# Prüfung der Sicherheit und Verfügbarkeit im Betrieb GEVER

## Bundeskanzlei und Information Service Center des Eidgenössischen Departements für Wirtschaft, Bildung und Forschung

## Das Wesentliche in Kürze

Die Bundeskanzlei (BK) möchte mit dem Programm GENOVA ein einheitliches elektronisches Geschäftsverwaltungsprodukt (GEVER) für die gesamte Bundesverwaltung einführen. Die Einführung des auf über 68 Millionen Franken veranschlagten Programms ist zwischen November 2015 und September 2021 geplant. Das Information Service Center des Eidgenössischen Departements für Wirtschaft, Bildung und Forschung (ISCeco) trägt für den Betrieb der Plattform die Hauptverantwortung. Im Herbst 2020 arbeiten über 22 000 Benutzer mit dem neuen System.

Die Eidgenössische Finanzkontrolle (EFK) evaluiert im Rahmen dieser Prüfung, ob die umgesetzten betrieblichen Massnahmen unter dem Aspekt der Sicherheit und der Verfügbarkeit angemessen sind. Sie prüft auch, ob der Übergang vom Projekt- zum Betriebsstatus geregelt und die Weiterverfolgung offener Fragen sichergestellt ist. Schliesslich führt sie eine Nachprüfung der Umsetzung von vier Empfehlungen aus früheren Revisionen durch.

Die EFK ist zum Schluss gekommen, dass das Ergebnis insgesamt zufriedenstellend ist, obwohl die komplexe Systemarchitektur hohe Anforderungen an den Betrieb stellt und noch viel zu tun ist.

**Die Sicherheitsanforderungen sind definiert, aber der Prozess ist nicht vollständig abgeschlossen**

Die Systemarchitektur ist komplex, da mehrere Akteure am Betrieb beteiligt sind. Ihre Befugnisse sind klar definiert und die Zusammenarbeit wird von ihnen als zufriedenstellend bezeichnet. Die Stellen konnten mit Fachleuten besetzt werden, der Betrieb kann als stabil angesehen werden, die Anzahl an Störungen nimmt ab. Die Führungs-, Planungs- und Betriebsprozesse werden im Rahmen des ISCeco definiert. Eine erste interne Prüfung des Betriebs wurde durchgeführt, weitere sind geplant. Aus Sicht der EFK sind die Definitionen der Organisation, der Führung und der Betriebsprozesse angemessen. Die Sicherheitsanforderungen an die technische Lösung und den Betrieb sind dokumentiert. Die Restrisiken sind erkannt und akzeptiert. Die EFK hat allerdings festgestellt, dass die Umsetzung des Basisschutzes nicht vollständig dokumentiert ist.

Seitens der Leistungsbezüger hat die EFK keine vertiefte Prüfung des Status der Sicherheitsmassnahmen vorgenommen. Sie stiess jedoch auf einen Fall, bei dem die Aufgabenteilung zwischen dem Departement und den Ämtern nicht klar geregelt war. Die EFK fordert weitere Anstrengungen im Bereich Kommunikation.

**Zugriffs- und Integritätsschutz: Zweckmässige Mechanismen und punktueller Klärungsbedarf**

Die GEVER-Plattform befindet sich in der «Private Cloud» der Bundesverwaltung und ist im Bundesamt für Informatik und Telekommunikation (BIT) gehostet. Die Plattform wird innerhalb des geschützten Informatiknetzwerks des Bundes genutzt. Die Zwei-Faktor-Authentifizierung erfolgt über den IKT-Standarddienst eIAM[1]. Die Nutzer werden dem System ihres jeweiligen Departements zugewiesen und erhalten nur Zugriff auf die Geschäfte und Inhalte, für die sie zugangsberechtigt sind. Auf der Anwendungsebene und in technischer Hinsicht wird eine beschränkte Anzahl an Administratoren definiert. Die geschaffenen Mechanismen sind insgesamt angemessen. Die EFK hat jedoch festgestellt, dass die jährlichen Überprüfungen der Listen der privilegierten Nutzer noch nicht betriebsbereit sind.

Eine Lösung der Gruppe Verteidigung gewährleistet die Vertraulichkeit der Dokumente bis zur Stufe VERTRAULICH. Das Nutzungsreglement untersagt hingegen die Verarbeitung von Dokumenten der Stufe GEHEIM und das System blockiert die Definition eines Dokuments in dieser Klassifizierungskategorie. Das Risiko, schützenswerte Daten in den Metadaten zu erfassen, besteht und wird vom Auftraggeber anerkannt.

Der beim ISCeco eingeleitete Change-Management-Prozess legt die zu befolgenden Schritte angemessen fest (Antrag, Validierung, Ausführung, Tests). Die Änderungen werden jedoch nicht systematisch in allen Systemkomponenten erfasst. Die EFK konnte somit die Wirksamkeit des Change-Management-Prozesses nicht überprüfen. Die Serverintegrität wird regelmässig mit entsprechenden Tools kontrolliert. Auf der Plattform sind Hashmechanismen[2] verfügbar, sie werden aber noch nicht genutzt. Die EFK bat um Klärung dieses Punktes.

**Kontinuitätsmanagement: Der Prozess ist nicht vollständig abgeschlossen**

Um den erhöhten Anforderungen an die Systemverfügbarkeit gerecht zu werden, ist die Infrastruktur redundant in getrennten Rechenzentren ausgelegt. Die Tests haben ergeben, dass die Ausfallsicherung bei Störungsfällen funktionieren. Im ISCeco ist ein Überwachungssystem der Plattformkomponenten installiert, das Alarm auslöst und im Falle ernsthafter Störungen automatische Fehlertickets generiert. Diese werden nach den geltenden Verfahren bearbeitet. Die EFK weist darauf hin, dass manche Komponenten nicht der Kontrolle des ISCeco unterstehen. In solchen Fällen muss das ISCeco andere Leistungserbringer für die Problemlösung beiziehen.

Die EFK stellt hinsichtlich des Wiederherstellungsmanagements fest, dass gewisse Aspekte noch nicht dokumentiert werden. Es wurden zwar verschiedene Massnahmen definiert, regelmässige Backups und Wiederherstellungstests werden durchgeführt, doch es fehlt eine strukturierte Gesamtsicht in diesem Bereich («Policy»). Auch Ausfallszenarien, aktuelle Wiederherstellungspläne und umfassendere Wiederherstellungstests sind vorzubereiten.

**Der Übergang zur ständigen Organisation ist geregelt**

Für den Übergang zum Betriebsstatus wurden verschiedene Aktivitäten und Instanzen definiert. Arbeitsgruppen, die die verschiedenen betroffenen Akteure einbeziehen, befassen sich regelmässig mit Fragen rund um die Steuerung, die Führung und die Ausführung. Dies

[1] IKT-Standarddienst für das Zugriffs- und Berechtigungssystem, das vom ISB verwaltet wird.
[2] Verschlüsselungsfunktion, die zu Überprüfungszwecken verwendet wird.

erleichtert den Wissenstransfer. Pendenzenlisten werden auf diesen Ebenen geführt. Die EFK hält zwar diese Mechanismen für angemessen, rechnet aber mit gewissen Unsicherheiten im Zusammenhang mit der Übernahme der Funktionen des ISB durch die Bundeskanzlei ab Januar 2021.

Die bisherigen Empfehlungen der EFK sind weitgehend umgesetzt.

**Originaltext auf Französisch**