Prüfung der Sicherheit von CuriaPlus
Parlamentsdienste

Das Wesentliche in Kürze

Die Parlamentsdienste (PD) unterstützen die Bundesversammlung und ihre Organe bei der Erfüllung ihrer Aufgaben. Neben anderen Dienstleistungen stellen sie die Informatiksysteme und -anwendungen für die Bundesversammlung und die eigenen Mitarbeitenden bereit. Der Verwaltungsdelegation obliegt die oberste Leitung der PD. Mit einer 2018 angenommenen Motion beauftragte das Parlament die Verwaltungsdelegation, die Digitalisierung des Rats- und Kommissionsbetriebs voranzutreiben und den PD die dafür notwendigen Aufträge zu erteilen. Die beiden IT-Projekte CuriaPlus und Cervin (Parlnet) sind dafür von zentraler Bedeutung.

Bereits 2021 prüfte die Eidgenössische Finanzkontrolle (EFK) die Anwendung CuriaPlus, resp. Parlnet und die darunterliegende Plattform Liferay.[1] Dabei stellte sie diverse Mängel fest. Entsprechend hat die EFK die IT-Sicherheit vor der Inbetriebnahme von CuriaPlus erneut geprüft. Zudem überprüfte sie den Stand der Umsetzung früherer Empfehlungen.

Trotz positiver Entwicklungen bei der Governance und der Organisation bestehen bei beiden Projekten CuriaPlus und Parlnet noch Verbesserungspotenziale, insbesondere in den Bereichen Informatiksicherheit, Service Level Agreements (SLA) und Datensicherung.

Die Festlegung einer Governance und die Reorganisation der IT sind zielführend

Die Geschäftsleitung der PD hat im Oktober 2022 die Digitalisierungsstrategie der Parlamentsdienste in Kraft gesetzt. Anfang 2023 hat die Verwaltungsdelegation die «Weisung zur Gouvernanz in Bezug auf die digitalen Dienstleistungen» in Kraft gesetzt. In der Informatik führten die PD eine umfassende Reorganisation durch und stellten sich neu nach dem agilen Framework SAFe auf. Zusätzlich wurde das neue Ressort «Digitale Dienstleistungen» personell aufgestockt.

Künftige Entwicklungen wie das neue Informationssicherheitsgesetz oder mögliche Folgen einer Nutzung von Cloud-Diensten wurden proaktiv angegangen und der Verwaltungsdelegation vorgestellt.

Die Sicherheitsdokumente müssen überarbeitet und abgenommen werden

Die PD richten sich bei der Projektdurchführung nach den Vorgaben von SAFe. CuriaPlus wird noch nach HERMES geführt und nach Inbetriebnahme und formellem Abschluss nach den Vorgaben von SAFe weitergeführt. Entsprechend wurden auch eine Schutzbedarfsanalyse und ein Informationssicherheits- und Datenschutzkonzept erstellt. Es erfolgte jedoch keine formelle Abnahme dieser Dokumente.

[1] «Prüfung des Projektes CURIAplus» (PA 21310), abrufbar auf der Website der EFK.

Der IT-Grundschutz soll die minimalen organisatorischen, personellen und technischen Sicherheitsvorgaben im Bereich Informatiksicherheit für sämtliche Informatikmittel verbindlich festlegen, inkl. der zu ergreifenden Massnahmen. Bei den PD ist nicht klar geregelt, welche Standards für den Grundschutz beigezogen werden und welche Massnahmen vorgesehen sind.

Der Umfang der IT-Sicherheitstests soll erweitert werden

Für Parlnet und die Plattform Liferay wurden mehrere externe Sicherheitsprüfungen durchgeführt. Die Befunde daraus konnten noch nicht alle behoben werden. Zusätzlich wurde ein Quellcode-Review vorgenommen, bei dem keine kritischen Schwachstellen festgestellt wurden. Eine bereits in der letzten EFK-Prüfung geforderte Ausweitung des Testumfangs auf weitere verbundene Umsysteme wurde zudem nicht umgesetzt. Dies ist jedoch nötig, um eine ganzheitliche Sicht der IT-Sicherheit der PD zu erhalten.

Eine externe Sicherheitsprüfung von CuriaPlus im April 2023 konnte aufgrund von Neuinstallationen nicht vollständig durchgeführt werden. Die PD haben die Wiederholung der Tests für August 2023 in Auftrag gegeben, d. h. nach der im Juli erfolgenden Inbetriebnahme. Die Tests sollten gemäss Empfehlung der EFK auf die Umsysteme ausgeweitet werden.

Die SLA und Notfallkonzepte müssen definiert und aufeinander abgestimmt werden

Um im Störungsfall rasch reagieren zu können, müssen die Verantwortlichkeiten der verschiedenen Lieferanten geklärt und vertraglich in den SLA definiert werden. Sowohl für CuriaPlus als auch für Parlnet fehlen noch Notfallkonzepte. Ausserdem muss die Durchführbarkeit der Notfallmassnahmen regelmässig getestet werden.

Ausgelagerte Backups müssen erstellt und eine Georedundanz geprüft werden

Da die PD als kritische Infrastruktur eingestuft wurden, sollten sie eine Georedundanz mit zwei räumlich getrennten Rechenzentren prüfen. Im Minimum sollten die PD Offsite-Backups auf einem entfernten Server oder auf Medien ausserhalb des eigenen Rechenzentrumstandorts bereithalten.

Drei Empfehlungen aus der Prüfung von 2021 sind teilweise umgesetzt

Die PD haben eine weitere Sicherheitsprüfung und einen Code Review durchführen lassen. Der Umfang der Sicherheitsprüfung wurde jedoch nicht wie empfohlen erweitert.

Die geforderten Dokumente, Verträge und eine Risikoanalyse sind vorhanden, jedoch noch in Bearbeitung. Somit sind die Empfehlungen nur teilweise umgesetzt.