architektonischer Natur, seitens LE jedoch nicht verifiziert werden. Wo möglich wird die Einhaltung technischer Vorgaben auf Ebene Plattform mit verschiedenen Mitteln durchgesetzt und überprüft. Eine regelmässige, automatisierte Überprüfung und Berichterstattung zur Compliance der Workloads mit den ISC-EJPD-eigenen Vorgaben findet zum Prüfzeitpunkt nicht statt. Weiterführende Security- Compliance und Reporting-Werkzeuge, welche solche Funktionen potenziell bereitstellen könnten, werden evaluiert.

EMPFEHLUNG 3 — PRIORITÄT 2

Die EFK empfiehlt dem ISC-EJPD, die Einhaltung der architektonischen, organisatorischen und insbesondere technischen Vorgaben für den Betrieb der Fachanwendungen auf der SPC durch die LB zu überwachen und regelmässig auszuwerten.

STELLUNGNAHME DES ISC-EJPD

Die Empfehlung ist akzeptiert.

Das ISC-EJPD setzt bereits heute umfassende Massnahmen um. Die Systemarchitektur und mögliche Abweichungen werden durch das Architektur Board ISC-EJPD (ABI) und das Architektur Board Departement EJPD (ABD) geprüft, bewertet und bei Konformität bewilligt. Diese Prozesse sichern den kontrollierten Betrieb der Workloads auf der Secure Private Cloud (SPC).

Die Sicherheitsvorgaben des ISC-EJPD gelten bereits heute für alle Kunden, auch departementsfremde. Um Abweichungen künftig noch besser zu erkennen, ist der Einsatz von "Runtime Security

Tools" geplant. Diese sollen Abweichungen zentral dokumentieren und melden, um frühzeitig den Dialog mit betroffenen Kunden zu ermöglichen.

Mit diesen Massnahmen sieht sich das ISC-EJPD gut aufgestellt, um die Empfehlungen der EFK umzusetzen und den sicheren Betrieb der Fachanwendungen zu gewährleisten.

2.5 Voraussetzungen zum Betrieb von externen Fachanwendungen müssen geschärft werden

Das ISC-EJPD erbringt bereits heute Leistungen für LB ausserhalb des EJPD. Entsprechend sind die zugehörigen Prozesse vorhanden und müssen nicht von Grund auf neu definiert werden. Zum Zeitpunkt der Prüfung läuft ein Pilot mit einem externen LB in einem separaten Cluster auf dem Tenant des ISC-EJPD. Künftig sollen Anwendungen externer LB auf einem separaten Tenant betrieben werden.

Verschiedene Implementierungsdetails der CSB Rolle sind jedoch noch nicht hinreichend definiert. Ein entsprechendes Konzept soll 2024 erarbeitet werden. Um die Rolle weiter zu schärfen hat das ISC-EJPD zusätzliche Stellen geschaffen und ist daran diese zu besetzen.

BEURTEILUNG

Aus technologischer Sicht ist die SPC gut skalierbar, die verwendeten Technologien sind zweckmässig gewählt und die Redundanz zwischen den Rechenzentren sorgt für zusätzliche Flexibilität. Implementierungsdetails für die Aufnahme weiterer externer LB sind jedoch noch nicht hinreichend definiert, was zu Missverständnissen oder nicht idealen Integrationen weiterer Fachanwendungen führen könnte. Im Hinblick auf die Einarbeitung von neuen Mitarbeitenden ist es sinnvoll, wenn möglichst konsistente und standardisierte Vorgaben zur Verfügung stehen.

EMPFEHLUNG 4 — PRIORITÄT 1

Die EFK empfiehlt dem ISC-EJPD, die Details der Cloud Service Broker Rolle nach Evaluation des aktuell laufenden Piloten festzulegen und zu dokumentieren, so dass die Integration künftiger externer Leistungsbezüger vereinfacht wird.

STELLUNGNAHME DES ISC-EJPD

Die Empfehlung ist akzeptiert.

Die Arbeiten sind im Gang, Erkenntnisse aus dem Piloten fliessen in die Konzeption der CSB-Services (Cloud Service Broker) für externe Kunden ein, für welche das ISC-EJPD bereits eine externe Firma beauftragt hat.

Ziel ist es, durch ein klar definiertes CSB-Konzept die Rahmenbedingungen und Voraussetzungen für die professionelle Bereitstellung dieser Services zu schaffen und die Integration externer Leistungsbezüger zu vereinfachen. Mit diesem Ansatz wird eine fundierte Grundlage für die zukünftige Nutzung und Weiterentwicklung der CSB-Services geschaffen.

2.6 Security Monitoring sollte zentral aufgesetzt werden

Das Logging und Monitoring erfolgen mittels unterschiedlicher Mechanismen und mehrheitlich innerhalb des Plattform-Betriebs. Gewisse sicherheitsrelevante Logs werden an einen zentralen, bereichs-

übergreifenden Log-Sammler weitergeleitet. Der Umfang der Informationen ist jedoch aufgrund lizenztechnischer und konzeptioneller Limitierungen eingeschränkt und folgt aktuell keinem übergreifenden Konzept für Security-Monitoring.

Für 2025 ist vorerst die Konzeption eines Security Operations Centers (SOC) mit Hilfe eines externen Dienstleisters vorgesehen. Der Betrieb soll im Verlauf des Jahres 2026 aufgenommen werden.

BEURTEILUNG

Logging und Monitoringinformationen bzgl. der Plattform werden gesammelt und sind für das Plattform-Team für Auswertungen zugänglich. Für die Fehlersuche reicht dies aus. Da die Logs noch nicht systematisch korreliert und analysiert werden, besteht die Möglichkeit, dass fortgeschrittene Angriffe oder auch Angriffe über die Lieferkette auf die Plattform unentdeckt bleiben. Die Konzeption und Implementierung eines SOC im ISC-EJPD ist ein geeigneter Ansatz um ein wirksames Security-Monitoring aufzubauen.

Der Aufwand für die Produktivsetzung und Feinjustierung eines SOC ist dabei nicht zu unterschätzen und sollte, damit der Ansatz seine volle Leistungsfähigkeit entfalten kann, über einen grösseren Zeitpunkt hinweg laufend verbessert und mittels simulierter Angriffe getestet werden.

Auf Grund einer offenen Empfehlung[1] an das SEPOS zum Ausbau der Überwachungs- und Reaktionsfähigkeit durch verbesserte Kollaboration und Nutzung von Werkzeugen sollte sich das ISC-EJPD mit ihnen diesbezüglich austauschen.

Der Einbezug eines externen Dienstleisters ist aus Sicht EFK sinnvoll.

EMPFEHLUNG 5 — PRIORITÄT 2

Die EFK empfiehlt dem ISC-EJPD, den Aufbau eines zentralen Security Monitorings in Absprache mit dem SEPOS zu forcieren.

STELLUNGNAHME DES ISC-EJPD

Die Empfehlung ist akzeptiert.

Cybersicherheit ist für das ISC-EJPD eine prioritäre Herausforderung. Im Rahmen des Jahresziels „Ausbau Sicherheit“ werden 2025 die Machbarkeit und die Anforderungen für die Implementierung eines zentralen Security Operations Centers (SOC) geprüft.

Das SOC soll als zentrale Einheit sicherstellen, dass IT-Services effektiv vor Gefahren geschützt werden. Ein zentralisiertes Security Monitoring ist dabei wesentlich, um Sicherheitsvorfälle frühzeitig zu erkennen, zu analysieren und abzuwehren.

Das ISC-EJPD strebt eine Stärkung der Resilienz und eine nachhaltige Verbesserung der Wahrnehmung der Cybersicherheitsmassnahmen innerhalb der Organisation an und wird die Konzeption sowie die Umsetzungsoptionen für ein SOC vorantreiben. Dazu erfolgen situativ Absprachen mit SEPOS.

2.7 Die IT-Security Auditplanung sollte verfeinert werden

Im Rahmen von externen, technischen Audits wird die Infrastruktur Konfigurationsreviews und Penetrationstests unterzogen. Der letzte externe Audit fand im Mai 2024 statt, der vorangehende war im 2020.

[1] «Querschnittsprüfung der Erkennung von Sicherheitsvorfällen» (PA 23703), Empfehlung 2

Im Dokument «Secure Private Cloud EJPD – Security Whitepaper» wurde eine Prüfung «in regelmässigen Abständen (mind. alle drei Jahre)» definiert. In den Interviews wurde erwähnt das es angedacht ist, solche technischen Prüfungen im Zweijahresrhythmus durchführen zu lassen.

Zudem führt das ISC-EJPD weitere IT-Security Prüfungen auf anderen Plattformen und Umsystemen durch. Eine dokumentierte Auditplanung ist zum Zeitpunkt der Prüfung nicht vorhanden.

BEURTEILUNG

Der angedachte Zweijahresrhythmus erscheint angemessen um sicherzustellen, dass Schwachstellen oder Fehlkonfigurationen nicht über längere Zeit hinweg unentdeckt bleiben. Die technische Auditierung der Plattform sollte daher wie angedacht umgesetzt und der Prüffokus längerfristig definiert werden. Zudem sollte bei grösseren Änderungen verifiziert werden ob zusätzliche Tests nötig sind.

Da das ISC-EJPD nicht nur die SPC testen lässt, sollte die Planung der Audits abteilungsübergreifend abgestimmt werden.

EMPFEHLUNG 6 — PRIORITÄT 2

Die EFK empfiehlt dem ISC-EJPD, eine verbindliche Planung für IT-Security Audits mit Einbezug aller Systeme zu erstellen und Audits im Zweijahresrhythmus oder nach grösseren Änderungen durchzuführen. Durch eine vorausschauende Planung soll sichergestellt werden, dass alle wesentlichen Risiken abgedeckt werden.

STELLUNGNAHME DES DES ISC-EJPD

Die Empfehlung ist akzeptiert.

Im Rahmen der angestrebten ISO 27001-Zertifizierung, welche das ISC-EJPD bis Ende 2024 erreichen möchte, wird der zentralen IT-Security Audit-Planung besondere Beachtung geschenkt. Diese Planung wird künftig zentral koordiniert, um eine konsistente und umfassende Abdeckung der wesentlichen Risiken sicherzustellen.

Die vorgeschlagene vorausschauende Planung wird integraler Bestandteil des Informationssicherheitsmanagementsystems (ISMS) und trägt dazu bei, die Sicherheit der Systeme und Daten kontinuierlich zu überprüfen und zu stärken. Durch die regelmässige und systematische Durchführung von Audits (Zweijahresrhythmus) wird nicht nur die Einhaltung regulatorischer und sicherheitsrelevanter Anforderungen gewährleistet, sondern auch ein Beitrag zur kontinuierlichen Verbesserung der IT-Sicherheitsmassnahmen geleistet.

2.8 Das Lifecycle Management wird konsequent umgesetzt

Die SPC basiert auf etablierten und weitverbreiteten Open Source Lösungen. Ein für den Betrieb und insbesondere die Orchestrierung der Plattform zentraler, zusätzlicher Technologielayer stammt aktuell primär von VMware. Das ISC-EJPD verfolgt eine Multivendor-Strategie auf mehreren Ebenen und evaluiert laufend Alternativen (um Abhängigkeiten zu einzelnen Lieferanten möglichst gering zu halten. Dies hat sich in der Vergangenheit bewährt. Für notwendige technische Unterstützung besteht ein Supportvertrag mit VMWare.

Der technologische Lifecycle der Plattform wird vom Cloud Plattform Team sichergestellt und VMWare ist im Rahmen des obenerwähnten Supportvertrags beratend involviert. Regelmässige Upgrades der Komponenten sind in die Jahresziele des Teams integriert. Upgrades können auch durch neu

bekanntgewordene Schwachstellen getrieben sein. Schwachstellen werden aus verschiedenen Quellen an das ISC-EJPD gemeldet.

BEURTEILUNG

Die Multivendorstrategie verhindert eine vollständige Abhängigkeit von einem Lieferanten und hat sich in der Vergangenheit bewährt. Der Lifecycle der SPC ist vom Bereich «Cloud Plattformen» umfassend gesteuert und der Support des Herstellers der Orchestrierungslösung geregelt.

3 UMSETZUNG FRÜHERER EMPFEHLUNG

Im Rahmen dieser Prüfung wurde eine vom Geprüften als umgesetzt gemeldete Empfehlung nachgeprüft.

3.1 Das Dokument «Bewältigung von Cybervorfällen im EJPD» wurde erstellt

Bei der Prüfung der Sicherheit der Datenbank INFOSTAR[1] wurde folgende Empfehlung ausgesprochen:

«Die EFK empfiehlt dem ISC-EJPD, die Operationalisierung der Verfahren zur Behandlung von Cybervorfällen zu verstärken, indem die Leistungsbezüger (BJ, Kantone) vermehrt in die detaillierte Definition der Schritte und Entscheidungskompetenzen, die für die Notfallmassnahmen zuständig sind, einbezogen werden. Das ISC-EJPD soll auch dafür sorgen, dass die Zweckmässigkeit der Definition von Reaktionsmodellen für die häufigsten Arten von Vorfällen erneut analysiert wird.» (21135.004).

Bei der Stellungnahme zur Umsetzung hat das ISC-EJPD folgendes gemeldet:

«Die bestehende und funktionierende Praxis ist in einem Dokument zusammengefasst und der Abteilung Kunden übergeben zur Kommunikation an die LB. Mit dieser Massnahme wird das bereits existierende und in der Praxis bewährte Vorgehen für alle einsehbar und abrufbar.»

Bei der Nachprüfung hat sich gezeigt, dass ein Dokument vorliegt welches auf die in der Empfehlung beschriebenen Elemente eingeht. Dieses wurde den ISBOs der LB per Mail zur Verfügung gestellt.

BEURTEILUNG

Das Dokument wurde erstellt und den ISBO zur Verfügung gestellt. Die Empfehlung 21135.004 kann geschlossen werden.

[1] «Prüfung Sicherheit der Datenbank INFOSTAR» (PA 21135) auf der Webseite der EFK abrufbar

ANHANG 1 – RECHTSGRUNDLAGEN UND RECHTSTEXTE

Bundesgesetz über die Eidgenössische Finanzkontrolle (Finanzkontrollgesetz, FKG) vom 28. Juni 1967 (Stand am 1. Januar 2018), SR 614.0
Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG), SR128 vom 18. Dezember 2020 (Stand am 1. Januar 2024)
Verordnung über die Informationssicherheit in der Bundesverwaltung und der Armee (Informationssicherheits-verordnung, ISV), SR 128.1 vom 8. November 2023 (Stand am 1. Juli 2024)
Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG), SR235.1 vom 25. September 2020 (1. September 2023)

VORGABEN

AR010 – Cloud-Prinzipien der Bundesverwaltung
SB020 – Cloud-Strategie der Bundesverwaltung
Si001 – IKT-Grundschutz in der Bundesverwaltung (Version 5.0)
SD125 Servicespezifikation SSO-Portal
Public Clouds Bund (https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/bundesarchi-tektur/cloud/public-clouds-bund.html)

ANHANG 2 – ABKÜRZUNGEN

CI/CD	Continuous Integration / Continuous Deployment (siehe Glossar)
CIS	Center for Internet Security
CSB	Cloud Service Broker (siehe Glossar)
DNS	Domain name System (siehe Glossar)
DTI	Bereich Digitale Transformation und IKT-Lenkung (der Bundeskanzlei)
EFK	Eidgenössische Finanzkontrolle
IaC	Infrastructure as Code (siehe Glossar)
IKT	Informations- und Kommunikationstechnologie
ISBO	Informatiksicherheitsbeauftragte/n der Organisationseinheit
ISC-EJPD	Informatik Service Center – Eidgenössisches Justiz- und Polizeidepartement
LB	Leistungsbezüger
LE	Leistungserbringer
PaaS	Plattform as a Service (siehe Glossar)
SEPOS	Staatssekretariat für Sicherheitspolitik
SLA	Service Level Agreement
SOC	Security Operations Center
SPC	Secure Private Cloud
SSO	Single-Sign-On (-Portal)

ANHANG 3 – GLOSSAR

Cloud-native	Bezeichnet eine Methode der Softwareentwicklung, bei der Anwendungen speziell für den Betrieb in Cloud-Umgebungen entworfen werden. Diese Anwendungen sind flexibel, skalierbar und in kleinere, unabhängige Teile (Microservices) zerlegt, die leicht aktualisiert und gewartet werden können. Durch den Einsatz moderner Technologien wie Containern und Automatisierung können cloud-native Anwendungen effizient betrieben werden und bieten eine hohe Verfügbarkeit sowie Resilienz gegenüber Ausfällen. Insgesamt ermöglicht der cloud-native Ansatz, die Vorteile der Cloud optimal zu nutzen und schnelle, kontinuierliche Verbesserungen zu erzielen.
Cloud Service Broker	Der CSB ist eine Art Vermittler respektive Integrator, der Unternehmen dabei hilft, die richtigen Cloud-Dienste (wie Speicher, Rechenleistung oder Software) für ihre Bedürfnisse auszuwählen, zu verwalten und zu nutzen.
Continuous Integration / Continuous Deployment	Methoden in der Softwareentwicklung, die dabei helfen, Software schneller und zuverlässiger zu entwickeln und bereitzustellen.
DNS	„Telefonbuch“ des Internets. Es übersetzt Webadressen (wie www.google.com) in IP-Adressen, welche Computer verstehen, damit sie die richtige Website finden können. Ohne DNS müsste man sich die komplizierten IP-Adressen der Websites merken.
Container Registry	Speicherort, in dem Container-Images aufbewahrt werden.
ESXi	Software von VMware, die es ermöglicht, mehrere „Computer“ (virtuelle Maschinen) auf einem einzigen echten Computer (Server) laufen zu lassen.
Full-Stack	Fähigkeit, sowohl die Vorderseite (Frontend) als auch die Rückseite (Backend) einer Anwendung oder Webseite zu entwickeln. Ein Full-Stack-Entwickler kann beide Seiten einer Anwendung entwickeln und versteht, wie sie zusammenarbeiten. Er ist in der Lage, eine komplette Anwendung von Grund auf zu erstellen – von der Benutzeroberfläche bis zur Datenbank und allem dazwischen.
GitOps	Methode zur Verwaltung und Automatisierung der IT-Infrastruktur und Anwendungen mithilfe von Git, einem Versionskontrollsystem, das normalerweise für die Softwareentwicklung verwendet wird. Das ISC-EJPD hat eine eigene Instanz welche von ihnen selber betrieben wird im Einsatz.
Infrastructure-as-Code	Ein Ansatz, bei dem die IT-Infrastruktur (wie Server, Netzwerke und Datenbanken) durch Code bereitgestellt wird anstatt durch dedizierte physische Komponenten mit manuellen Konfigurationen. Mit IaC werden Infrastrukturumgebungen definiert und automatisiert bereitgestellt, aktualisiert und gewartet, ähnlich wie Software-Code. Dies ermöglicht schnelle, konsistente und wiederholbare Bereitstellungen, erhöht die Skalierbarkeit und reduziert menschliche Fehler.
Kubernetes	Open-Source-System, das dabei hilft, Anwendungen, die in sogenannten Containern laufen, automatisch bereitzustellen, zu verwalten und zu skalieren.
Orchestrierung	Prozess der automatisierten Verwaltung, Koordination und Überwachung von komplexen IT-Systemen, Diensten und Anwendungen
Plattform-as-a-Service	Stellt Entwicklungswerkzeuge, Datenbanken und Laufzeitumgebungen bereit, wodurch der Fokus auf die Entwicklung und Innovation der Software gelegt werden kann, während die Cloud-Anbieter die Verwaltung und Wartung der Infrastruktur übernehmen.

Workloads	In Cloud-Systemen sind Workloads die Aufgaben oder Prozesse, die Anwendungen ausführen, wie z. B. Daten verarbeiten oder speichern. Sie werden je nach Bedarf flexibel auf verschiedenen Servern betrieben und skaliert um Leistung, Kosten und Verfügbarkeit zu optimieren.

ANHANG 4 – CLOUD-STUFEN DER BUNDESVERWALTUNG

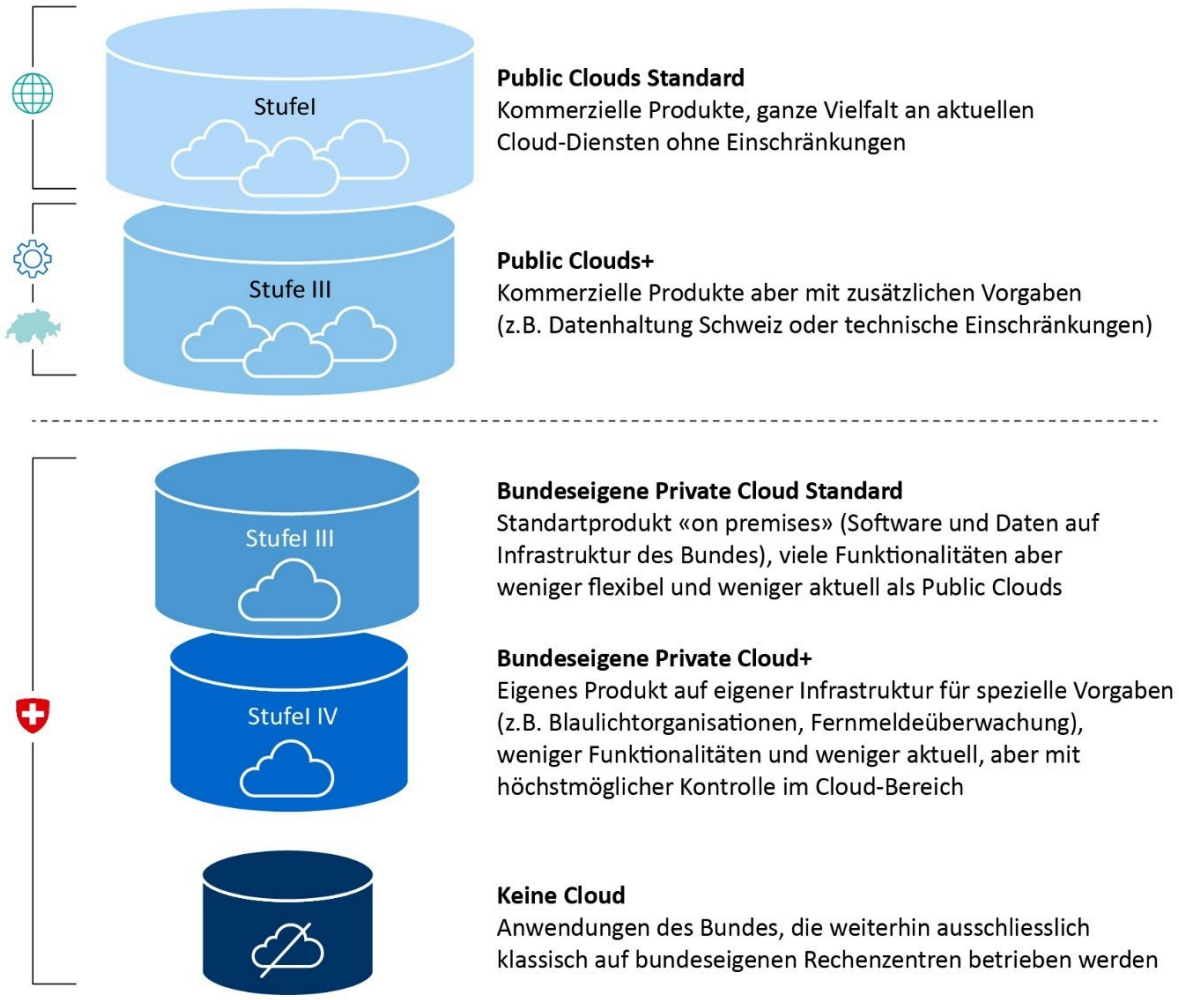


Abbildung 3 Cloud-Stufen der Bundesverwaltung, Quelle: Bundeskanzlei, Darstellung EFK