Sécurité informatique au sein du Service de renseignement de la Confédération

Rapport de la Délégation des Commissions de gestion (résumé)

du 30 août 2013

Rapport

1 Introduction

Le 30 mai 2012, le directeur du Service de renseignement de la Confédération (SRC) a fait savoir au président de la Délégation des Commissions de gestion (DélCdG) qu'un collaborateur de son service avait dérobé de gros volumes de données classifiées et qu'il avait été arrêté par la suite.

La DélCdG a effectué diverses investigations au sujet de l'incident, avant de décider, le 15 octobre 2012, de consacrer une inspection formelle à la sécurité informatique au sein du SRC. Le 16 octobre 2012, elle a informé le public de son intention (au moyen d'un communiqué de presse[1] et d'une conférence de presse), après en avoir parlé avec le chef du Département fédéral de la défense, de la protection de la population et des sports (DDPS).

De novembre 2012 à février 2013, la DélCdG a procédé à plusieurs auditions dans le cadre de son inspection. Elle s'est en outre rendue au service informatique du SRC en décembre 2012. Lors de sa séance de fin avril 2013, elle s'est entretenue pour la dernière fois avec le chef du DDPS au sujet de cette affaire.

Début juin 2013, la DélCdG a invité les départements concernés à prendre position sur le projet de son rapport d'inspection. Le 2 juillet 2013, elle a rencontré une délégation du Conseil fédéral, avec qui elle a discuté des conclusions de son inspection. Le lendemain, elle a transmis son rapport d'inspection assorti de onze recommandations au Conseil fédéral[2].

La DélCdG souhaitait éviter que la publication de certaines informations concernant le SRC ne viole les intérêts supérieurs de l'Etat, aussi a-t-elle décidé de ne pas rendre public son rapport complet. Elle a alors rédigé le présent résumé à l'intention du public, en y incluant ses recommandations et une synthèse des principales conclusions de son inspection.

2 Situation du service informatique du SRC

Pour se conformer aux exigences de la loi fédérale sur le renseignement civil (LFRC)[3], en mars 2009 le Conseil fédéral avait décidé de regrouper le Service d'analyse et de prévention (SAP) et le Service de renseignement stratégique (SRS) au sein d'un unique office fédéral. A la demande du DDPS, cette opération devait être réalisée début 2010 «sans ressources supplémentaires». Cela impliquait que le futur SRC devrait s'accommoder des ressources informatiques dont disposait jusque-là le SRS, puisque le DDPS avait précédemment repris le SAP du Département fédéral de justice et police (DFJP), sans le personnel nécessaire pour couvrir les besoins informatiques de ce service. Cette lacune n'ayant pas été comblée lors de la

1 «Sécurité de l'informatique au sein du Service de renseignement de la Confédération», communiqué de presse de la DélCdG du 16.10.2012.
2 «Inspection de la DélCdG relative à la sécurité informatique au sein du SRC», communiqué de presse de la DélCdG du 3.7.2013.
3 Loi fédérale du 3.10.2008 sur le renseignement civil (LFRC; RS **121**).

conception du SRC ni ultérieurement, le SRC a dû se contenter d'effectifs très restreints pour gérer un ensemble de systèmes complexes et toujours plus nombreux.

Pour les banques de données du SRC, cela signifiait qu'en cas d'absence de l'unique gestionnaire interne de banques de données, la sécurité de l'exploitation pouvait être garantie uniquement pour autant qu'aucun problème grave ne survienne. A la suite de la fusion, différents systèmes repris par le SRC devaient être remplacés ou adaptés. Cependant, le manque d'informaticiens disponibles limitait le nombre de projets que le SRC pouvait réaliser.

Selon le rapport que le DDPS a publié le 11 avril 2013 sur le vol de données au SRC, «[l]e SRC s'est ainsi retrouvé à devoir gérer un nombre de systèmes et d'applications nettement plus élevé et près du double d'utilisateurs avec des capacités en personnel qui n'[avaient], elles, pas évolué»[4]. Aux yeux de la DélCdG, cette situation était due à une planification insuffisante, qui remontait à la décision du Conseil fédéral, prise en mai 2008, de transférer le SAP au DDPS. Le 25 mars 2009, sur proposition du DDPS, le Conseil fédéral a décidé de créer le SRC à partir des deux services existants sans augmenter les ressources. Le DDPS aurait dû combler le manque d'effectifs qui en a résulté dans le domaine informatique, si ce n'est pendant les travaux de mise sur pied du SRC, au plus tard après sa création.

Au printemps 2011, le SRC a informé pour la première fois la DélCdG de sa situation concernant le personnel informatique, laquelle découlait des origines du SRC. Avant le vol de données, le SRC n'avait toutefois jamais signalé qu'il estimait sa sécurité informatique menacée à cause de cette situation. La Délégation des finances (DélFin) n'avait pas non plus reçu d'informations qui auraient révélé une quelconque nécessité d'intervenir[5].

La DélCdG en conclut que ni le transfert du SAP au DDPS ni la création du SRC qui a suivi n'ont été préparés avec suffisamment de soin. Considérant la nouvelle loi sur le renseignement, la délégation estime qu'il est impératif que le DDPS s'appuie sur une analyse irréprochable, en comparant la situation réelle et la situation idéale, en vue d'évaluer les futurs besoins en personnel du service.

Recommandation 1

La DélCdG recommande au Conseil fédéral de charger le DDPS de mener une analyse approfondie et précise sur les effectifs dont le SRC a besoin pour pouvoir exécuter les missions supplémentaires prévues par la nouvelle loi sur le Service de renseignement.

3 Gestion des risques au sein du SRC

La sécurité informatique du SRC n'était pas intégrée dans un processus de gestion des risques, qui aurait permis d'identifier les conséquences de la pénurie de personnel dans le domaine informatique et de réduire de manière ciblée les risques exis-

4 «Service de renseignement de la Confédération: fuite de données déjouée», rapport du DDPS du 11.4.2013, p. 10.
5 Lettre de la DélFin à la DélCdG du 5.6.2013, p. 2.

tants. Ces dernières années, le SRC a bien apporté une contribution plus large au reporting du département sur les risques[6], mais la gestion interne des risques – y compris pour l'informatique – n'a débouché ni sur la définition et l'évaluation des risques, ni sur leur affectation à des «propriétaires des risques». L'inspection de la DélCdG n'a pas révélé d'indices selon lesquels la direction du SRC aurait procédé activement, avant le vol de données, à une gestion des risques systématique au sein du service.

Le «document approuvé concernant la protection et la sécurité»[7] dont fait mention le rapport du DDPS du 11 avril 2013 réglait les responsabilités en matière de gestion des risques de façon lacunaire, sans compter qu'il n'avait été approuvé qu'au sein du SRC lui-même. Or le SRC devrait plutôt aligner sa gestion des risques sur les directives générales de la Confédération et un document propre devrait seulement servir à compléter ou différencier les directives en question avec des règles spécifiques au service.

Se fondant sur sa politique de gestion des risques définie en 2004, le Conseil fédéral a édicté des directives sur la politique de gestion des risques menée par la Confédération[8] en 2010. Après quoi, des directives de l'Administration fédérale des finances (AFF) sur la gestion des risques menée par la Confédération sont entrées en vigueur à l'automne 2011. Ces dernières ont été complétées par un manuel de gestion des risques au sein de la Confédération[9].

Recommandation 2

La DélCdG recommande au Conseil fédéral de s'assurer que le DDPS lui rende compte, d'ici à juin 2014, de l'état de la gestion des risques au sein du SRC et précise dans quelle mesure le SRC met en œuvre de manière adéquate les directives du Conseil fédéral en la matière.

4 Mesures prises par le SRC en matière de sécurité informatique avant le vol de données

L'ordonnance sur l'informatique dans l'administration fédérale[10] et les directives[11] du Conseil de l'informatique de la Confédération (CI) contiennent plusieurs dispositions relatives à la sécurité informatique. Le DDPS a en outre édicté sa propre directive et le service chargé de la sécurité informatique à la Protection des informations et des objets (PIO) a publié, en sa qualité d'organe prescriptif et de contrôle, un

6 «Reporting sur les risques à l'attention du Conseil fédéral», rapport des Commissions de gestion du Conseil national et du Conseil des Etats du 28.5.2010 (FF **2010** 5157–5164).
7 Rapport du DDPS du 11.4.2013, p. 11.
8 Directives du 24.9.2010 sur la politique de gestion des risques menée par la Confédération (FF **2010** 5965).
9 Documents disponibles sur le site Internet de l'AFF: www.efv.admin.ch/f/dokumentation/finanzpolitik_grundlagen/risiko_versicherungspolitik.php
10 Ordonnance du 9.12.2011 sur l'informatique et la télécommunication dans l'administration fédérale (OIAF; RS **172.010.58**).
11 Directives du CI du 27.9.2004 concernant la sécurité informatique dans l'administration fédérale, disponibles sur le site Internet de l'UPIC: www.isb.admin.ch/themen/sicherheit/00150/00836/index.html?lang=fr

guide de sécurité informatique, qui demeure toutefois incomplet eu égard au standard recherché.

La DélCdG a constaté que le SRC n'appliquait pas, avant le vol de données, différentes mesures techniques et organisationnelles qui auraient dû faire partie de la protection fondamentale de son informatique et dont certaines étaient prescrites par la Confédération ou par le DDPS.

De plus, il n'y avait pas suffisamment – voire pas du tout – de personnel pour accomplir la mission de délégué à la sécurité informatique de l'unité organisationnelle (DSIO), ce qui rendait impossible une gestion des risques adéquate dans le domaine informatique. Par ailleurs, les concepts de sécurité requis pour les applications et les systèmes – lorsqu'ils existaient – étaient pour la plupart insuffisants.

Les mots de passe permettant d'accéder aux comptes d'administrateur non nominatifs étaient gérés au sein même du service informatique et leur utilisation n'était pas contrôlée. Vu la minceur des effectifs, cette pratique simplifiait la garantie de l'exploitation informatique. Cependant, elle fournissait aussi aux informaticiens concernés des droits d'accès illimités et il était impossible de déterminer après coup qui en avait fait usage.

Alors que certaines activités du système étaient enregistrées à des fins de sécurité, la DélCdG n'est pas parvenue à trouver la preuve que les enregistrements des activités du système (fichiers journaux) étaient systématiquement évalués. Ainsi, aucune analyse n'a été effectuée durant les cinq mois de l'année 2012 qui ont précédé l'information, venue de l'extérieur, concernant un éventuel vol de données. Il n'existait non plus aucun plan d'urgence applicable en cas de soupçon d'une menace pour les systèmes ou leurs données. Enfin, le SRC ne disposait pas du personnel dont il aurait eu besoin pour l'exploitation d'un système de surveillance efficace.

Après le vol de données, la direction du SRC s'est empressée, avec la diligence requise, d'engager un DSIO à plein temps (en novembre 2012) et de satisfaire ainsi aux directives de la Confédération. Par contre, l'importance des concepts de sécurité pour la gestion des risques liés aux systèmes informatiques a été reconnue plus tard. De fait, ce n'est qu'à fin 2012 que le SRC a commencé, avec le concours de la PIO, à se demander de quels concepts il pourrait avoir besoin et comment ceux-ci pourraient être améliorés.

Un concept de sûreté de l'information et de protection des données (concept SIPD) sert à évaluer les risques pour la sécurité d'un système et, sur cette base, à choisir les mesures techniques, organisationnelles et autres grâce auxquelles ces risques pourront être réduits. Cette approche axée sur les risques évite la mise en œuvre de mesures qui ne déboucheront pas sur une réduction appropriée des risques, compte tenu de la diversité des risques et des ressources disponibles.

Recommandation 3

La DélCdG demande au DDPS de veiller à ce que le DSID DDPS contrôle, d'ici à la fin de l'année 2014, si toutes les applications et tous les systèmes du SRC ont été dotés d'un concept de sécurité valable contenant une analyse des risques fondée et complète. Un plan de mesures contraignant sera établi pour la correction des carences éventuelles.

L'inspection a montré que la direction du SRC ne prêtait pas suffisamment attention à la question de savoir quelles directives le service devait suivre dans le domaine de la sécurité informatique. C'est la seule façon d'expliquer que l'art. 7, al. 1, OSI-SRC[12], qui demande le cryptage du système de communication interne au SRC (SiLAN), n'ait jamais été mis en œuvre alors que la nouvelle direction du SRC avait, à la création du service en 2009, voulu une telle mesure et proposé au Conseil fédéral d'édicter une norme correspondante par voie d'ordonnance.

Recommandation 4

La DélCdG demande au Conseil fédéral de charger le DDPS d'examiner, d'ici à la fin de l'année 2013, si les dispositions de l'art. 7, al. 1, OSI-SRC relatives au cryptage du SiLAN peuvent être mises en œuvre de manière que la charge de travail exigée soit proportionnée aux gains pour la sécurité informatique. Selon le résultat de cet examen, cette disposition devra soit être appliquée dans les meilleurs délais soit être immédiatement abrogée.

5 Contrôles de sécurité relatifs aux personnes

Les deux services qui ont donné naissance au SRC connaissaient des régimes différents dans le domaine des contrôles de sécurité relatifs aux personnes (CSP). Au SAP, les personnes assumant par exemple des fonctions purement administratives étaient exemptées de ces contrôles, tandis qu'au SRS tous les employés y étaient soumis. Le plus haut degré des CSP, soit le contrôle de sécurité élargi avec audition (art. 12 OCSP[13]), n'était toutefois pas appliqué à tous les collaborateurs du SRS, et notamment pas à ceux du service informatique.

Après la fusion du SAP et du SRS, le SRC a décidé de soumettre tous les nouveaux employés et tous ceux qui doivent réitérer leur contrôle après une durée de cinq ans à un CSP selon l'art. 12 OCSP. Compte tenu des capacités limitées du service spécialisé chargé des CSP et d'entente avec la PIO, il a cependant renoncé à avancer les contrôles dont la répétition n'était pas encore à l'ordre du jour.

A la suite d'une révision totale de l'OCSP[14], en 2011, le DDPS a édicté, le 1er avril 2012, une ordonnance (OCSP-DDPS[15]) en vertu de laquelle toutes les fonctions exercées au sein du SRC étaient soumises au contrôle selon l'art. 12 OCSP. Aux termes des dispositions transitoires de l'OCSP-DDPS, les personnes pour lesquelles un contrôle de sécurité d'un degré supérieur était désormais prescrit devaient faire l'objet d'un nouveau contrôle de sécurité dans un délai d'un mois au plus suivant l'entrée en vigueur de l'ordonnance. Or, l'inspection de la DélCdG a révélé que le SRC n'avait pas satisfait à cette exigence et que, en février 2013, un tiers des em-

12 Ordonnance du 4.12.2009 sur les systèmes d'information du Service de renseignement de la Confédération (OSI-SRC; RS **121.2**).
13 RO **2002** 377
14 Ordonnance du 4.3.2011 sur les contrôles de sécurité relatifs aux personnes (OCSP; RS **120.4**).
15 Ordonnance du DDPS du 12.3.2012 concernant les contrôles de sécurité relatifs aux personnes (OCSP-DDPS; RS **120.423**).

ployés du SRC n'avait pas encore été soumis au contrôle selon l'art. 12 OCSP – dont un quart du personnel de l'informatique.

En raison du nombre croissant des projets informatiques, dus notamment à la fusion du SAP et du SRS, le SRC est devenu de plus en plus dépendant d'informaticiens externes. Ceux-ci ne sont toutefois pas soumis, contrairement au personnel du SRC, à un contrôle de sécurité de degré maximal. L'inspection de la DélCdG n'a pas apporté de réponse concluante à la question de savoir quel service est responsable de l'ouverture des CSP pour les collaborateurs externes ainsi que de la décision du niveau de ces contrôles.

La DélCdG estime que les services de la Confédération qui sont les destinataires finaux des prestations fournies par des tiers doivent garantir qu'ils ne travaillent qu'avec des collaborateurs et des entreprises externes qui ont fait l'objet de contrôles de sécurité appropriés. Les offices concernés devraient donc avoir une vue d'ensemble de tous leurs collaborateurs externes, ce qui, selon les investigations menées par la DélCdG, n'est pas encore le cas aujourd'hui.

Recommandation 5

La DélCdG recommande au Conseil fédéral de réviser l'OCSP de sorte que les collaborateurs externes soient soumis au même degré de contrôle de sécurité que les employés de la Confédération qui exercent la même activité qu'eux. Le service de la Confédération qui est le destinataire final des prestations fournies par les entreprises externes doit être responsable du respect, par ces entreprises et par leurs collaborateurs, des prescriptions applicables.

Le problème de l'exécution des CSP au SRC ou ailleurs ne peut pas être considéré indépendamment des ressources en personnel, restreintes depuis des années, dont dispose le service compétent de la PIO. Selon un rapport de l'Inspectorat du DDPS du 21 décembre 2012, le nombre de CSP en suspens avait augmenté à 1500 environ à la fin 2012. Bien que le chef du DDPS ait temporairement renforcé, en novembre 2012, le personnel du service chargé des CSP, l'Inspectorat du DDPS estimait que le retard pris dans les CSP ne serait pas rattrapé avant cinq ans. Cette situation est d'autant plus épineuse qu'une grande partie des dossiers en attente concerne des cas qui présentent un risque potentiel élevé et qui exigent par conséquent un travail considérable.

Comme les CSP doivent être régulièrement répétés, il n'est pas possible de remédier durablement au manque de personnel par le biais d'un renfort temporaire. En outre, le nombre de contrôles demandés par les départements n'a cessé de croître au cours des dernières années. La question se pose donc de savoir si la Confédération n'affecte pas assez de personnel aux CSP, de manière générale, ou si les départements ont prescrit le contrôle de degré maximal pour trop de fonctions, par exemple parce que c'est une façon pour les supérieurs de se décharger de leurs responsabilités au lieu d'assumer effectivement les tâches de direction qui leur incombent.

La DélCdG est pleinement convaincue de la nécessité des CSP, qui constituent une sorte de protection de base dans le domaine de la sécurité de l'information. Néanmoins, elle tient à souligner les conclusions de son inspection selon lesquelles il est indispensable d'assurer une conduite effective du personnel, ce qui n'a pas été fait

des semaines durant dans le cas du vol de données au SRC, et ce, alors que des signes avant-coureurs étaient apparus suffisamment tôt.

La tendance à privilégier les CSP pour garantir la sécurité, plutôt que de mettre l'accent sur les responsabilités en termes de direction, ressort également de la réaction officielle du DDPS face au vol de données. Dans son rapport du 11 avril 2013, le DDPS affirme que rien ne prouve qu'un contrôle de sécurité élargi avec audition aurait permis de formuler des réserves quant à la poursuite de l'activité du gestionnaire des banques de données[16]. En tout état de cause et sans tenir compte de la question des ressources disponibles, le DDPS s'interroge sur l'opportunité d'introduire partout dans l'administration fédérale, en vue de réduire encore les risques, des CSP plus élargis et un rythme de contrôle plus serré.

Plus les CSP seront élargis et généralisés pour toutes les fonctions imaginables de l'administration fédérale, plus le danger sera grand de voir des personnes dirigeantes renoncer à d'autres approches de la gestion des risques ou aux instruments prévus par le droit du personnel.

Recommandation 6

La DélCdG recommande au Conseil fédéral de présenter, dans son message relatif à la loi sur la sécurité de l'information (LSI), une explication détaillée des rôles imputables aux contrôles de sécurité relatifs aux personnes et à la conduite du personnel dans le domaine de la sécurité de l'information et de les différencier clairement. Parallèlement, il faudrait établir un rapport séparé comportant une estimation des effectifs que la Confédération doit affecter à la réalisation des contrôles de sécurité, d'une part, et une description de la contribution que la Confédération entend ainsi apporter à la sécurité de l'information, d'autre part.

6 Vol de données en mai 2012

La DélCdG constate que le SRC, en raison de ressources en personnel trop limitées dans le domaine informatique et d'une gestion des risques inadaptée, ne s'est pas suffisamment employé à garantir la disponibilité, l'intégrité et la confidentialité des données, qui constituent l'objectif principal de la sécurité informatique.

En avril 2012, une nouvelle absence pour cause de maladie de l'unique gestionnaire des banques de données du SRC avait engendré, d'après ses supérieurs, un risque croissant pour la sécurité de l'exploitation de ces systèmes. En outre, la collaboration avec cet employé avait été ressentie comme à nouveau plus difficile. La direction du service informatique a alors jugé nécessaire d'intervenir au niveau hiérarchique supérieur. Le 26 avril 2012, elle a attiré son attention sur le fait qu'il était possible que le gestionnaire porte atteinte à l'intégrité des logiciels de gestion des banques de données. Concrètement, elle a aussi proposé de lui retirer l'accès aux systèmes qu'il était chargé d'administrer.

La direction de la division à laquelle sont rattachés le service informatique, la cellule de sécurité, le service juridique et le service du personnel a ainsi été placée face à un

16 Rapport du DDPS du 11.4.2013, p. 18.

choix cornélien: suspendre le gestionnaire des banques de données et mettre en péril la disponibilité des systèmes, ou le maintenir à son poste et courir le risque que l'intégrité et – comme le confirmerait la suite de l'affaire – la confidentialité des données soient compromises.

Alors que le chef de la division concernée connaissait clairement les risques encourus, il a laissé passer une semaine avant de parler, le 7 mai 2012, avec ses subordonnés directs des possibilités d'intervention. Il n'a pourtant pas encore pris de mesures contre le gestionnaire des banques de données à ce moment-là, mais a attendu trois jours supplémentaires pour décider de le faire convoquer à un entretien.

Durant cette phase critique, il aurait fallu adopter une conduite et un encadrement rigoureux à l'égard du collaborateur en question, ce qui n'a pas été le cas. Ainsi, le gestionnaire des banques de données a pu, seulement une heure après le rendez-vous du 16 mai 2012 auquel il ne s'était pas présenté, s'attarder longuement à son poste de travail sans que cela provoque la moindre réaction de la part de la direction de la division.

La réaction déficiente de la division en matière de conduite du personnel et de gestion des risques a finalement rendu possible le vol de données opéré en mai 2012. Le directeur du SRC n'a eu connaissance des risques identifiés en avril 2012 qu'après que le SRC a été informé par un tiers, le 18 mai 2012, du comportement suspect du gestionnaire des banques de données.

D'après la DélCdG, il est inexact de prétendre que le droit du personnel de la Confédération ne permettait pas au SRC d'agir en conséquence envers le gestionnaire des banques de données. Le SRC aurait dû envisager à temps les possibilités offertes par l'art. 103 OPers[17], qui prévoit la suspension de l'employé ou son affectation à une autre fonction. Comme le SRC n'avait pas consigné les problèmes qu'il rencontrait depuis déjà longtemps avec ce collaborateur, il n'avait toutefois aucun élément sur lequel s'appuyer pendant la crise pour prononcer, par exemple, une suspension pour cause d'irrégularités répétées et établies au sens de l'art. 103, al. 1, let. b, OPers.

La DélCdG ne partage pas non plus le point de vue selon lequel le SRC aurait réagi assez tôt, sur la base des problèmes constatés en avril 2012, afin de pouvoir découvrir lui-même le vol en temps utile, même sans l'information externe. Alors que l'identification du gestionnaire des banques de données, avec l'aide de la grande banque suisse qui avait signalé son comportement suspect, se prolongeait, le SRC n'a pas envisagé, par exemple, de vérifier les fichiers journaux liés aux interfaces externes par lesquelles le gestionnaire aurait pu copier des données. De même, dans cette période, le SRC n'a pas vérifié si le soupçon selon lequel le gestionnaire avait compromis les logiciels des banques de données, était fondé. Ces deux vérifications n'ont été effectuées qu'après que le SRC ait définitivement vérifié le renseignement fourni par la banque.

La DélCdG n'a aucune raison de supposer que le dispositif de surveillance et de contrôle qui était en place au service informatique du SRC et qui, dans le meilleur des cas, était lacunaire, aurait permis de découvrir le vol de données.

17 Ordonnance du 3.7.2001 sur le personnel de la Confédération (OPers; RS **172.220.111.3**).

7 Mesures prises par le SRC après le vol

Aux yeux de la DélCdG, le directeur du SRC ne s'est pas acquitté de ses devoirs de surveillance de manière suffisamment systématique après le vol de données et il n'a pas confié les enquêtes internes aux organes appropriés. Une décision en particulier fait problème, à savoir celle d'avoir confié l'élucidation interne de l'affaire au chef de la division qui était directement responsable de tous les domaines ayant défini l'action du SRC avant le vol de données.

Le chef de la division a ensuite focalisé son analyse sur la personne du gestionnaire des banques de données, sans chercher les causes possibles du vol de données dans l'organisation et les procédures du SRC. Il n'y a pas eu non plus d'évaluation concernant la question de savoir si le SRC avait appliqué les mesures de sécurité prescrites dans le domaine informatique. C'est le chef de la sécurité qui en a été chargé ultérieurement. Il n'était toutefois pas la personne idéale pour juger si les responsabilités en termes de direction avaient été correctement assumées à l'égard du gestionnaire des banques de données, autrement dit pour évaluer le comportement de son chef de division.

Tout comme la Surveillance des services de renseignement (Surveillance SR), la DélCdG considère que le rattachement organisationnel de la cellule de sécurité à une division opérationnelle pose des problèmes. L'affaire du vol de données a montré que les intérêts divergents des domaines de la sécurité, de l'exploitation informatique et du personnel avaient empêché qu'une intervention énergique n'ait lieu dans l'intérêt de la sécurité. Dans ces circonstances, les décisions nécessaires auraient dû être prises à un échelon supérieur de la hiérarchie.

Recommandation 7

La DélCdG recommande au chef du DDPS de veiller à ce que le SRC déplace la cellule de sécurité dans son organigramme afin qu'elle ne soit plus subordonnée à la division SRCA. Parallèlement, il y a lieu de repenser la répartition des tâches relatives à la gestion des risques à l'échelle du service.

La DélCdG estime qu'il était opportun que le SRC réagisse relativement vite à l'incident en prenant certaines mesures immédiates, par exemple dans la gestion des mots de passe. Peu à peu, la délégation a toutefois eu l'impression que la multiplication des mesures prises par la direction du SRC servait surtout à prouver sa maîtrise active des conséquences du vol de données. La mise en évidence des mesures en cours et des mesures prévues reléguait à l'arrière-plan la question des causes de l'incident.

Les mesures visant à renforcer la sécurité ont en outre été décidées sans être étayées par un processus de gestion des risques pertinent. Le directeur du SRC a notamment approuvé des mesures qui n'ont jamais été appliquées ou qui se sont révélées techniquement irréalistes par la suite. La DélCdG est d'avis qu'il faut une gestion des risques efficace pour que les mesures de sécurité adéquates soient prises dans le service et que les priorités y afférentes soient fixées à bon escient.

Comme le SRC avait négligé d'analyser les causes systémiques du vol de données, le problème des ressources en personnel ne s'est pas vu accorder, pendant trop

longtemps, la priorité qu'il aurait méritée. Ce n'est que dans la deuxième quinzaine du mois d'octobre 2012 que la direction du service s'est déclarée prête à en faire davantage que de se limiter à une augmentation minimale des ressources en personnel dans le domaine informatique.

Finalement, les besoins en personnel de la sécurité informatique au SRC ont été confirmés par la décision du Conseil fédéral du 1er mai 2013 de lui octroyer onze postes supplémentaires. Bien que cette décision n'ait été prise qu'un an après le vol de données, la DélCdG s'en félicite. Néanmoins, elle regrette que l'augmentation des ressources en personnel ne prenne effet qu'à partir de 2014 pour une partie et qu'à partir de 2015 pour une autre. La situation difficile que connaît le service informatique du SRC en termes de personnel durera ainsi plus longtemps que ce que la sensibilité des données du SRC ne permettrait en fait de tolérer.

Recommandation 8

La DélCdG recommande au DDPS de permettre au SRC de pourvoir les postes d'informaticiens dès 2013, en puisant dans la réserve de personnel du département, et ce même si le Conseil fédéral n'a approuvé ces postes qu'à partir de 2014.

8 Enquête sur la sécurité de l'information menée sur mandat du Conseil fédéral

A la suite du vol de données survenu au SRC, le Conseil fédéral a décidé, le 24 octobre 2012, sur la proposition du DDPS, de demander une analyse des risques liés à la sécurité de l'information au niveau fédéral. Un groupe de travail, qui était déjà en train d'élaborer la future LSI sous la direction du professeur Markus Müller (Université de Berne), devait détecter, jusqu'à la fin février 2013, les lacunes frappant la sécurité de l'information et proposer des moyens de les combler immédiatement. Ce délai s'est toutefois révélé trop court, de sorte que l'objet de l'enquête s'est limité au vol de données commis par des collaborateurs internes.

Le 1er mars 2013, le DDPS a présenté le rapport du groupe de travail au Conseil fédéral en l'invitant formellement à en prendre acte. Celui-ci s'est exécuté le 15 mars 2013 et a décidé de mettre en œuvre dès l'automne 2013 la recommandation visant à former et à sensibiliser les cadres de l'administration fédérale en matière de prévention d'actes malveillants internes.

Le groupe de travail a également souligné la nécessité d'appliquer sans restriction les dispositions fédérales en vigueur dans le domaine de la sécurité de l'informatique et de l'information. De plus, les mesures propres à améliorer la sécurité informatique que le Conseil fédéral avait édictées en décembre 2009 et en juin 2010 pour l'ensemble de l'administration fédérale à la suite des attaques perpétrées contre l'informatique du Département fédéral des affaires étrangères (DFAE) devraient être rigoureusement appliquées. Certaines de ces mesures ont été examinées par le Contrôle fédéral des finances (CDF) en 2011 et en 2012 sur mandat du Conseil fédéral.

A cet égard, il convient de mentionner aussi que l'Unité de pilotage informatique de la Confédération (UPIC)[18] rédige chaque année, à l'intention du Conseil fédéral, un rapport sur la sécurité informatique au sein de la Confédération, dans lequel elle fait le point sur la mise en œuvre des mesures de sécurité (cf. art. 11, al. 2 et 3, OIAF). Jusqu'ici, la PIO établissait en sus un rapport annuel sur la protection des informations à la Confédération, à l'intention de la Délégation du Conseil fédéral pour la sécurité (DélSéc). A la suite de la dernière révision de l'ordonnance concernant la protection des informations (OPrI), du 1er mai 2013, ce rapport ne sera plus adressé que tous les deux ans à la Conférence des secrétaires généraux.

Les deux rapports précités reposent sur les indications livrées par les départements. Afin que les auteurs de ces rapports puissent effectivement dresser l'état de la sécurité informatique et de la protection des informations, il faudrait que les données qu'ils reçoivent soient vérifiées, comme le sont en partie celles qui concernent les mesures décidées en 2009 et 2010 par le Conseil fédéral en matière de sécurité informatique.

Vu les procédures qui ont déjà été institutionnalisées, la DélCdG a l'impression que le mandat donné au groupe de travail du professeur Müller est une mesure isolée, que le DDPS a proposée sans tenir compte des instruments qui sont déjà disponibles au niveau fédéral.

La DélCdG estime que le rapport annuel sur la sécurité informatique au sein de la Confédération rédigé par l'UPIC et les mesures visant à améliorer la sécurité informatique que le Conseil fédéral a prises en 2009 et en 2010, à la demande du Département fédéral des finances, constituent une base appropriée pour entamer un processus durable d'amélioration de la sécurité informatique au niveau de la Confédération. Les rapports de l'UPIC, qui se fondent aujourd'hui principalement sur les déclarations spontanées des départements, pourraient être transformés en un système de controlling. En outre, le contrôle des mesures de sécurité décidées par le Conseil fédéral, auquel procède actuellement le CDF, pourrait être institutionnalisé sous une forme adéquate.

Par ailleurs, la DélCdG considère que les conclusions du contrôle de l'état de la sécurité informatique devraient être intégrées, de façon appropriée, dans les directives et les exigences concernant la sécurité informatique au sein de la Confédération. Enfin, le pilotage informatique au niveau de la Confédération devrait être conçu de telle manière que les directives et les expériences faites en matière de sécurité informatique puissent être prises en compte aussi tôt que possible dans la planification et l'acquisition des moyens informatiques.

Recommandation 9

La DélCdG recommande au Conseil fédéral d'élaborer des propositions visant à améliorer le processus de contrôle de l'état de la sécurité informatique au sein de la Confédération. Ces mesures devront permettre au Conseil fédéral d'identifier les risques liés à la sécurité informatique suffisamment tôt, d'adopter les mesures requises pour réduire ces risques et de suivre leur mise en œuvre dans le cadre d'un processus institutionnalisé.

18 Avant 2012, l'UPIC portait le nom d'Unité de stratégie informatique de la Confédération.

9 Surveillance exercée par le chef du DDPS

Durant les trois premiers mois qui ont suivi la découverte du vol de données, le chef du DDPS s'est fondé sur l'appréciation de l'incident qu'il avait reçue de la part du SRC. Or, cette appréciation se concentrait sur la personne du gestionnaire des banques de données et négligeait les autres causes qui auraient pu contribuer à la réalisation des faits.

Ce n'est que vers la fin août 2012 que le chef du DDPS a demandé à un organe extérieur au SRC d'éclaircir le contexte qui avait amené le vol de données et d'analyser la réaction du service. Des mandats en ce sens ont été confiés, le 24 août 2012, à la Surveillance SR du département et, en octobre 2012, à la PIO.

Le 22 octobre 2012, la PIO a procédé à une évaluation de la sécurité informatique au sein du SRC à l'intention du chef du DDPS. Selon la PIO, les ressources en personnel du SRC étaient insuffisantes dans les domaines de l'informatique et de la sécurité. Dans un rapport complémentaire établi à la demande du chef du DDPS, la PIO a estimé qu'il fallait créer, en plus du poste de DSIO, deux autres postes dans le domaine de la sécurité et de cinq à dix postes à plein temps afin d'être en mesure de doubler les fonctions particulièrement sensibles du service informatique.

En vue d'améliorer la capacité de réaction du SRC en termes de conduite et de personnel, la PIO a suggéré d'étendre les possibilités de suspendre rapidement un employé occupant des fonctions sensibles pour la sécurité. Une telle mesure devrait cependant s'accompagner de compensations financières ou autres pour l'employé concerné. Ainsi, la PIO a proposé que celui-ci, en cas de suspension immédiate, continue de percevoir son salaire pour une plus longue période ou se voie proposer une activité équivalente dans un domaine moins sensible en termes de sécurité.

Selon la PIO, il conviendrait toutefois d'examiner encore la faisabilité de ces propositions sous l'angle du droit du personnel. Le DDPS n'a pourtant pas profité de l'occasion, dans la perspective de son rapport final du 11 avril 2013, pour éclaircir ces questions juridiques, ni pour présenter des modèles de conditions d'embauche correspondantes.

Recommandation 10

La DélCdG recommande au Conseil fédéral de constituer un groupe de travail interdépartemental placé sous la conduite de l'Office fédéral du personnel (OFPER), dont la mission consistera à élaborer des conditions d'embauche particulières permettant d'améliorer la capacité de réaction des organes de conduite du personnel face aux risques d'attaques internes. Pour obtenir l'adhésion nécessaire du personnel visé, il convient notamment d'envisager des mesures de compensation de nature financière ou autre. Le Conseil fédéral est invité à donner son avis sur les conclusions du groupe de travail d'ici fin 2014.

En septembre 2012, la Surveillance SR a remis au chef du DDPS un premier rapport intermédiaire, puis, en prévision de la rencontre de la mi-octobre 2012 entre la DélCdG et lui-même, un second rapport intermédiaire. Après quoi, le chef du DDPS

a prié la Surveillance SR de terminer pour fin novembre 2012 les différentes investigations dont il l'avait chargée depuis août 2012.

Ainsi que l'a appris la DélCdG, le SRC avait refusé, fin octobre 2012, de fournir à la Surveillance SR son analyse du potentiel de dommage représenté par les données volées avant que le directeur du service n'ait demandé et reçu l'accord du chef du DDPS à cet effet. A la connaissance de la DélCdG, le droit en vigueur ne comporte pourtant aucune disposition qui justifie une telle réserve de la part du SRC.

La délégation accorde une grande importance à cet incident, car le SRC avait déjà refusé de renseigner la Surveillance SR, et ce, avec l'assentiment du chef du DDPS, dans une autre affaire sans aucun rapport avec l'objet de l'inspection de la DélCdG. Cette dernière a appris l'existence de ce cas lors d'un entretien avec le professeur Koller au sujet de ses conclusions concernant la surveillance interne au département. Selon la DélCdG, le chef du département ne peut permettre et encore moins approuver que le SRC décide quelles informations il livrera ou non à l'organe de surveillance.

Recommandation 11

La DélCdG demande au chef du DDPS de veiller au respect inconditionnel des droits à l'information garantis à la Surveillance SR par la loi (art. 8 LFRC, en relation avec l'art. 26, al. 1, LMSI) et l'ordonnance (art. 33, al. 1, OSRC). Le SRC ne peut limiter ces droits à l'information ni de son propre chef, ni d'entente avec le chef du département.

Dans ses deux rapports intermédiaires, la Surveillance SR a formulé cinq recommandations à l'adresse du chef du DDPS. Elle les a réitérées dans son rapport final de fin novembre 2012.

La DélCdG ne comprend pas pourquoi ce n'est qu'en avril 2013 que le chef du DDPS s'est prononcé sur ces recommandations et qu'il les a transmises au SRC pour que celui-ci les mette en œuvre – d'autant moins que ces recommandations figuraient déjà dans le deuxième rapport intermédiaire de la Surveillance SR, publié six mois auparavant.

Globalement, la DélCdG constate aussi que la manière dont le chef du DDPS a exercé son devoir de surveillance a été source d'ambiguïtés quant à la répartition des rôles entre la Surveillance SR et le SRC.

Le chef du DDPS a finalement chargé, le 19 novembre 2012, le professeur Heinrich Koller, ancien directeur de l'Office fédéral de la justice (OFJ), d'effectuer une enquête sur la Surveillance SR. Il souhaitait ainsi «avoir un examen […] de tous les acteurs concernés» du DDPS à la suite du vol de données[19]. Les résultats de l'expertise ont été livrés fin mars 2013. Ils n'apportaient rien de nouveau au sujet de la sécurité informatique au sein du SRC.

Etant donné l'objectif que le DDPS avait fixé au professeur Koller pour son enquête, la DélCdG ne comprend pas pourquoi le chef du DDPS a limité celle-ci à la Surveillance SR. La délégation estime qu'il aurait été non seulement pertinent, mais encore

19 Rapport du DDPS du 11.4.2013, p. 16.

justifié, après le vol de données commis au SRC, de soumettre aussi la PIO à l'examen en question. En effet, cette unité ne joue pas qu'un rôle de surveillance puisqu'elle doit également approuver les concepts SIPD du SRC.

En octobre 2012, la DélCdG a appris que le chef du DDPS prévoyait de rédiger, sur la base des conclusions de l'incident, un rapport final portant sur les enseignements à tirer pour l'ensemble de l'administration fédérale. Contrairement aux déclarations du chef du DDPS, le Conseil fédéral ne lui avait jamais confié un tel mandat.

Le DDPS a finalisé son rapport le 11 avril 2013 et celui-ci a été présenté au Conseil fédéral le 24 avril 2013 sous la forme d'une simple note d'information. Le 30 avril 2013, le rapport a été rendu public lors d'une conférence de presse du département.

Le DDPS est arrivé à la conclusion que le SRC n'était, «de loin, pas le seul service de l'administration fédérale à conserver des données particulièrement sensibles» et que, «si des données venaient à disparaître dans un autre service, le potentiel de dommage serait aussi très important»[20]. Le DDPS s'est dit convaincu que le SRC avait effectué, en édictant 40 mesures à la suite du vol, un travail de base qui pourrait s'avérer utile à l'ensemble de l'administration. Le DDPS a même proposé d'examiner dans quelle mesure il serait judicieux de mettre en œuvre ces dispositions également hors du SRC.

Les documents qui ont servi de base au rapport final du DDPS ne comprennent aucune indication du potentiel de dommage au sein de l'informatique de l'administration fédérale. La DélCdG n'exclut cependant pas que certaines des mesures décidées par le SRC puissent contribuer à améliorer la sécurité informatique de l'un ou l'autre service de la Confédération. Les autres services de la Confédération ne devraient cependant pas répéter l'erreur du SRC et se focaliser sur une liste de mesures avant d'avoir identifié et évalué les risques pertinents. Ce n'est en effet qu'après une telle analyse qu'il convient de décider quelles mesures sont appropriées et lesquelles doivent être prises en vue de réduire les risques avérés.

20 Rapport du DDPS du 11.4.2013, p. 18.

10 Suite de la procédure

La DélCdG a déjà envoyé son rapport d'inspection complet au Conseil fédéral le 3 juillet 2013, en le priant de prendre position sur le rapport même et sur les recommandations qu'il contient d'ici fin octobre 2013. Ces recommandations sont intégralement reproduites dans le présent résumé du rapport.

30 août 2013

Pour la Délégation des Commissions de gestion

Le président:
Pierre-François Veillon, conseiller national

La secrétaire:
Beatrice Meli Andres

Les Commissions de gestion du Conseil des Etats et du Conseil national ont pris acte du présent résumé du rapport et approuvé sa publication.

4 septembre 2013

Pour les Commissions de gestion

Le président de la Commission de gestion du Conseil des Etats:
Paul Niederberger, conseiller aux Etats

Le président de la Commission de gestion du Conseil national:
Ruedi Lustenberger, conseiller national

La secrétaire:
Beatrice Meli Andres

Index des abréviations

AFF	Administration fédérale des finances
CDF	Contrôle fédéral des finances
CdG	Commissions de gestion du Conseil national et du Conseil des Etats
CI	Conseil de l'informatique de la Confédération
Concept SIPD	Concept de sûreté de l'information et de protection des données
CSP	Contrôles de sécurité relatifs aux personnes
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DélCdG	Délégation des Commissions de gestion
DélFin	Délégation des finances
DélSéc	Délégation du Conseil fédéral pour la sécurité
DFAE	Département fédéral des affaires étrangères
DFJP	Département fédéral de justice et police
DSID	Délégué à la sécurité informatique au niveau départemental
DSIO	Délégué à la sécurité informatique de l'unité organisationnelle
FF	Feuille fédérale
LFRC	Loi fédérale du 3.10.2008 sur le renseignement civil (RS *121*)
LMSI	Loi fédérale du 21.3.1997 instituant des mesures visant au maintien de la sûreté intérieure (RS *120*)
LSI	Loi fédérale sur la sécurité des informations (projet)
OCSP	Ordonnance du 4.3.2011 sur les contrôles de sécurité relatifs aux personnes (RS *120.4*)
OCSP-DDPS	Ordonnance du DDPS du 12.3.2012 concernant les contrôles de sécurité relatifs aux personnes (RS *120.423*)
OFJ	Office fédéral de la justice
OFPER	Office fédéral du personnel
OIAF	Ordonnance du 9.12.2011 sur l'informatique et la télécommunication dans l'administration fédérale (ordonnance sur l'informatique dans l'administration fédérale; RS *172.010.58*)
OPers	Ordonnance du 3.7.2001 sur le personnel de la Confédération (RS *172.220.111.3*)
OPrI	Ordonnance du 4.7.2007 concernant la protection des informations de la Confédération (ordonnance concernant la protection des informations; RS *510.411*)
OSI-SRC	Ordonnance du 4.12.2009 sur les systèmes d'information du Service de renseignement de la Confédération (RS *121.2*)
OSRC	Ordonnance du 4.12.2009 sur le Service de renseignement de la Confédération (RS *121.1*)
PIO	Protection des informations et des objets
RS	Recueil systématique
SAP	Service d'analyse et de prévention

SiLAN	Système de communication chiffré
SRC	Service de renseignement de la Confédération
SRCA	Aide à la conduite et à l'engagement
SRS	Service de renseignement stratégique
Surveillance SR	Surveillance des services de renseignement
UPIC	Unité de pilotage informatique de la Confédération