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