AUDIT

Audit de la gestion des identités et des accès (eIAM)

Chancellerie fédérale – secteur Transformation numérique et gouvernance informatique

L'ESSENTIEL EN BREF

La solution eIAM *(electronic Identity and Access Management)* de l'Office fédéral de l'informatique et de la télécommunication (OFIT) constitue la plateforme centrale d'authentification pour l'ensemble de l'administration fédérale. Elle sert à gérer les identités numériques et les droits d'accès à toutes les applications et à tous les services Web qui lui sont rattachés et doit offrir aux autorités fédérales une solution d'authentification à la fois sûre, efficace et centralisée.

En septembre 2024, quelque 100 000 utilisateurs recouraient chaque jour au système eIAM pour se connecter à plus de 800 applications, ce qui représente environ 250 000 connexions par jour. Les coûts d'exploitation et de développement du système eIAM se montent à environ 20 millions de francs par an.

La gestion du service standard a été conçue de manière ciblée et permet d'assurer une exécution efficace des tâches. Les risques associés à la dépendance vis-à-vis du fournisseur clé ont été évalués et font l'objet d'un suivi. L'exploitation est stable, les procédures sont définies et les documents de sécurité sont mis à jour en continu. Depuis le dernier audit, réalisé en 2018[2], des progrès remarquables ont été réalisés dans le domaine de la virtualisation et de la gestion de plusieurs instances.

Des améliorations sont néanmoins nécessaires en ce qui concerne les mesures destinées à réduire les risques inhérents à la dépendance vis-à-vis de l'eIAM.

Il convient d'élargir les tests de basculement d'urgence

L'OFIT a installé le système eIAM dans deux centres de calcul (CC) pour assurer sa géo-redondance. Le premier test de basculement *(failover test)*, au cours duquel le cœur du système eIAM a été basculé du CC PRIMUS au CC CAMPUS, s'est déroulé avec succès. Il a cependant révélé l'existence de différents problèmes. Les enseignements tirés de ce test ont conduit à optimiser le fonctionnement, notamment pour ce qui est de veiller à la disponibilité immédiate de l'équipe et d'automatiser les processus. D'autres défis techniques restent à résoudre avant un nouveau test de basculement complet.

En septembre 2024, l'OFIT a décidé de réaliser un test de basculement des composants essentiels du système eIAM vers l'environnement de référence lors de chaque mise à jour. Ces tests font cependant l'impasse sur des composants importants, car tester ces composants exigerait d'impliquer les équipes responsables d'autres applications. L'exclusion délibérée de ces composants des tests comporte cependant un risque, car ils jouent un rôle central dans la structure d'authentification et de contrôle d'accès du système eIAM. Une défaillance ou une erreur de configuration pourraient entraîner des conséquences graves pour l'accès aux applications critiques. Il convient dès lors d'inclure également ces composants dans les tests.

Des solutions opérationnelles font défaut en cas de panne des centres de calcul

L'OFIT a élaboré des plans d'urgence et de redémarrage pour les centres de calcul qui hébergent le système eIAM. Au sein de l'office, le plan de redémarrage est régi par le service chargé de la continuité des activités *(Business Continuity Management, BCM)* et intégré dans le programme de la continuité du service de l'OFIT. L'OFIT a établi un document formel concernant le redémarrage du système eIAM, qui est en cours de validation interne et qui ne concerne, dans un premier temps, que le CC PRIMUS à Berne.

[2] Audit de la gestion et de l'exploitation du service standard « gestion de l'identité et de l'accès » (nº d'audit 18502).

Le basculement vers le CC CAMPUS est également consigné dans un document et sera effectué sous la conduite du service BCM. Au moment de l'audit, aucun plan concret n'existait cependant pour le cas d'une panne simultanée des deux centres de calcul.

AGOV sera le premier grand service à utiliser l'identité électronique (e-ID) comme preuve d'identité pour accéder aux applications des autorités. Cette solution renforcera encore le rôle central du système eIAM/AGOV dans la gestion des identités de la Confédération et des autorités suisses.