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

Prüfung der Sicherheit von CuriaPlus

Parlamentsdienste

EFK-23702 | inkl. Stellungnahmen | 14. September 2023

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	101.23702
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)

Inhaltsverzeichnis

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.

Audit de la sécurité de CuriaPlus
Services du Parlement

L'essentiel en bref

Les Services du Parlement (SP) assistent l'Assemblée fédérale et ses organes dans l'accomplissement de leurs tâches. Parmi d'autres services, ils mettent des systèmes et des applications informatiques à disposition de l'Assemblée fédérale et de son personnel. La Délégation administrative assume la direction suprême des SP. Dans une motion adoptée en 2018, le Parlement l'a chargée d'aller de l'avant avec la numérisation des activités des conseils et des commissions et de donner aux SP les mandats nécessaires à cette fin. Les deux projets informatiques CuriaPlus et Cervin (Parlnet) sont essentiels à cet égard.

En 2021 déjà, le Contrôle fédéral des finances (CDF) a examiné les applications CuriaPlus et Parlnet ainsi que la plateforme sous-jacente Liferay.[1] À cette occasion, il a relevé diverses lacunes. Par conséquent, le CDF a à nouveau examiné la sécurité informatique avant la mise en service de CuriaPlus. Il a en outre vérifié dans quelle mesure les précédentes recommandations ont été mises en œuvre.

Malgré des développements positifs en matière de gouvernance et d'organisation, les deux projets CuriaPlus et Parlnet présentent encore un potentiel d'amélioration, en particulier dans les domaines de la sécurité informatique, des accords de niveau de service (*Service Level Agreements*, SLA) et de la sécurité des données.

La mise en place d'une gouvernance et la réorganisation de l'informatique sont appropriées pour atteindre l'objectif visé

En octobre 2022, la direction des SP a mis en place la stratégie de numérisation des Services du Parlement. Au début de l'année 2023, la Délégation administrative a mis en vigueur une « Directive sur la gouvernance en matière de prestations numériques ». Dans le domaine de l'informatique, les SP ont procédé à une réorganisation complète et l'ont restructuré selon la méthode agile SAFe. En outre, les effectifs de la nouvelle unité « Prestations numériques » ont été augmentés.

Les développements futurs tels que la nouvelle loi sur la sécurité de l'information ou les conséquences possibles d'une utilisation de services en nuage ont été abordés de façon proactive et présentés à la Délégation administrative.

Les documents relatifs à la sécurité doivent être révisés et approuvés

Les SP se basent sur les directives de SAFe pour la mise en œuvre des projets. L'application CuriaPlus est toujours gérée conformément à HERMES et, une fois mise en service et achevée formellement, elle s'appuiera sur les directives de SAFe. Par conséquent, une analyse des besoins de protection a été effectuée et un concept de sécurité de l'information et de protection des données a été établi. Ces documents n'ont toutefois pas fait l'objet d'une acceptation formelle.

[1] « Audit du projet CURIAplus » (n° d'audit 21310), disponible sur le site Internet du CDF.

La protection informatique de base doit établir les exigences minimales de sécurité informatique à respecter concernant l'organisation, le personnel et la technique pour tous les moyens informatiques, y compris les mesures à prendre. Les SP n'ont pas clairement défini les normes à prendre en compte pour la protection de base, ni les mesures prévues.

Les tests de sécurité informatique doivent être étendus

L'application Parlnet et la plateforme Liferay ont été soumises à plusieurs tests de sécurité externes. Les failles constatées n'ont pas toutes pu être corrigées. De plus, une revue de code a été effectuée, lors de laquelle aucune faille critique n'a été détectée. Les tests n'ont en outre pas été étendus aux systèmes environnants connectés, comme cela avait été demandé dans le dernier audit du CDF. Cette extension est pourtant nécessaire pour obtenir une vue d'ensemble de la sécurité informatique des SP.

En avril 2023, il n'a pas été possible d'effectuer un examen externe complet de la sécurité de CuriaPlus en raison de nouvelles installations. Les SP ont demandé que les tests soient répétés en août 2023, soit après la mise en service qui a eu lieu en juillet. Les tests devraient être étendus aux systèmes environnants, conformément à la recommandation du CDF.

Les SLA et les plans d'urgence doivent être définis et harmonisés

Afin de pouvoir réagir rapidement en cas de perturbations, les responsabilités des différents fournisseurs doivent être clarifiées et définies contractuellement dans les SLA. Il n'existe aucun plan d'urgence pour CuriaPlus ni pour Parlnet. En outre, la faisabilité des mesures d'urgence doit être testée régulièrement.

Des sauvegardes hors-site doivent être établies et une géoredondance envisagée

Les SP étant considérés comme infrastructure critique, ils devraient envisager une géoredondance, soit le recours à deux centres de calcul situés à des endroits distincts. Au minimum, les SP devraient disposer de copies de sauvegarde hors-site sur un serveur éloigné ou sur des supports situés à un autre endroit que leur propre centre de calcul.

Trois recommandations de l'audit de 2021 ont été partiellement mises en œuvre

Les SP ont fait effectuer un nouvel audit de sécurité et une revue de code. Toutefois, la portée de cet examen n'a pas été étendue comme recommandé.

Les documents et les contrats demandés ainsi qu'une analyse des risques sont disponibles, mais en cours d'élaboration. Les recommandations ne sont donc que partiellement mises en œuvre.

Texte original en allemand

Verifica della sicurezza di CURIAplus
Servizi del Parlamento

L'essenziale in breve

I Servizi del Parlamento (SP) coadiuvano l'Assemblea federale e i suoi organi nell'adempimento dei loro compiti. Oltre a fornire altri servizi, essi predispongono le applicazioni e i sistemi d'informazione per l'Assemblea federale e per i propri collaboratori. La Delegazione amministrativa è incaricata della direzione suprema dei SP. In una mozione accolta nel 2018, il Parlamento ha incaricato la Delegazione amministrativa di accelerare il processo di digitalizzazione dell'attività delle Camere e delle commissioni e di attribuire ai SP i mandati necessari a tal fine. In quest'ambito, i due progetti informatici CURIAplus e Cervin (Parlnet) sono di centrale importanza.

Già nel 2021 il Controllo federale delle finanze (CDF) ha verificato l'applicazione CURIAplus, Parlnet e la piattaforma di base Liferay.[1] In quell'occasione il CDF aveva constato diverse lacune. Di conseguenza, prima della messa in funzione di CURIAplus ha riesaminato la sicurezza informatica. Ha inoltre verificato lo stato di attuazione delle raccomandazioni formulate in precedenza.

Malgrado alcuni progressi nell'ambito della governance e dell'organizzazione permangono potenziali di miglioramento per entrambi i progetti CURIAplus e Parlnet, in particolare nei settori della sicurezza informatica, dei Service Level Agreement (SLA) e del backup dei dati.

La definizione di una governance e la riorganizzazione informatica sono efficaci

Nel mese di ottobre 2022 la Direzione dei SP ha posto in vigore la strategia di digitalizzazione dei Servizi del Parlamento. All'inizio del 2023 la Delegazione amministrativa ha posto in vigore le istruzioni concernenti la governance in relazione ai servizi digitali (disponibili solo in tedesco e francese). Nel settore dell'informatica i SP hanno effettuato un'ampia riorganizzazione passando al framework agile SAFe. Inoltre è stato potenziato l'effettivo del nuovo Comparto servizi digitali.

Le tematiche degli sviluppi futuri, come la nuova legge sulla sicurezza delle informazioni, o delle possibili conseguenze di un utilizzo di servizi cloud sono state affrontate in maniera proattiva e presentate alla Delegazione amministrativa.

I documenti relativi alla sicurezza devono essere rielaborati e approvati

Per la realizzazione del progetto, i SP si basano sulle direttive del framework SAFe. CURIAplus viene ancora gestito in conformità a HERMES e, una volta effettuati la messa in funzione e il completamento formale, si fonderà sulle direttive applicate a SAFe. Di conseguenza sono stati predisposti anche un'analisi del bisogno di protezione nonché un piano per la sicurezza delle informazioni e la protezione dei dati. Tuttavia non vi è stata alcuna approvazione formale di questi documenti.

[1] «Verifica del progetto CURIAplus» (n. della verifica 21310), disponibile sul sito Internet del CDF.

La protezione IT di base deve stabilire in maniera vincolante i requisiti minimi in ambito di sicurezza informatica dal punto di vista organizzativo, tecnico e del personale per tutti i mezzi informatici, inclusi i provvedimenti da adottare. Nel caso dei SP, non è definito in modo chiaro quali standard vengano presi in considerazione per la protezione di base e quali provvedimenti siano previsti.

La portata dei test sulla sicurezza informatica deve essere ampliata

Sono state condotte diverse verifiche esterne sulla sicurezza inerenti a Parlnet e alla piattaforma Liferay. Per ora non è stato ancora possibile risolvere tutte le problematiche emerse. È stata inoltre eseguita una revisione del codice sorgente, dalla quale non è emersa alcuna vulnerabilità critica. L'ampliamento della portata dei test ad altri sistemi periferici collegati, richiesto già nell'ultima verifica del CDF, non è stato attuato. Tuttavia, ciò è necessario per ottenere una visione globale della sicurezza informatica dei SP.

A causa di nuove installazioni, nel mese di aprile del 2023 non è stato possibile condurre una verifica esterna completa sulla sicurezza. I SP hanno commissionato la nuova esecuzione dei test per il mese di agosto del 2023, ovvero dopo la messa in funzione avvenuta nel mese di luglio. Secondo la raccomandazione del CDF, i test dovrebbero essere estesi ai sistemi periferici.

I SLA e i piani di emergenza devono essere definiti e coordinati tra di loro

Per poter reagire rapidamente in caso di malfunzionamento, le responsabilità dei vari fornitori devono essere chiarite e definite contrattualmente nei SLA. Mancano ancora i piani di emergenza sia per CURIAplus che per Parlnet. Inoltre, l'attuabilità delle misure di emergenza deve essere verificata regolarmente.

Occorre creare i backup esternalizzati e verificare la georidondanza

Poiché i SP sono stati classificati come infrastruttura critica, essi dovrebbero verificare la georidondanza in due centri di calcolo fisicamente separati. I SP dovrebbero perlomeno mettere a disposizione backup offline su un server remoto o su supporti esterni al proprio centro di calcolo.

Tre raccomandazioni risalenti alla verifica del 2021 risultano parzialmente attuate

I SP hanno fatto eseguire un'altra verifica sulla sicurezza e una revisione del codice. Tuttavia, la portata di tale verifica non è stata estesa come consigliato.

I documenti richiesti, i contratti e l'analisi dei rischi sono disponibili, ma tuttora in fase di elaborazione. Pertanto, le raccomandazioni risultano attuate solo parzialmente.

Testo originale in tedesco

Audit of CuriaPlus security
Parliamentary Services

Key facts

Parliamentary Services (PS) support the Federal Assembly and its bodies in the fulfilment of their tasks. Among other services, they provide the IT systems and applications for the Federal Assembly and their own staff. The Administrative Delegation is responsible for the overall management of PS. In a motion adopted in 2018, Parliament instructed the Administrative Delegation to push ahead with the digitalisation of council and committee operations and to give PS the necessary mandates to do so. The two IT projects CuriaPlus and Cervin (Parlnet) are of central importance for this.

Back in 2021, the Swiss Federal Audit Office (SFAO) audited the CuriaPlus application and Parlnet, and the underlying Liferay platform.[1] It identified various deficiencies during the course of the audit. Accordingly, the SFAO audited IT security again before CuriaPlus went into operation. It also examined the status of implementation of previous recommendations.

Despite positive developments in terms of governance and organisation, there is still room for improvement in both the CuriaPlus and Parlnet projects, particularly in terms of IT security, service level agreements (SLAs) and data backup.

The establishment of governance and the reorganisation of IT have provided the desired results

In October 2022, PS management put the Parliamentary Services' digitalisation strategy into effect. At the beginning of 2023, the Administrative Delegation put into force the directive on governance for digital services. In terms of IT, PS carried out a comprehensive reorganisation and restructured themselves according to the agile SAFe framework. In addition, the new digital services department received additional staff.

Future developments such as the new Information Security Act or the possible consequences of using cloud services were proactively addressed and presented to the Administrative Delegation.

Security documents need to be revised and accepted

PS are following the SAFe guidelines for project implementation. CuriaPlus is still being managed according to HERMES and will continue to be managed according to SAFe specifications after commissioning and formal completion. Accordingly, a protection needs analysis and an information security and data protection concept were also prepared. However, these documents have not been formally accepted.

The basic IT protection is intended to define the minimum organisational, HR and technical security requirements in terms of IT security. This applies to all IT resources in a binding manner, including the measures to be taken. Within PS, it is not clearly regulated which standards are to be used for basic protection and which measures are planned.

[1] "Audit of the CURIAplus project" (audit mandate 21310), available on the SFAO website.

The scope of the IT security tests should be expanded

A number of external security tests were carried out on Parlnet and the Liferay platform. It has not yet been possible to resolve all of the findings from these. In addition, a source code review was conducted, which did not identify any critical vulnerabilities. Furthermore, there was no extension of the scope of testing to other connected peripheral systems, as requested in the last SFAO audit. This is necessary, however, to obtain a holistic view of PS' IT security.

An external security audit of CuriaPlus in April 2023 could not be fully carried out due to new installations. PS have requested that the tests be repeated in August 2023, i.e. after the installations have gone live in July. According to the SFAO's recommendation, the tests should be extended to include the peripheral systems.

The SLAs and emergency concepts must be defined and coordinated with each other

In order to be able to react quickly in the event of a fault, the responsibilities of the various suppliers must be clarified and contractually defined in the SLAs. Emergency concepts are still missing for both CuriaPlus and Parlnet. In addition, the emergency measures must be tested regularly to ensure they are feasible.

Outsourced backups must be created and geo-redundancy must be tested

Since PS are classified as critical infrastructure, they should consider geo-redundancy with two physically separated data centres. At the very least, PS should keep offsite backups on a remote server or on external media away from their own data centre location.

Three recommendations from the 2021 audit have been partially implemented

PS arranged a further security audit and a code review. However, the scope of the security audit was not expanded as recommended.

The required documents, contracts and risk analysis exist but are still being worked on. Therefore, the recommendations have been only partially implemented.

Original text in German

Generelle Stellungnahme des Parlamentsdienstes

Es ist erfreulich, dass die grundlegende Neuausrichtung der Informatik der Parlamentsdienste durch die Schaffung einer agilen digitalen Arbeitsorganisation, Festlegung der Digitalisierungsstrategie und Etablierung der Gouvernanz für die digitalen Dienstleistungen von der EFK inhaltlich als zielführend angesehen wird; zudem begrüsst sie ausdrücklich die proaktive Bearbeitung von künftigen Entwicklungen Inkrafttreten des ISG und Cloud-Thematik durch die Parlamentsdienste.

Bezüglich der Sicherheit der Anwendung CURIAplus sind die in der ersten Prüfung der EFK formulierten Befürchtungen nicht eingetreten. Die Empfehlungen der EFK aus der erneuten Prüfung beziehen sich einerseits auf formale Aspekte (Abnahme der entsprechenden Sicherheitsdokumente). Andererseits betont die EFK die Einstufung des Parlaments als kritische Infrastruktur und empfiehlt deshalb zusätzliche weitgehende und umfassende Sicherheitsmassnahmen (u.a. zentralisiertes Risikomanagement, zentralisiertes Schwachstellenmanagement, Durchführung von Sicherheitsprüfungen für CURIAplus und alle Umsysteme, georedundant ausgelegte Server-Infrastruktur).

Die Parlamentsdienste teilen die Einschätzung der EFK, dass mit der voranschreitenden Digitalisierung die Abhängigkeit der parlamentarischen Tätigkeit von IT-Systemen zunimmt. Sobald keine Alternativen mehr (primär in Form von Papierunterlagen) für die Parlamentsarbeit zur Verfügung stehen, führt der Ausfall von kritischen Anwendungen zu operativen Einschränkungen. Da dies heute noch nicht der Fall ist (mit Ausnahme der Abstimmungssysteme in den Ratssälen), verstehen die Parlamentsdienste die diesbezüglichen Empfehlungen der EFK als wertvolle Hinweise für eine künftige, rein digitale Arbeitsweise des Parlaments. In diesem Sinn sind die Parlamentsdienste mit allen Empfehlungen der EFK einverstanden und haben Massnahmen ergriffen, um diese so weit wie möglich umzusetzen. Angesichts des erheblichen Ressourcenbedarfs in personeller und finanzieller Hinsicht für die vollständige Umsetzung werden die Parlamentsdienste der Verwaltungsdelegation Optionen vorlegen, welche jeweils den zusätzlichen Nutzen und die finanziellen Auswirkungen aufzeigen.

Die Parlamentsdienste bedanken sich für die dieses Mal sehr professionelle Haltung der EFK während der Prüfung und die gute Zusammenarbeit.

Da der erste Prüfbericht zu CURIAplus (PA 21310) veröffentlicht wurde und medial auf Interesse stiess, ersuchen die Parlamentsdienste die EFK, auch den vorliegenden Bericht zu veröffentlichen.

1 Auftrag und Vorgehen

1.1 Ausgangslage

Die Parlamentsdienste (PD) sind die Stabsstelle des Parlaments und unterstützen die Bundesversammlung bei der Erfüllung ihrer Aufgaben. Damit die Parlamentarier ihren verfassungsmässigen Aufgaben nachkommen können, stellen die Parlamentsdienste die notwendigen Mittel bereit, insbesondere auch Informatiklösungen und Prozesse. Die Aufsicht und oberste Leitung der Parlamentsdienste obliegt der Verwaltungsdelegation.

CuriaPlus und Cervin (Parlnet) sind zwei wichtige Informatikprojekte der PD. Mit beiden Vorhaben soll einerseits ein wesentlicher Schritt zur Digitalisierung realisiert, andererseits die Grundlage für nachfolgende Digitalisierungs-Vorhaben gelegt werden.

Die Prüfung des Projekts Curia Plus[2] im Jahr 2021 hat grundlegende Mängel in der Governance und der IT-Architektur der PD zu Tage gefördert. Im Projekt waren wesentliche Mängel bezüglich IT-Sicherheit nicht behoben. Mit Unterstützung einer externen Firma haben die PD 2021 verschiedene Massnahmen zur Optimierung der IT-Abläufe umgesetzt.

Im zweiten Quartal 2023 sollen die Abnahmetests erfolgen und CuriaPlus vor dem Wechsel der Legislatur in Betrieb gehen. Mit der Prüfung zur IT-Sicherheit soll beurteilt werden, ob die geplante Lösung sicher und zuverlässig betrieben werden kann. Aus der Prüfung 21310 sind Empfehlungen hervorgegangen, welche als umgesetzt gemeldet wurden und durch die EFK überprüft werden.

1.2 Prüfungsziel und -fragen

Das Prüfziel ist zu beurteilen, ob CuriaPlus im Gesamtumfeld der IT der Parlamentsdienste sicher und zuverlässig betrieben werden kann.

Die Prüffragen lauten:

1. Ist die Anwendung CuriaPlus so konzipiert und in die IT-Umgebung eingebettet, dass eine angemessene Sicherheit (Verfügbarkeit, Vertraulichkeit, Integrität) und Resilienz sichergestellt ist?
2. Ist eine lückenlose und permanente Überwachung der Infrastruktur am Perimeter und im inneren des Netzes sichergestellt und werden Auffälligkeiten zeitnah detektiert und bearbeitet?
3. Bestehen angemessene Massnahmen zur Erhaltung resp. Wiederherstellung der Verfügbarkeit bei Angriffen?
4. Sind die Empfehlungen aus der Prüfung 21310 umgesetzt?

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Christian Brunner (Revisionsleiter), Martin Scheid und mit Unterstützung einer externen Firma vom 17. April bis 2. Juni 2023 durchgeführt. Sie erfolgte unter der Federführung von Bernhard Hamberger. Der vorliegende Bericht berücksichtigt nicht die Entwicklung nach der Prüfungsdurchführung.

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

1.4 Unterlagen und Auskunftserteilung

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

1.5 Schlussbesprechung

Die Schlussbesprechung fand am 9. August 2023 statt. Teilgenommen haben von Seiten PD der Generalsekretär, der Bereichsleiter Infrastruktur + Sicherheit, der Leiter Digitale Plattformen + Lösungen sowie der Unternehmensarchitekt. Seitens EFK der Direktor, der zuständige Mandatsleiter, der zuständige Fachbereichsleiter und der Revisionsleiter.

Die EFK dankt für die gewährte Unterstützung und erinnert daran, dass die Überwachung der Empfehlungsumsetzung dem Generalsekretär der Parlamentsdienste und der Verwaltungsdelegation obliegt.

EIDGENÖSSISCHE FINANZKONTROLLE

2 Informationssicherheit bei CuriaPlus

Die PD führten 2021/22 in der Informatik eine umfassende Reorganisation durch und stellten sich neu in einer agilen Organisation auf. Diese orientiert sich am Scaled Agile Framework (SAFe). Das neue Ressort «Digitale Dienstleistungen» wurde personell aufgestockt. Die wichtigsten Rollen und Verantwortlichkeiten sind in der «Weisung zur Gouvernanz in Bezug auf die digitalen Dienstleistungen» und die Strategie in der «Digitalisierungsstrategie der Parlamentsdienste» formuliert und in Kraft gesetzt.

Zukünftige Änderungen wie z. B. die Auswirkungen des neuen Informationssicherheitsgesetzes (ISG) auf die PD oder mögliche Folgen der Nutzung von Clouddiensten wurden bereits analysiert und in der Verwaltungsdelegation behandelt.

Betreffend CuriaPlus sind noch diverse Verbesserungsmassnahmen offen, respektive müssen noch umgesetzt werden. Auf diese Punkte wird in den folgenden Kapiteln vertieft eingegangen.

2.1 Sicherheitsdokumentente müssen überarbeitet und abgenommen werden

Die PD richten sich inhaltlich nach SAFe. CuriaPlus wird noch nach der Projektmethode HERMES geführt, welche die erforderlichen Sicherheitsdokumentationen vorgibt. Die Schutzbedarfsanalyse (Schuban) sowie der Entwurf des Informationssicherheits- und Datenschutzkonzepts (ISDS) für CuriaPlus wurden erstellt. Zudem sind diese Dokumente auch für Parlnet und die unterliegende Liferay-Plattform erstellt worden.

Die Schuban von CuriaPlus ist nicht formell abgenommen. Gleich verhält es sich mit dem ISDS-Konzept von Parlnet. Dieses Dokument wird laufend angepasst, z. B. nach einer Anpassung der Firewall Regeln oder dem Beheben von Befunden aus den Sicherheitsprüfungen. Weitere zur Verfügung gestellte Dokumente von relevanten Umsystemen wie z. B. die Schuban des Projekts «Gottardo» lagen in einer abgenommenen und signierten Version vor.

Kein IT-Grundschutz Check vorhanden

Bei mehreren Interviews wurde von den Befragten festgehalten, dass der IT-Grundschutz eingehalten werde. Es konnte jedoch nicht eruiert werden an welche Vorgaben und Standards sich die PD konkret orientieren und wie sie deren Umsetzung prüfen. Dokumente mit dem Nachweis der Umsetzung waren nicht verfügbar. Die verschiedenen Lieferanten hatten gemäss ihren Aussagen auch verschiedene Standards wie ISO27001 oder OWASP Top-Ten angewendet, um einen Grundschutz sicherzustellen.

Beurteilung

Änderungen an Systemen in den ISDS-Konzepten zu erfassen ist grundsätzlich zweckdienlich. Die Dokumente sollten jedoch initial und nach Änderungen formell abgenommen werden. Dies stellt sicher, dass die aktuellste und gültige Version klar definiert ist und die Vorgaben umgesetzt werden. Zudem ist eine formelle Abnahme auch ein Element der Qualitätssicherung und kann Risiken aufdecken, welche das System gefährden könnten.

Der IT-Sicherheitsprozess sollte einheitlich auf sämtliche Systeme der PD angewendet werden.

Es ist nicht klar geregelt, an welchen Standards sich die PD bei der Festlegung des IT-Grundschutzes orientieren. Dies kann eine lückenhafte oder suboptimale Umsetzung desselben zur Folge haben. Die PD sollten einen etablierten Standard auswählen und für verbindlich erklären, damit für alle Anwendungen, ungeachtet des jeweiligen Lieferanten, derselbe Grundschutz umgesetzt wird. Dies fördert ein klar definiertes Minimalniveau der IT-Sicherheit und macht diese messbar. Die Umsetzung des Grundschutzes sollten dokumentiert und überwacht werden.

Der für die Bundesverwaltung definierte IT-Grundschutz gemäss Cyberrisikenverordnung (CyRV) ist für die PD rechtlich nicht verbindlich. Er wäre aber eine geeignete Vorgabe.

Empfehlung 1 (Priorität 1)

Die EFK empfiehlt den Parlamentsdiensten, ein einheitliches Sicherheitsverfahren zu implementieren. Darin sind sowohl die anzuwendenden Vorgaben klar zu definieren als auch die formellen Abnahmeverfahren.

Die Empfehlung ist akzeptiert.

Stellungnahme der PD

Die Parlamentsdienste erarbeiten zurzeit eine neue Grundlage für einheitliche Sicherheitsanforderungen. Als Basis dient das Dokument “Si001 IKT Grundschutz in der Bundesverwaltung” des NCSC. Die Inkraftsetzung ist für den Beginn des Jahres 2024 – auch unter Berücksichtigung der Anforderungen des neuen Informationssicherheitsgesetzes – vorgesehen.

2.2 Risiken werden nicht zentral verwaltet

Für die Erfassung der Risiken sowie deren Beurteilung und Einstufung sind gemäss «Weisung zur Gouvernanz in Bezug auf die digitalen Dienstleistungen» der Product Manager und der Product Owner verantwortlich. Diese teilen die Ergebnisse dem Business Owner mit und schlagen geeignete Massnahmen vor. Zusätzlich müssen sie auch den rechtzeitigen Einbezug des Informationssicherheitsbeauftragten (ISB) sicherstellen.

Für den Umgang mit (Rest-)Risiken der Stufe «Grundschutz» ist der IT-Ausschuss zuständig, über solche mit Stufe «hoher Schutz» und «sehr hoher Schutz» muss die Geschäftsleitung entscheiden.

Die (Rest)-Risiken werden in verschiedenen Systemen erfasst. Die Risiken werden danach entweder in den Protokollen des IT-Ausschusses, der Geschäftsleitungssitzungen oder in den ISDS Konzepten festgehalten. Es existiert ausserdem ein Information Security Management System (ISMS) in welchem auch Risiken erfasst und Massnahmen verfolgt werden. Für CuriaPlus werden die Risiken via Projektrisiken rapportiert und es ist geplant, diese nach der Inbetriebnahme in das Risikomanagement der Digitalen Dienstleistungen zu überführen.

Der ISB amtet zum Zeitpunkt der Prüfung auch als Risikomanager. Die Rolle eines Compliance Managers wurde in der Digitalisierungsstrategie festgelegt und die Stelle mittlerweile besetzt. Zum Zeitpunkt der Prüfung war die Person jedoch noch nicht bei den PD tätig.

Beurteilung

Grundsätzlich werden die Risiken erfasst und aus Sicht der Prüfer korrekt eingeschätzt. Die Genehmigung und Übernahme der Restrisiken ist auf den verschiedenen Stufen etabliert und wird gelebt. Eine Gesamtsicht aller Risiken fehlt jedoch. Eine regelmässige Prüfung des Risikomanagements auf Angemessenheit und Wirksamkeit findet nicht statt.

Ohne eine Gesamtsicht der Risiken besteht die Gefahr, dass bei der Bearbeitung durch unterschiedliche Stellen einzelne Risiken und Massnahmen nicht genügend zusammengeführt, behandelt und weitergemeldet werden.

Die Tatsache, dass die Rollen des ISB und des Risikomanagers derselben Person zugewiesen wurden, könnte zu einem Kapazitätsengpass führen. Die künftige Behandlung der Risiken durch den Compliance Manager ist zu prüfen.

Empfehlung 2 (Priorität 2)

Die EFK empfiehlt den Parlamentsdiensten, den Aufbau eines zentralen Risikomanagements zu prüfen und den Betrieb angemessen zu ressourcieren.

Die Empfehlung ist akzeptiert.

Stellungnahme der PD

Der Prozess Risikomanagement wird bereits zentral geführt. Neu werden auch die Risiken selbst zentral im Tool SMS@PD geführt. Das Risikomanagement ist beim Team integrale Sicherheit (Prozesseigner und Prozessverantwortlicher) angesiedelt. Das Team besteht aus drei Mitarbeitenden, die sich teilweise vertreten können. Als Compliance Manager amtiert der seit 1. Juni 2023 bei den PD tätige Jurist Digitalisierung / Compliance. Die geforderte Trennung der Rollen Informationssicherheitsbeauftragter und Risikomanager ist nur mit zusätzlichen Ressourcen umsetzbar.

2.3 Systemprüfungen müssen wiederholt und erweitert werden

Nach der Sicherheitsprüfung im Mai 2020 wurde Parlnet im Juni 2022 erneut einem IT-Sicherheitstest desselben Umfangs unterzogen. Danach konnten bis zum Prüfzeitpunkt aber noch nicht alle Befunde behoben werden. Zusätzlich wurde auch der Quell-Code von Parlnet und CuriaPlus geprüft. Dabei wurden keine kritischen Schwachstellen festgestellt.

Die PD haben mit Parlnet zudem an dem vom Nationalen Zentrum für Cybersicherheit (NCSC) durchgeführten Bug-Bounty-Pilotprojekt[3] vom Mai 2021 teilgenommen.

Die Sicherheitsprüfung von CuriaPlus muss wiederholt werden

Die Sicherheitsprüfung von CuriaPlus im April 2023 konnte nicht vollständig durchgeführt werden. Die Prüfung wurde durch zwei Neuinstallationen von CuriaPlus unterbrochen. Des Weiteren wurde sie auf einer Testumgebung durchgeführt, welche Abweichungen zur Produktivumgebung aufwies. Dabei wurden keine Befunde mit hohen oder kritischen Lücken entdeckt. Die PD haben sofort einen weiteren Test in Auftrag gegeben. Aus Ressourcengründen bei der externen Firma kann dieser jedoch erst im August, also nach dem Go live von CuriaPlus im Juli, durchgeführt werden.

[3] https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2022/bug-bounty-plattform.html.

Beurteilung

Eine IT-Sicherheitsprüfung, welche eine Anwendung isoliert betrachtet, zeigt ein wenig repräsentatives Bild zum Sicherheitsstand in einer Gesamtumgebung. Weitere Komponenten der Infrastruktur wie z. B. die Virtualisierung, das Backup und die Anbindung an die Umsysteme müssen auch im Fokus von IT-Sicherheitsprüfungen stehen. Für eine umfassende und vollständige Aussage zur Sicherheit muss daher eine Überprüfung unter Einbezug der Umsysteme erfolgen.

Der bei CuriaPlus durchgeführte Web Application Penetration Test ist wenig aussagekräftig, da er nicht wie vorgesehen durchgeführt werden konnte, und nach dem Test die Plattform neu installiert wurde. Der Auftrag zur Wiederholung des Tests ist sinnvoll und notwendig.

Mit einer ungenügend getesteten Applikation in Produktion zu gehen, birgt erhöhte Risiken. Allfällige später entdeckte Befunde müssten zwingend und rasch behoben werden können.

Aus Sicht der EFK sollte der Umfang der für August 2023 geplanten IT-Sicherheitsprüfung auf die Umsysteme erweitert werden.

Empfehlung 3 (Priorität 1)

Die EFK empfiehlt den Parlamentsdiensten, rasch eine umfassende Sicherheitsprüfung von Parlnet und CuriaPlus durchzuführen, welche auch die direkt verbundenen Umsysteme abdeckt.

Die Empfehlung ist akzeptiert.

Stellungnahme der PD

Die Wiederholung der bereits erfolgten Sicherheitsprüfung der Anwendung CURIAplus durch die externe Firma nach der Inbetriebnahme war schon vor der EFK-Prüfung vorgesehen und hat am 8.8.2023 begonnen.

Die Parlamentsdienste sind einverstanden, weitere Sicherheitsprüfungen in Umsystemen vorzunehmen. Wie umfassend diese sein sollen, wird auf der Basis einer Risikoanalyse entschieden, da der Aufwand einer alle Umsysteme umfassenden Sicherheitsprüfung wie sie die EFK empfiehlt ist, sehr hoch ist.

Zusätzlich zum bereits erteilten Mandat wurde die externe Firma beauftragt, die erwähnte Risikoanalyse vorzunehmen und darauf basierend eine Empfehlung abzugeben, welche Schnittstellen und/oder Umsysteme zusätzlich geprüft werden sollen.

Mit Blick auf eine künftige rein digitale Arbeitsweise des Parlaments sollen zuhanden der VD Optionen für künftige Sicherheitsprüfungen erarbeitet werden.

2.4 Kein übergeordnetes Monitoring vorhanden

Die Systeme von CuriaPlus sowie das Netzwerk werden von unterschiedlichen externen Partnern überwacht. Eine übergeordnete Monitoring-Strategie fehlt. Es ist daher nicht möglich, Korrelationen über die gesamte Servicelandschaft der PD zu sehen. Die PD haben dies erkannt und einen Antrag zur Durchführung eines Proof of Concept (POC) erstellt und genehmigt.

Identitätsübernahme wird überwacht

Als besonders kritisch wurde im Bericht 21310 die Möglichkeiten der Identitätsübernahme (impersonation) durch Administratoren der Liferay-Plattform bewertet. Dies ist eine Grundfunktionalität dieser Plattform und kann nicht einfach abgestellt werden. Durch ein spezifisches Monitoring wird neu bei einer Identitätsübernahme ein Alarm ausgelöst und der Vorgang wird protokolliert. Zudem haben nur die Administratoren des Betreibers von Liferay die Berechtigung, die Identitätsübernahme zu aktivieren. Es ist geplant, dass der ISB per Mail informiert wird, wenn eine Identitätsübernahme erfolgt.

Beurteilung

Die PD haben mit dem POC zur Einführung eines übergeordneten Monitorings Möglichkeiten zur besseren Störungserkennung und -behebung adressiert. Die Fähigkeit, zusammenhängende Ereignisse über diverse Netzwerke und Systeme hinweg zu erkennen, verbessert die Detektions-, sowie Reaktionsmöglichkeit unter anderem bei Cyberangriffen. Zudem ist es für die PD wichtig eine eigene Sicht auf alle Systeme zu haben.

Die Funktionalität der Identitätsübernahme birgt besondere Risken hinsichtlich der Integrität der Informationen. Die PD haben seit der letzten Prüfung Massnahmen ergriffen, um deren Einsatz zu entdecken. Die geplante Einführung der automatischen Alarmierung des ISB hilft potentielle Missbräuche rasch zu entdecken.

Da der POC bereits genehmigt wurde, verzichtet die EFK auf eine Empfehlung.

2.5 Ein übergeordnetes Schwachstellenmanagement fehlt

Die PD verfügen über verschiedene Quellen zur Identifizierung von Schwachstellen in ihren IT-Systemen. Zu diesen gehören insbesondere IT-Sicherheitsprüfungen durch externe Partner, ein Threat detection und response Service der Swisscom, Mitteilungen des NCSC und Security Advisories im Zusammenhang mit Liferay.

Es existiert jedoch kein übergeordnetes Schwachstellenmanagementsystem: Eine einheitliche Sicht auf Schwachstellen, deren Behebungsstand und auf die diesbezüglichen Verantwortlichkeiten zwischen den Lieferanten und den PD ist nicht vorhanden.

Beurteilung

Ein Schwachstellenmanagementsystem hilft bei der Behandlung von Schwachstellen und dient der Sicherstellung der Kommunikation zwischen Sicherheitsprüfern und den entsprechenden Ansprechgruppen. Ein solches System beinhaltet mindestens Prozesse, Rollen, Werkzeuge, Abstimmungsgremien und ein angemessenes Reporting. Dabei ist die Kommunikation für den Austausch zwischen Sicherheitstestern, Entwicklern, Betreibern und Nutzern ein Schlüsselaspekt für einen langfristig sicheren Betrieb. Wegen unterschiedlichen Verantwortlichkeiten im Betrieb sind auch die Schnittstellen, der Austausch und die Verantwortlichkeiten zu klären.

Empfehlung 4 (Priorität 2)

Die EFK empfiehlt den Parlamentsdiensten ein zentrales IT-Schwachstellenmanagement zu implementieren.

Die Empfehlung ist akzeptiert.

Stellungnahme der PD

Das Schwachstellenmanagement ist gestützt auf Risikoüberlegungen in wichtigen Teilbereichen bereits etabliert.

Systemmeldungen (Fehler, Störungen und weitere) werden in einem zentralen System gesammelt. Wichtige Sicherheits-Updates (Patchmanagement als Subdisziplin des Schwachstellenmanagements) werden, wenn immer möglich, automatisch installiert. Für die Liferay-Plattform (Parlnet und Intranet) wurde in enger Zusammenarbeit mit den Lieferanten ein Schwachstellenmanagement etabliert. Der Betrieb und die Überwachung des Netzwerkes der Parlamentsdienste wird durch Swisscom gewährleistet, welche über ein gut funktionierendes Schwachstellenmanagement verfügt.

Bei der Entwicklung neuer oder der Anpassung bestehender digitaler Produkte wird im Rahmen der Risikobeurteilung geprüft, ob und wie diese in das bestehende Schwachstellenmanagement aufgenommen werden sollen.

Ausserdem werden die digitalen Produkte externen Audits und Reviews unterzogen, welche ebenfalls dazu dienen, Schwachstellen rechtzeitig aufzudecken.

Mit Blick auf eine künftige rein digitale Arbeitsweise des Parlaments sollen zuhanden der VD Optionen für ein weitergehendes Schwachstellenmanagement erarbeitet werden, welche den finanziellen und personellen Ressourcenbedarf aufzeigen.

2.6 Die Verantwortlichkeiten im Lieferantenmanagement müssen geklärt werden

Die PD arbeiten an einem Grundlagenpapier zu den Anforderungen für künftige Dienstleistungsverträge mit externen Partnern. Das Dokument ist zum Prüfzeitpunkt noch nicht in einer finalen Version vorhanden. Die Verantwortlichkeiten der Lieferanten sind darin nicht beschrieben.

Organisatorische und prozessuale Themen für CuriaPlus in Bezug auf das Incident Management sind zwischen den Parlamentsdiensten und den Lieferanten noch nicht geklärt.

Beurteilung

Die PD arbeiten mit unterschiedlichen Lieferanten zusammen. Daher ist es wichtig, die Verantwortlichkeiten in den Vereinbarungen zu definieren. Da mehrere Parteien involviert sind, müssen die verschiedenen SLAs sorgfältig aufeinander abgestimmt sein.

Die Rollen und Verantwortlichkeiten aller beteiligten Parteien im Bereich Incident Management müssen detaillierter definiert und schriftlich festgehalten werden. Ein wirksames Zusammenspiel bei einem Vorfall muss vorgängig geübt werden. Ohne diese Vorbereitung kann die Reaktions- und Wiederherstellungszeit verzögert werden.

Empfehlung 5 (Priorität 1)

Die EFK empfiehlt den Parlamentsdiensten das Incident Management in den SLA zum Betrieb für Parlnet (inkl. Liferay) und CuriaPlus klar zu regeln. Die Verantwortlichkeiten zwischen den Lieferanten sind zu definieren und die Umsetzbarkeit von reaktiven Massnahmen zu testen.

Die Empfehlung ist akzeptiert.

Stellungnahme der PD

Im «Betriebskonzept Liferay Anwendungsportal» ist das Incident Management für Parlnet geregelt (Diagramm der Verantwortlichkeiten, Verantwortlichkeitsmatrix, Incident Management Prozess). Monitoring und Alarming bei Incidents als reaktive Massnahmen sind implementiert und getestet. Mit der Betreiberfirma des Portals (clavis IT) besteht ein entsprechendes SLA. Mit dem Lieferanten der Anwendung CURIAplus (ti&m) sind noch die Betriebs-Vereinbarungen abzuschliessen. Ein Test- und Notfallkonzept mit allen Beteiligten ist in Erarbeitung.

2.7 Fehlende Georedundanz und fehlende Offsite Backups können zu Betriebsunterbrüchen und Datenverlust führen

Die Systeme für CuriaPlus werden in den beiden nahe beieinanderliegenden Rechenzentren (RZ) der PD betrieben. Die Datensicherungen befinden sich ebenfalls in diesen RZ. Die gesicherten Daten werden nicht an einem entfernten Standort gelagert.

Um die Folgen eines Ransomware-Angriffs zu minimieren, wurden erste Gespräche mit dem Bundesamt für Informatik und Telekommunikation (BIT) geführt, um abzuklären, welche Möglichkeiten es für ein ausgelagertes Backup geben könnte.

Beurteilung

Gemäss der Nationalen Strategie zum Schutz kritischer Infrastrukturen 2018 – 2022 vom 8. Dezember 2017 gehört das Parlament zu den kritischen Infrastrukturen. Die PD müssen vorbereitet sein, ihre Dienstleistungen auch in ausserordentlichen Situationen zur Verfügung zu stellen.

Ein Grossereignis im Raum Bern kann die Verfügbarkeit von CuriaPlus beinträchtigen. Bei einem Ausfall der beiden RZ gibt es kein Ausweichsystem und kein weiteres Backup der Daten.

Ohne Ausweichstandort und Auslagerung von Datensicherungen an einem weiter entfernten Standort, ist der Weiterbetrieb oder die Wiederherstellung nach einem grossen Ereignisfall sehr zeitintensiv, wenn nicht unmöglich. Die Auslagerung der Datensicherungen – nach Möglichkeit als Offline Kopie – kann auch nach einem Angriff mit einer Verschlüsselungssoftware hilfreich sein. Die Datensicherung muss mittels regelmässigen Wiederherstellungstests geprüft werden.

Zur Vermeidung von langfristigen Ausfällen nach einem Grossereignis, sollte ein georedundanter Standort für die Systeme oder mindestens für die Datensicherungen geprüft werden.

Empfehlung 6 (Priorität 1)

Die EFK empfiehlt den Parlamentsdiensten, eine georedundant ausgelegte Server-Infrastruktur zu prüfen und allenfalls umzusetzen. Minimal sollte ein ausgelagertes Offline Backup erstellt werden.

Die Empfehlung ist akzeptiert.

Stellungnahme der PD

Die Parlamentsdienste betreiben zwei Rechenzentren (Parlamentsgebäude und Bundeshaus Ost). Ein Rechenzentrum an einem weit entfernten Standort wurde bisher aus wirtschaftlichen Gründen abgelehnt. Die Frage soll 2024 noch einmal geprüft werden.

Die Parlamentsdienste arbeiten gemeinsam mit dem Bundesamt für Informatik und Telekommunikation (BIT) am Aufbau einer zusätzlichen Backuplösung, die es ermöglichen soll, die Daten unveränderbar und verschlüsselt in einem Rechenzentrum des BIT abzulegen.

Zudem wird geprüft, inwiefern die Auslagerung von unkritischen Daten in eine cloudbasierte Infrastruktur die Georedundanz gewährleisten kann.

2.8 Das betriebliche Kontinuitätsmanagement deckt Abhängigkeiten von der IT nicht ausreichend ab

Die PD verfügen über eine Cyber-Notfallorganisation sowie eine Krisenstabsorganisation auf Stufe Geschäftsleitung, welche beide beübt werden.

Die PD haben ein Handbuch für das Business Continuity Management (BCM) aus dem Jahr 2019. Im Handbuch sind keine Referenzen zu den wichtigen Informatiksystemen vorhanden. Die Massnahmen und Abläufe des BCM fokussieren auf die Durchführung der Sessionen. Unterstützungsprozesse wie zum Beispiel die Bereitstellung der Informatik-Landschaft sind nicht angemessen adressiert. Im Entwurf des ISDS-Konzepts von CuriaPlus existiert ein Verweis hinsichtlich der Notwendigkeit zur Erstellung eines Notfallkonzepts und von Wiederherstellungsplänen. Im ISDS-Konzept Parlnet wird das Thema «Notfallkonzept» nicht adressiert.

Beurteilung

Das BCM Handbuch der PD reflektiert noch nicht die seit 2019 vorangetriebenen Digitalisierungsbestrebungen und die damit einhergehende stärkere Abhängigkeit von IT-Systemen. Der Ausfall von kritischen Anwendungen – bspw. CuriaPlus – kann zu erheblichen operativen Einschränkungen führen und muss daher im Rahmen der Business Impact Analyse und der BCM-Planung detailliert bearbeitet werden.

Der Bedarf für generelle und spezifische IT-Notfallkonzepte resp. Wiederherstellungspläne wurde in den ISDS-Konzepten dokumentiert. Zudem wurde auch im Bericht der Krisenstabsübung vom Oktober 2022 auf Optimierungsbedarf in diesen Themen hingewiesen.

Um auf Notfälle wirksam vorbereitet zu sein, ist es unabdingbar Notfallkonzepte und Wiederanlaufpläne zu erarbeiten und diese regelmässig zu üben.

Empfehlung 7 (Priorität 1)

Die EFK empfiehlt den Parlamentsdiensten, die kritischen Anwendungen und Systeme zu identifizieren und für diese geeignete Massnahmen zur Betriebsweiterführung im Störungsfall vorzusehen. Dies muss mit dem übergreifenden BCM abgestimmt sein und die Planung von Übungen beinhalten.

Die Empfehlung ist akzeptiert.

Stellungnahme der PD

Die PD verfügen über eine Cyber-Notfallorganisation (Cyber NFO) sowie eine Krisenstabsorganisation auf Stufe Geschäftsleitung. Beide Gremien führen regelmässige Übungen durch, die Cyber NFO zuletzt am 4. Juli mit Beteiligung eines für die PD kritischen Lieferanten. in Zukunft ist mindestens eine solche Cyber-NFO-Übung pro Jahr geplant, die nächste nach der Sommersession 2024.

Die Überarbeitung des BCM-Handbuchs unter Einschluss des Themas IT-Service-Continuity war bereits geplant und ist im Gang.

3 Umsetzung früherer Empfehlungen

3.1 Sicherheitsprüfungen von isolierten Systemen zeigen ein wenig realistisches Bild

Im Rahmen der Prüfung des Projektes CuriaPlus wurde folgende Empfehlung (21310.001) ausgesprochen:

«Die EFK empfiehlt den Parlamentsdiensten, rasch eine umfassende Sicherheitsprüfung von Liferay und direkt damit verbundenen Komponenten wie auch einen Code-Review der sicherheitsrelevanten Eigenentwicklungen in Liferay durchzuführen. Die Ergebnisse müssen in der zu erarbeitenden Soll-Architektur berücksichtigt werden.»

In der Stellungnahme der PD wird angekündigt, dass die bereits durchgeführte Sicherheitsüberprüfung zwar wiederholt werden soll, weitergehende Prüfungen aber als "nicht verhältnismässig" abgelehnt werden.

Die externe Prüferin führt in ihrem Bericht aus, dass gewisse Komponenten der Parlnet Infrastruktur von der Prüfung ausgenommen wurden, jedoch *"für eine umfassende und vollständige Aussage zur Sicherheit der Parlnet Infrastruktur (...) eine Überprüfung der Out of Scope Elemente erfolgen [muss]"*. Dies deckt sich mit der Empfehlung der EFK, die "verbundenen Komponenten" in eine Sicherheitsüberprüfung mit einzuschliessen.

Der Code Review wurde gemacht und bei diesem wurden keine Auffälligkeiten festgestellt.

Beurteilung

Aus Sicht der EFK ist eine vollständige Sicht der Sicherheit der Parlnet Infrastruktur erforderlich (siehe Kapitel 2.3)

Die Massnahme 21310.001 wird geschlossen. Das Thema des erweiterten Umfangs wird jedoch in der Empfehlung 3 in diesem Bericht aufgenommen.

3.2 Dokumente und Verträge sind zu finalisieren

Im Rahmen der Prüfung des Projektes CuriaPlus wurde folgende Empfehlung (21310.005) ausgesprochen:

«Die EFK empfiehlt den Parlamentsdiensten, die fehlenden Lieferergebnisse für Liferay rasch zu erstellen. Dies betrifft insbesondere die Infrastruktur für umfassende Tests, einen überarbeiteten Rahmenvertrag, Betriebs- und Wartungsverträge (inkl. SLA), fehlende Konzepte, die Prüfung der Sicherheitsanforderungen sowie vollständige Tests und formelle Abnahme. Sobald die übergeordneten Grundlagen vorliegen, müssen die Lieferergebnisse überprüft und bei Bedarf angepasst werden.»

Das Projekt Cervin wurde in die neue Betriebsorganisation «Digitale Dienstleistungen» übergeben.

Im Empfehlungscontrolling wurden Betriebs- und Wartungsverträge inkl. SLA sowie Service-Management-Konzepte für den produktiven Betrieb mit dem Dienstleister überprüft. Der SLA und das Betriebskonzept liegen als Entwurf vor.

Die weiteren in der Empfehlung der EFK geforderten Konzepte und -Verträge wurden von Seiten der PD erstellt und in finalen Versionen vorgelegt.

Beurteilung

Die Umsetzungsmeldung der PD konzentriert sich darauf, dass keine neuen Befunde hoher Kritikalität aus der erneuten Sicherheitsprüfung festgestellt wurden (vgl. 21310.001). Diese Aussage ist korrekt. Der Nachweis einer formellen Projektabnahme, sowie der Abnahmen der in der Empfehlung erwähnten SLAs, des Betriebs- und Wartungsvertrags und des Service Management Konzeptes ist jedoch noch pendent.

Die Massnahme 21310.005 bleibt weiterhin offen.

3.3 Eine Risikoanalyse wurde erstellt, die geforderten Dokumente für CuriaPlus sind noch in Bearbeitung

Im Rahmen der Prüfung des Projektes CuriaPlus wurde folgende Empfehlung (21310.006) ausgesprochen:

«Die EFK empfiehlt den Parlamentsdiensten, für CuriaPlus umgehend mit Unterstützung eines Sicherheitsexperten eine vollständige Gefahren- und Risikoanalyse vorzunehmen. Anschliessend sind die fehlenden Lieferergebnisse rasch fertigzustellen (Infrastruktur für umfassende Tests, Betriebskonzepte und ISDS-Konzept und deren Umsetzung). Sobald die übergeordneten Grundlagen vorliegen, müssen die Lieferergebnisse überprüft und bei Bedarf angepasst werden. Die Arbeiten sind in interdisziplinären Teams voranzutreiben.»

Gemäss der Stellungnahme der PD zur Empfehlung der EFK wird eine Gefahren- und Risikoanalyse als "nicht sinnvoll" abgelehnt. Es wird jedoch ausgeführt, dass das Projekt CuriaPlus eine sicherheitstechnische Überprüfung vornehmen wird, sobald die Schnittstellenanbindungen bestehen.

Nachweise der durchgeführten und weiterer geplanter sicherheitstechnischer Überprüfungen, wie auch in interdisziplinären Teams durchgeführte Risikoanalysen im Rahmen des ISDS Konzeptes wurden der EFK vorgelegt.

Ferner wurden die folgenden in der Empfehlung geforderten Konzepte zwischenzeitlich erstellt resp. aktualisiert:

- Zielarchitektur (inkl. Test-Infrastruktur): Vorgelegt und in Umsetzung
- Betriebskonzepte: Vorgelegt in der Entwurfsversion 0.64
- ISDS Konzept: Vorgelegt in der Entwurfsversion 0.5, wird gem. PD nicht abgenommen, sondern laufend erweitert

Beurteilung

Die PD haben sicherheitstechnische Überprüfungen veranlasst und planen weitere bis zum GoLive der Applikation CuriaPlus durchzuführen. Das Betriebskonzept sowie das ISDS-Konzept sind noch nicht formell abgenommen. Dies muss spätestens bis zur Betriebsaufnahme erfolgen.

Die Massnahme 21310.006 bleibt weiterhin offen.

Anhang 1: Rechtsgrundlagen und parlamentarische Vorstösse

Rechtstexte
Bundesgesetz über die Eidgenössische Finanzkontrolle (Finanzkontrollgesetz, FKG) vom 28. Juni 1967 (Stand am 1. Januar 2021), SR 614.0
Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV) vom 27. Mai 2020 (Stand am 1. April 2021); SR 120.73
Bundesgesetz über die Bundesversammlung (Parlamentsgesetz, ParlG) vom 13. Dezember 2002 (Stand am 2. Dezember 2019), SR171.10
Verordnung der Bundesversammlung zum Parlamentsgesetz und über die Parlamentsverwaltung (Parlamentsverwaltungsverordnung, ParlVV) vom 3. Oktober 2003 (Stand am 2. Dezember 2019), SR 171.115
Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) vom 18. Dezember 2020, noch nicht in Kraft gesetzt
Vorgaben und Standards
Si001 – IT-Grundschutz in der Bundesverwaltung, V5.0 vom 23.Februar 2022
Parlamentarische Vorstösse
20.4260 – Zukunftsfähige Daten-Infrastruktur und Daten-Governance in der Bundesverwaltung. Motion eingereicht von der Finanzkommission des Nationalrates, 6.10.2020 Der Bundesrat beantragte am 25.11.2020 die Annahme der Motion. Von beiden Räten angenommen am 17.12.2020 und 8.3.2021.
17.4026 – Digitaler Ratsbetrieb bis 2020. Motion eingereicht von Sebastian Frehner, Nationalrat, 7.12.2017 Von beiden Räten im Jahr 2018 angenommen, damit Auftragserteilung an die Verwaltungsdelegation.
17.3640 – Papierloser Ratsbetrieb. Interpellation eingereicht von Sebastian Frehner, Nationalrat, 11.9.2017 Am 10.11.2017 vom Büro des Nationalrates beantwortet und am 15.12.2017 vom Nationalrat als erledigt eingestuft.
13.3493 – Vorwärts mit dem digitalen Parlament. Motion eingereicht von Thomas Aeschi, Nationalrat, 19.6.2013 Am 12.9.2013 vom Büro des Nationalrates beantwortet und Antrag auf Ablehnung. Am 26.9.2013 im Nationalrat angenommen, am 12.12.2013 im Ständerat abgelehnt.

Anhang 2: Abkürzungen

BCM	Business Continuity Management
BCMS	Business Continuity Management System
BIT	Bundesamt für Informatik und Telekommunikation
CyRV	Cyberrisikenverordnung
EFK	Eidgenössische Finanzkontrolle
GL	Geschäftsleitung
ISB	Informationssicherheitsbeauftragter
ISDS	Informationssicherheits- und Datenschutzkonzept
ISG	Informationssicherheitsgesetz
ISMS	Information Security Management System
ISO	International Organization for Standardization
NCSC	Nationalen Zentrum für Cybersicherheit
OWASP	Open Worldwide Application Security Project
PD	Parlamentsdienste
POC	Proof of Concept
SAFe	Scaled Agile Framework
Schuban	Schutzbedarfsanalyse
SLA	Service Level Agreements

Anhang 3: Glossar

Bug Bounty	Ethische Hacker im Rahmen von sogenannten Bug Bounty-Programmen die produktiven IT-Systeme und Applikationen der Bundesverwaltung nach Schwachstellen durchsuchen.
Cervin	Informatikprojekt «Digitale Arbeitsplattform für die Bundesversammlung» der Parlamentsdienste zur Ablösung von Intranet/Extranet der Parlamentsdienste. Dies ist lediglich ein erster Schritt. Schlussendlich sollen viel weitergehende Anforderungen erfüllt werden: «Eine zentrale, digitale Arbeitsplattform, die alle geschäfts- und supportrelevanten Prozesse sowie die dafür benötigten Funktionen, orts- und geräteunabhängig, auf einer webbasierten Plattform abbilden bzw. zur Verfügung stellen kann. Das dynamische Aggregieren von Inhalten unterschiedlicher Quellsysteme garantiert jederzeit einen umfassenden und aktuellen Informationsstand.» Im Projekt Cervin wurde auch die Plattform Liferay eingeführt, auf welcher Parlnet (ehemals Intranet/Extranet) und CuriaPlus laufen.
CuriaPlus	Informatikprojekt der Parlamentsdienste, mit dem die bestehenden CURIA-Anwendungen und die Datenbank ersetzt werden sollen. Der parlamentarische Betrieb im Zusammenhang mit der Kommissions- und Sessionsarbeit soll gesamtheitlich in einer Grundausstattung digitalisiert werden
Incident Management	IT-Incident Management bzw. IT-Störungsmanagement umfasst typischerweise den gesamten organisatorischen und technischen Prozess der Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Betriebsstörungen in IT-Bereichen sowie hierzu vorbereitende Maßnahmen und Prozesse.[4]
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.

[4] Quelle: wikipedia.org.

Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept)	Das ISDS-Konzept bildet die Grundlage für die Festlegung der Mass-nahmen für die Informationssicherheit und den Datenschutz. Es zeigt die (Rest-)Risiken auf, die mit dem Betrieb des IT-Systems und der Organisation verbunden sind. Es beschreibt das Notfall-konzept. Gemäss der «Richtlinie Informationssicherheit in Projekten» der Parlamentsdienste muss das ISDS-Konzept gegen Ende der Konzeptphase erstellt sein (inkl. Risikoanalyse). Die Prüfung/Abnahme muss mit dem Phasenabschluss Konzept erfolgen. Die Umsetzung des ISDS-Konzeptes muss während der Realisierung erfolgen und vor der Einführung in die Produktion abgenommen werden. (Quelle: https://intranet.ncsc.admin.ch/ncscintra/de/home/vorgaben-hilfsmittel/sicherheitsverfahren/erhoehter-schutz.html)
ISMS	Ein Information Security Management System (ISMS) ist die Aufstellung von Verfahren und Regeln innerhalb einer Organisation, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.
ISO 2700x	Die ISO/IEC 27000-Reihe ist eine Sammlung von Standards zur Informationssicherheit. Herausgegeben werden die über 20 Normen von der International Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC).
Kritische Infrastruktur	Als KI werden Prozesse, Systeme und Einrichtungen bezeichnet, die essenziell für das Funktionieren der Wirtschaft bzw. das Wohlergehen der Bevölkerung sind.
SAFe	Das Scaled Agile Framework® (SAFe) besteht aus einer Reihe von Organisations- und Workflow-Mustern zur Implementierung von Agile-Praktiken im gesamten Unternehmen. Das Framework ist eine Wissenssammlung mit strukturierten Leitlinien zu Rollen und Zuständigkeiten, zur Planung und Verwaltung von Aufgaben und zu förderungswürdigen Werten. SAFe fördert die Abstimmung, Zusammenarbeit und Ausführung über zahlreiche «Agile Teams» hinweg. Es ist keine Projektmanagementmethode.

Schutzbedarfsanalyse (Schuban)	Mit der Schuban werden die Anforderungen an die Informationssicherheit und den Datenschutz erhoben. Zeigt die Schuban, dass ein erhöhter Schutz nötig ist, muss eine vertiefte Risikoanalyse durchgeführt und ein Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) verfasst werden. Gemäss der «Richtlinie Informationssicherheit in Projekten» der Parlamentsdienste muss die Freigabe der Schuban zu Beginn der Initialisierung erfolgen. (Quelle: https://intranet.ncsc.admin.ch/ncscintra/de/home/vorgaben-hilfsmittel/sicherheitsverfahren/beurteilung-schutzbedarf.html
Verwaltungsdelegation	Der Verwaltungsdelegation obliegt die oberste Leitung der Parlamentsverwaltung. Sie befasst sich mit sämtlichen Fragen im Zusammenhang mit der Haushaltsführung, dem Personalmanagement, der Sicherheit, der Informatik und der Infrastruktur des Parlaments. Ausserdem übt die VD die Oberaufsicht über die Parlamentsdienste. (Quelle: www.parlament.ch)

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).