Audit transversal sur la sécurité TI dans l'administration fédérale
Rapport à l'attention du Conseil fédéral

L'essentiel en bref

Le Contrôle fédéral des finances (CDF) a reçu le 24 juin 2010, par décision du Conseil fédéral du 4 juin 2010, une demande écrite du Délégué à la stratégie informatique de la Confédération, qui le priait de contrôler le degré de mise en œuvre des mesures prises pour renforcer la sécurité informatique. Le CDF y a répondu favorablement le 27 août 2010, en promettant de mener un audit transversal en 2011. Son rapport de révision a été porté à la connaissance des membres du Conseil fédéral le 2 décembre 2011, par une note d'information du Département fédéral des finances (DFF).

Dans son concept des audits de 2011, le CDF a défini pour cette révision tant les mesures à examiner, avec le degré de priorité ou d'approfondissement requis, que les domaines pertinents de l'administration fédérale. Trois thèmes ont été retenus, soit le «respect des exigences en matière de mot de passe», la «réparation dans les délais des lacunes de sécurité» et la «surveillance accrue des réseaux». L'audit portait au total sur sept fournisseurs de prestations informatiques de l'administration fédérale. En outre, le CDF a mené auprès de 71 bénéficiaires de prestations une enquête écrite sur le «respect des exigences en matière de mot de passe», la «réparation dans les délais des lacunes de sécurité» et l'«amélioration de la gestion de l'information». Ces thèmes se recoupaient avec les mesures immédiates de l'arrêté du Conseil fédéral du 16 décembre 2009.

Les principales conclusions de cet audit sont les suivantes:

L'environnement Windows ne présente que des lacunes sans gravité. Les fournisseurs de prestations examinés ont atteint un bon niveau, tant pour le respect des exigences en matière de mot de passe que pour la réparation dans les délais des erreurs des nouveaux systèmes Windows.

La sécurité de l'environnement non-Microsoft laisse sérieusement à désirer. Le CDF constate que les lacunes de sécurité des produits non-Microsoft fonctionnant sur les plates-formes Windows sont loin d'être corrigées dans les délais. Le problème vient des applications spécialisées, qui ne permettent parfois plus d'actualiser les composantes vulnérables. En outre, les compétences pour la mise à jour de tels produits ne sont pas clairement définies. Enfin, les systèmes anciens sont techniquement peu sûrs: d'une part, ils ne satisfont pas aux exigences en matière de mot de passe, d'autre part on ne trouve parfois plus d'actualisation pour corriger les lacunes de sécurité récentes.

Les bénéficiaires de prestations s'accommodent de ces lacunes de sécurité, et les fournisseurs de prestations ne parviennent pas à s'imposer. Bien des utilisateurs n'accordent, exemples à l'appui, qu'un faible degré de priorité aux questions de sécurité:

- Une partie des postes de travail bénéficient de droits d'accès privilégiés (droits d'administrateur local). Ces paramètres ont été installés en réponse aux vœux des utilisateurs.
- Les domaines d'activité continuent d'exploiter des applications et des systèmes désuets, en sachant pertinemment qu'ils laissent à désirer sur le plan de la sécurité ou qu'ils empêchent de mettre à jour des composantes importantes pour la sécurité.

- Les règles concernant les mots de passe avaient été désactivées au niveau de la direction d'un département. Les mécanismes d'escalade en place ont visiblement été impuissants face aux ordres venus d'en haut.
- La responsabilité en matière de sûreté de l'information reste souvent assimilée, de manière réductrice, à la responsabilité technique incombant aux fournisseurs de prestations. La prise de conscience de la répartition des tâches et des responsabilités entre fournisseurs et bénéficiaires de prestations ne s'est pas encore faite.
- Certains fournisseurs de prestations déplorent de ne pas avoir, bien souvent, les moyens de s'imposer face aux utilisateurs, faute de réglementation contraignante ou suffisamment spécifique. D'où la nécessité de préciser sur ce plan les directives de sécurité.

Les synergies entre les fournisseurs de prestations sont plutôt le fruit du hasard. Lors de ses vérifications, le CDF a constaté que de bonnes solutions ont été adoptées à bien des endroits. Or à ses yeux, ce savoir est trop peu diffusé parmi les fournisseurs de prestations, et les synergies sont insuffisamment exploitées. Chaque fournisseur de prestations a tendance à créer ou faire développer isolément ses propres solutions.

De nombreuses activités sont déployées au titre de la surveillance accrue du réseau. Les fournisseurs de prestations concernés ont réalisé de premiers projets et en sont à la phase de collecte des expériences. De nouvelles étapes sont prévues, notamment pour maîtriser et analyser l'afflux de données. Tous les fournisseurs de prestations ne sont pas favorables au délai de conservation de deux ans exigé d'eux pour les fichiers journaux. La volonté de renforcer la sécurité TI a beau être là, il ne faut pas s'attendre à des améliorations à court terme

La sécurité des réseaux cantonaux reste la «grande inconnue». Faute de base contractuelle, l'Office fédéral de l'informatique et de la télécommunication (OFIT) n'est pas habilité à s'assurer jusqu'ici que les cantons connectés ont atteint la qualité requise sur le plan de la sécurité des réseaux, et à prendre le cas échéant les mesures nécessaires. La situation changera d'ici la fin de l'année, avec la signature d'accords de niveau de service (SLA) remaniés avec les cantons. Leur mise en œuvre, soit la garantie de la sécurité des réseaux cantonaux et la fourniture des preuves correspondantes, ne sera possible dans certains cantons qu'à moyen terme.

Les réactions parvenues au CDF suggèrent que les bénéficiaires de prestations n'ont pas encore partout entièrement identifié leurs applications essentielles pour la protection de l'information.

Le CDF a adressé des recommandations ciblées au Conseil de l'informatique de la Confédération (CI) et à l'Unité de stratégie informatique de la Confédération (USIC), ainsi qu'aux divers fournisseurs de prestations. Les recommandations destinées à l'USIC ou au CI visaient notamment à préciser les exigences, à intensifier la collaboration entre les fournisseurs de prestations ainsi que la formation en matière de sécurité. Les réponses écrites reçues montrent que les recommandations du CDF ont été bien acceptées.

Texte original en allemand