PRÜFUNG

Prüfung der Identitäts- und Zugriffsverwaltung eIAM

Bundeskanzlei – Bereich Digitale Transformation und IKT-Lenkung

DAS WESENTLICHE IN KÜRZE

Die Lösung eIAM (Electronic Identity and Access Management) des Bundesamts für Informatik und Telekommunikation (BIT) stellt die zentrale Authentifizierungsplattform für die gesamte Schweizer Bundesverwaltung dar. Sie dient der Verwaltung von digitalen Identitäten und Zugriffsrechten über alle angebundenen Webanwendungen und Dienste hinweg und soll eine sichere, effiziente und zentrale Authentifizierungslösung für die Bundesbehörden gewährleisten.

Per September 2024 nutzen täglich etwa 100 000 Benutzerinnen und Benutzer die eIAM-Lösung, um auf über 800 Anwendungen zuzugreifen, wobei täglich rund 250 000 Anmeldungen verarbeitet werden. Die jährlichen Betriebs- und Weiterentwicklungskosten der eIAM-Lösung betragen rund 20 Millionen Franken.

Die Führung des Standarddienstes ist zielführend aufgebaut und ermöglicht eine effektive Umsetzung der Aufgaben. Die Risiken im Zusammenhang mit der Abhängigkeit vom Schlüssellieferanten wurden adressiert und werden überwacht. Der Betrieb läuft stabil, Prozesse sind etabliert, und die Sicherheitsdokumente werden kontinuierlich aktualisiert. Zudem wurden seit der letzten Prüfung im Jahr 2018[1] beachtliche Fortschritte im Bereich der Virtualisierung sowie in der Verwaltung mehrerer Instanzen erzielt.

Verbesserungsbedarf besteht jedoch bei den Massnahmen zur Minderung der Risiken im Zusammenhang mit der Abhängigkeit von eIAM.

Die Tests zur Notfallumschaltung sollten erweitert werden

Das BIT hat die eIAM Lösung georedundant in zwei Rechenzentren (RZ) aufgebaut. Die erste Notfallumschaltung (Failover-Test), bei dem der eIAM-Kern vom RZ «Primus» auf «Campus» umgestellt wurde, verlief erfolgreich. Er zeigte jedoch auch unterschiedliche Probleme auf. Zur Optimierung wurden Lehren aus der Übung gezogen, insbesondere hinsichtlich der sofortigen Verfügbarkeit der Teams und der Automatisierung von Prozessen. Weitere technische Herausforderungen müssen vor einem erneuten vollständigen Failover-Test gelöst werden.

Im September 2024 hat das BIT entschieden, dass bei jedem Release ein Failover-Test der eIAM-Kernkomponenten auf der Referenzumgebung durchgeführt wird. Bei diesen Tests werden jedoch wichtige Komponenten ausgeschlossen. Diese Komponenten zu testen, würde wiederum den Einbezug weiterer Anwendungsteams erfordern. Die bewusste Ausklammerung der Komponenten aus den Tests birgt ein Risiko, da diese eine zentrale Rolle in der Authentifizierungs- und Zugriffskontrollstruktur des eIAM-Systems spielen. Ein Ausfall oder eine Fehlkonfiguration könnte gravierende Auswirkungen auf den Zugang zu kritischen Anwendungen haben. Daher sollten diese Komponenten auch in die Tests einbezogen werden.

Es fehlen Betriebslösungen beim Ausfall der Rechenzentren

Das BIT hat Notfall- und Neustartpläne erarbeitet für die RZ, in denen eIAM betrieben wird. Der Neustartplan für eIAM wird beim BIT unter der Leitung des Business Continuity Managements (BCM) geregelt und ist Teil des Programms zur Dienstkontinuität des BIT. Das BIT hat ein Dokument für den Neustart von eIAM formalisiert, das sich derzeit in der internen Validierung befindet und zunächst nur das RZ «Primus» in Bern betrifft. Die Umschaltung zum RZ «Campus» ist ebenfalls dokumentiert und wird unter der BCM-Leitung durchgeführt. Zum Prüfzeitpunkt gibt es jedoch keine konkreten Pläne für einen möglichen Ausfall beider RZ.

[1] «Prüfung von Führung und Betrieb des Standarddienstes «Identitäts- und Zugangsverwaltung» (PA 18502).

AGOV wird als erster grosser Anwendungsfall die E-ID als weiteres Identitätsnachweismittel für den Zugang auf Behördenanwendungen nutzen. Dadurch wird die zentrale Rolle von eIAM/AGOV im Identitätsmanagement des Bundes und der Schweizer Behörden weiter ausgebaut.