Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense,
de la protection de la population et des sports DDPS

Service de renseignement de la Confédération : fuite de données déjouée

Rapport du DDPS

11 avril 2013

Sommaire

1. Résumé

En mai 2012, malgré les mesures de sécurité et de protection existantes, un collaborateur du Service de renseignement de la Confédération (SRC) a volé une quantité non négligeable de données classifiées et les a emportées hors des locaux du SRC. Le collaborateur en question est un spécialiste de systèmes qui connaissait depuis quelque temps des difficultés d'intégration sur son lieu de travail, n'acceptait qu'avec réticence les décisions de sa hiérarchie et avait connu plusieurs absences prolongées pour des raisons de santé. Avant le vol déjà, le SRC s'est efforcé de trouver une solution à ce problème et a tout entrepris afin de soutenir le collaborateur dans sa situation personnelle difficile.

Grâce à son bon réseau de relations avec l'économie privée, le SRC a été immédiatement informé de l'affaire liée au vol de données. Avec les autorités de poursuite pénale auxquelles il a été fait appel, il a ainsi pu prendre des mesures afin d'éviter que les données soient transmises plus loin. Dès que le vol a été connu, le DDPS et le SRC ont immédiatement informé les autorités compétentes (la présidente de la Confédération, le Ministère public, la Délégation des Commissions de gestion ainsi que le Conseil fédéral).

Les données du SRC n'ont jamais été en mains non autorisées. Cependant, sans les mesures fermes et rapides qui ont été prises à l'intérieur et à l'extérieur de l'administration, la possibilité qu'elles soient remises à des tiers, en Suisse ou à l'étranger, ou qu'elles soient publiées, n'aurait pas pu être exclue.

Suite à ces événements, la direction du DDPS et celle du SRC ont pris sans tarder les décisions qui s'imposaient. Plusieurs services et groupes d'experts internes et externes à l'administration ont été chargés d'analyser la situation et de mettre en évidence les points nécessitant que des mesures soient prises.

Le SRC a déjà identifié et introduit 40 mesures relevant de ses domaines de compétence. Elles concernent des aspects techniques et organisationnels ainsi que des restrictions de consultation et d'accès. Pour sa part, le DDPS a décidé d'augmenter les ressources en personnel du SRC, à la demande de ce dernier et sur recommandation de la Protection des informations et des objets (PIO). Onze nouveaux postes seront créés dans les domaines de l'informatique et de la sécurité. De même, la Surveillance des services de renseignement, rattachée au Secrétariat général du DDPS, sera également renforcée tant au niveau du personnel et que de ses méthodes de contrôle. On peut ainsi retenir que les responsables du SRC et du DDPS ont pris des mesures indispensables pour empêcher efficacement qu'un tel événement ne se reproduise.

Suite à ce vol de données, le Conseil fédéral a chargé le Département fédéral des finances (DFF) de prendre des mesures afin d'informer et de former les cadres de l'administration fédérale aux questions de sécurité de l'information. D'autres améliorations concernant la sécurité suivront avec la nouvelle loi fédérale sur la sécurité des informations qui est actuellement en cours d'élaboration sous la conduite du DDPS et qui sera prochainement mise en consultation.

Du point de vue du DDPS, on peut conclure que les mesures nécessaires ont été prises très rapidement suite au vol de données et qu'elles ont été mises en œuvre ou qu'elles sont en train de l'être. Comme la transmission des données à des tiers a pu être empêchée, il n'y a pas eu de dommages pour la Suisse et sa sécurité.

2. Mandat du chef du DDPS

Le 21 janvier 2013, le chef du DDPS a chargé le chef de son état-major de présenter les faits par le biais du présent rapport, ainsi que les mesures qui s'en sont suivies et celles qui doivent encore être mises en œuvre. Le rapport doit exposer de manière détaillée les événements avant, pendant et après le vol, de même que les résultats des examens qui ont été ordonnés suite à cette affaire.

3. Situation initiale et vol des données

3.1 Mandat du SRC

Organisé comme un office fédéral de l'administration centrale, le Service de renseignement de la Confédération (SRC) assume des tâches relevant du renseignement dans le domaine de la sûreté intérieure et extérieure. Son activité a pour objectif de détecter précocement et combattre les dangers liés au terrorisme, au service de renseignements prohibé et à l'extrémisme violent. Le SRC se consacre également à des travaux préparatoires relatifs à la lutte contre le commerce illicite d'armes et de substances radioactives ainsi que contre le transfert illégal de technologie. Afin d'établir une représentation de la situation en matière de sûreté intérieure, le SRC exploite un système électronique spécifique. Celui-ci sert d'instrument de conduite aux autorités fédérales et cantonales compétentes et permet de diffuser des informations en vue du pilotage et de la mise en œuvre de mesures de sécurité. Les cantons doivent spontanément informer le SRC lorsqu'ils constatent un danger concret pour la sûreté intérieure ou extérieure.

Le SRC a également pour mission de se procurer, d'établir et d'analyser des informations essentielles en matière de politique de sécurité sur les événements se déroulant à l'étranger. Il est chargé de présenter une appréciation globale de la menace et entretient en outre des contacts avec plus de cent services de renseignement, de police et de sécurité à travers le monde. Ces contacts ont tous été approuvés par le Conseil fédéral.

Pour accomplir ses tâches, le SRC a le droit de traiter des données personnelles, et notamment des données sensibles et des profils de personnalité, également à l'insu des personnes concernées.

Le SRC est né en 2010

Le SRC existe dans sa forme actuelle depuis le 1er janvier 2010. Auparavant, les tâches qu'il assume étaient partagées entre le Service d'analyse et de prévention (SAP ; rattaché au Département fédéral de justice et police (DFJP) jusqu'en 2008) et le Service de renseignement stratégique (SRS ; au DDPS). Les bases légales sur lesquelles s'appuie le SRC sont notamment la loi fédérale du 3 octobre 2008 sur le renseignement civil (LFRC ; RS 121) et la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI ; RS 120). Ces bases légales doivent être remplacées par une nouvelle loi sur les services de renseignement qui se trouve en phase de consultation jusqu'au 30 juin 2013.

La haute surveillance parlementaire à laquelle est soumis le SRC est assurée par la Délégation des Commissions de gestion. En tant qu'organe interne à l'administration, la Surveillance des services de renseignement examine, sur mandat du chef du DDPS, la légalité, l'opportunité et l'efficacité des activités du SRC.

3.2 Antécédents du vol de données

Afin d'accomplir les diverses missions, le SRC exploite plusieurs banques de données et systèmes d'information complexes qui, pour des raisons de sécurité, se trouvent en grande partie sur un réseau isolé. Pour assurer cette exploitation, il dispose d'un service d'informatique interne.

Le collaborateur X occupait un poste central au sein du service d'informatique du SRC. Au printemps 2012, il a profité de l'accès aux données du SRC dont il bénéficiait de part sa fonction pour télécharger un ensemble important de données. X était employé depuis le 1er avril 2007 en tant que spécialiste des banques de données au SRS, puis au SRC. Suite à son engagement, un contrôle de sécurité relatif à la personne réglementaire a été effectué, conformément à l'art. 11 de l'ordonnance du 4 mars 2011 sur les contrôles de sécurité relatifs aux personnes (RS 120.4 ; OCSP). Ce contrôle s'est conclu par un avis final positif. Depuis 2008, X a été de plus en plus fréquemment absent pour cause de maladie, ce qui n'a pas été sans conséquence pour le fonctionnement du service d'informatique. En 2009, X a déposé sa candidature pour un poste de cadre dans le domaine de l'informatique du SRC. Cependant, le choix s'est porté sur un autre collaborateur du SRC. Par la suite, l'intégration de X au sein de l'équipe TIC est devenue de plus en plus difficile. Individualiste hautement spécialisé et très compétent, X s'est progressivement distancié de ses collègues et de ses supérieurs.

L'accumulation d'absences pour raison de santé a poussé les supérieurs de X à demander, en 2011, un examen par un médecin-conseil. Cet examen a conclu que la capacité de travail ou l'aptitude professionnelle de X ne seraient pas compromises et que le travail ou des problèmes d'ordre professionnel n'auraient pas eu d'impact sur sa santé. Le SRC n'avait ainsi aucun motif de partir du principe que les capacités de X soient diminuées par son état de santé. Malgré une amélioration passagère, les problèmes concernant la santé de X ont toutefois perduré. De plus, des tensions croissantes entre X et ses supérieurs directs se sont fait ressentir. Les entretiens menés pour clarifier la situation n'ont pas permis de normaliser durablement les rapports. Les supérieurs s'interrogeaient de plus en plus à mesure que les absences s'accumulaient.

Situation personnelle tendue

Dans cette situation personnelle tendue, une nouvelle procédure de contrôle de sécurité relatif à la personne, qui doit être renouvelée après cinq ans selon les règles du SRC, a été entamée le 10 février 2012 à un niveau supérieur. Un contrôle de sécurité élargi avec audition, conformément à l'art. 12 de l'OCSP, devait être effectué.

Le 16 avril 2012, X a été mis en arrêt maladie à 100 % par son médecin. Sur ce, le service d'informatique du SRC a été chargé par le chef d'aide à la conduite et à l'engagement (NDBU) d'examiner dans quelle mesure le comportement de X présentait un risque pour le fonctionnement et la sécurité du SRC et quels moyens permettraient de remédier à cette situation. Cette enquête, dont les résultats ont été présentés le 27 avril et actualisés le 7 mai, a mis en évidence la tendance croissante à l'isolement de X face à ses collègues et à ses supérieurs. Elle a aussi retenu le fait que, par ses compétences techniques, X était le seul collaborateur du SRC à disposer de connaissances très pointues concernant l'exploitation de bases de données importantes du SRC. En conclusion, elle préconisait que, si X devait toujours être sous pression, l'accès aux bases de données devraient lui être retiré, et ce pour protéger l'exploitation des bases de données autant que le collaborateur de tout acte impulsif.

Le 10 mai 2012, les supérieurs de X, sous la conduite du chef d'aide à la conduite et à l'engagement, sont parvenus à la conclusion que X devait être invité à un entretien et que les scripts qu'il avait élaborés pour les bases de données devaient être analysés. X ne s'est pas présenté aux rendez-vous proposés, ni le 16 mai, ni le 18 mai 2012.

Il était difficile de prévoir, avant le vol de données, la réaction de X et l'enchaînement des événements qui s'en est suivi. Les différentes tentatives de clarification ont abouti à des avis divergents (expertise médicale vs. expériences faites sur le lieu de travail), ce qui n'a pas facilité la chose. Même si le SRC s'est efforcé à chercher le dialogue avec le collaborateur concerné, il était difficile de juger la situation personnelle et les intentions de ce dernier. La marge de manœuvre était limitée par le droit du personnel de la Confédération.

3.3 Les événements de fin mai 2012

Le 18 mai 2012, un collaborateur du SRC a été informé par téléphone, par le biais d'un contact existant avec une grande banque, qu'un certain Monsieur X avait voulu ouvrir un compte numérique auprès d'une filiale de ladite banque. Pour justifier l'ouverture de ce compte, il avait déclaré attendre le versement d'une somme importante suite à une vente de données de la Confédération. Comme le collaborateur de la banque rendait X attentif au fait que l'argent d'activités criminelles ne saurait être accepté par la banque et que X devait informer ses supérieurs, X a répondu que son supérieur n'était pas au courant. La banque a, quant à elle, explicitement fait savoir que l'ouverture d'un compte numérique n'est possible que pour des montants déclarés et ne provenant pas d'activités illégales.

Suite à ce téléphone, la direction du SRC a immédiatement entrepris les démarches nécessaires pour vérifier que la personne qui s'était présentée auprès de la banque en se faisant passer pour X était bien le collaborateur du SRC en question. Cette procédure a pris quelques jours, l'identification au moyen d'une photo qui a été transmise n'ayant, dans un premier temps, pas été possible. Le 23 mai, un des supérieurs de X a finalement pu l'identifier formellement sur la base des images de vidéosurveillance de la banque.

Réaction immédiate

Le 23 mai au soir, le directeur du SRC a donné pour mission au chef d'aide à la conduite et à l'engagement de dresser, d'ici au jour suivant à midi, un état des lieux et de faire une proposition pour la suite de la procédure, la priorité absolue devant être accordée à la sauvegarde des données afin de prévenir de possibles dommages pour la Suisse. Il a ordonné que des mesures immédiates soient prises et qu'une réunion avec le Ministère public de la Confédération soit planifiée. La saisie écrite de la documentation relative à cette affaire et des mesures prises par la suite ne devait souffrir d'aucune lacune.

Dans la matinée du 24 mai, un premier examen des scripts de bases de données a permis de déceler qu'il était possible que plusieurs milliers de données aient été exportées vers des supports externes.

Information immédiate

Le même jour, à 12h30, le directeur du SRC, son suppléant et le chef d'aide à la conduite et à l'engagement ont informé le chef du DDPS et la secrétaire générale du DDPS des événements et de la situation. Le chef du DDPS en a informé, le jour même, la présidente de la Confédération et, à la première occasion, lors de sa séance du 1er juin, le Conseil fédéral. Il a été pris acte des informations sans que suite y soit donnée.

Au soir du 24 mai, il était finalement établi de manière incontestable qu'une quantité non négligeable de données avait été exportée. Leur volume ne représente toutefois qu'un très faible pourcentage de l'ensemble des données du SRC. Il était également avéré que X était la personne ayant pris ces données. Pour ce faire, il avait pris des mesures afin d'empêcher que les autres collaborateurs du service d'informatique puissent voir ses exportations de données. Par ce procédé, X s'est procuré illicitement une quantité importante de données du SRC. Il a profité de son savoir étendu et des droits d'accès dont il disposait, abusé de la confiance qui lui était accordée, pour copier et exporter illégalement des données.

Dénonciation pénale auprès du Ministère public

Le 24 mai en fin de soirée, le directeur du SRC a présenté l'affaire au procureur général de la Confédération. Le 25 mai, le SRC a déposé une dénonciation pénale auprès du Ministère public de la Confédération dans laquelle il est également retenu que la sauvegarde des données et la préservation de la Suisse d'éventuels dommages devaient avoir la priorité absolue. X a été arrêté le soir du 25 mai. Lors de cette opération les supports de données ont pu être intégralement saisis. Ils ont été examinés durant ce même week-end, ce qui a permis de constater que toutes les données copiées se trouvaient là. Le 27 septembre 2012, le Ministère public a fait savoir publiquement que X avait déjà entrepris des préparations concrètes en vue de la vente des données. Les autorités de poursuite pénale ont également déclaré que rien ne donnait lieu de penser que les données dérobées aient été copiées ou transmises à des tiers. Le SRC n'a cependant pas reçu l'autorisation du Ministère public de consulter les données saisies. La procédure pénale ouverte contre X est toujours en cours.

Le 30 mai 2012, le directeur du SRC a mis le président de la Délégation des Commissions de gestion (DélCdG) au courant de l'affaire, ainsi que le chef de la Surveillance du service de renseignement du SG DDPS. Il a eu à plusieurs reprises des contacts avec le président de la DélCdG au cours du mois de juin.

Résiliation immédiate

Le 4 septembre 2012, le collaborateur X incriminé a été informé qu'une résiliation immédiate des rapports de travail était prévue, en précisant que la possibilité de parvenir à un accord commun demeurait ouverte. X a rejeté cette proposition. La résiliation immédiate des rapports de travail, sans possibilité de négocier un accord, lui a été présentée à nouveau le 28 septembre, un jour après que le Ministère public ait fait savoir publiquement que X avait déjà entrepris des préparations concrètes en vue de la vente des données. En guise de réaction, X a affirmé qu'il n'existait pas de motif de résiliation et que les rapports de travail devaient se poursuivre. Finalement, les rapports de travail avec le collaborateur X ont été résiliés avec effet immédiat le 10 octobre 2012. X a déposé un recours contre cette décision.

Il est à noter que l'objectif principal a été atteint : les données dérobées ont été récupérées et la fuite a pu être évitée, empêchant ainsi des dommages pour la Suisse. Les mesures adéquates ont été prises durant la crise grâce au bon réseau de relations et à l'action ferme du SRC. Les autorités compétentes ont été immédiatement informées.

4. Réaction du SRC après le vol

4.1 Mesures prises par le SRC

Le 1er juin 2012 déjà, le chef d'aide à la conduite et à l'engagement (NDBU) a présenté au directeur du SRC des propositions pour la suite de la procédure ainsi que des mesures immédiates. Il s'agissait notamment d'améliorer le contrôle des importations et exportations de données au sein des systèmes du SRC. Il demandait qu'un service externe soit mandaté afin de vérifier les processus de sécurité utilisés par le service d'informatique du SRC et de proposer des mesures d'amélioration. Ces propositions ont été approuvées et complétées.

Le 12 juillet 2012, le chef d'aide à la conduite et à l'engagement a soumis au directeur du SRC 17 mesures à court, moyen et long terme destinées à accroître la sécurité TIC. Elles cherchaient particulièrement à réduire le risque que d'importantes quantités de données soient retirées du système sans autorisation ou emportées. Dans un deuxième temps, ces mesures ont été complétées pour s'élever à 27, début octobre. Le 5 novembre, le SRC a finalement présenté un catalogue de 40 mesures en réaction au vol de données.

Ces 40 mesures élaborées par le SRC, qui sont déjà en partie mises en œuvre, ne peuvent pas être détaillées dans le présent rapport pour des raisons de confidentialité. Il s'agit de mesures organisationnelles, d'adaptations des conditions de consultation / d'accès ainsi que de mesures techniques et de conduite.

Constitution d'une task force

Suite au vol de données et après diverses vérifications internes, le directeur du SRC a mobilisé, le 28 septembre 2012, une *task force* interne. Elle impliquait une plus large information interne, ce qui était désormais possible après que l'affaire ait été rendue publique par les médias. La *task force* a relayé le groupe de travail existant. Le chef du DDPS a reçu des comptes rendus réguliers du suivi de l'affaire.

Afin d'analyser l'affaire au plus près, le SRC a déposé, le 30 octobre, auprès du Ministère public, une demande de copie-image, soit la mise à disposition d'une copie des données volées. Le SRC a également demandé à pouvoir consulter le dossier. Ces deux demandes ont été rejetées par le Ministère public en raison des principes de la procédure pénale.

Nouvelles directives relatives aux mesures de contrôle et de sécurité

Finalement, le 13 décembre 2012, le directeur du SRC a édicté de nouvelles directives relatives aux mesures de contrôle et de sécurité au SRC. Ces dispositions importantes pour garantir la sécurité des informations et des installations du SRC serviront de réglementation transitoire jusqu'à l'entrée en vigueur de la nouvelle loi sur les services de renseignement qui se trouve actuellement en phase de consultation. Elles précisent que le fournisseur de prestations du SRC enregistre automatiquement les données utilisateurs et les données secondaires (flux et transferts de données, sauvegardes, accès et impressions) lors de l'utilisation de moyens informatiques, de manière à garantir la traçabilité.

Les directives prévoient aussi la possibilité de procéder à des évaluations nominales en cas de soupçon concret d'usage abusif de l'infrastructure électronique ou afin de protéger l'infrastructure informatique en cas de menace concrète. Dans le cadre des contrôles de personnes ou du contenu des sacs, le SRC est désormais autorisé à vérifier si ses collaborateurs transportent des contenus classifiés, que ce soit sur des supports numériques (ordinateur, CD, DVD, clé USB, enregistreur, caméra, téléphone mobile) ou sur papier (documents). Des casiers pouvant être fermés à clé ont été mis à disposition dans l'entrée des sites permanents du SRC pour y ranger les appareils privés (p. ex. téléphones portables) avant de pénétrer dans les secteurs sensibles. Les sacs ou autres objets emportés avec soi peuvent être fouillés avant de quitter le site. Des contrôles de personnes peuvent également être effectués, y compris des palpations de sécurité.

Les collaborateurs doivent, sur demande, ouvrir leurs casiers ou supports de données électroniques afin que des contrôles du contenu puissent être effectués. Afin de garantir la « politique du bureau bien rangé » (*clean desk policy*), c'est-à-dire notamment la mise sous clé des informations classifiées, le SRC peut effectuer des contrôles des postes de travail dans ses locaux, une pratique qui avait d'ailleurs déjà lieu avant l'événement. Des caméras de surveillance peuvent être utilisées pour sécuriser les espaces réservés aux archives, aux coffres, aux serveurs ou au stockage ainsi que des coffres-forts individuels.

Autre nouveauté, il sera également possible de faire des contrôles ponctuels de véhicules. Pour les locaux devant faire l'objet d'une protection particulière, le chef d'aide à la conduite et à l'engagement du SRC peut décréter une interdiction formelle de prendre avec soi des téléphones portables, tablettes numériques, appareils photos ou autres appareils semblables. Grâce à ces diverses dispositions, la protection des informations au sein du SRC sera considérablement améliorée.

Le SRC a pris rapidement toutes les mesures qui étaient de son ressort et les a fermement mises en œuvre. Les dispositions prises permettent d'améliorer considérablement la sécurité à tous les niveaux et réduisent de manière substantielle le risque qu'un vol de données de ce type ne se reproduise.

4.2 Ressources en personnel au SRC

L'affaire du vol de données a mis en évidence que les ressources en personnel allouées au domaine de l'informatique du SRC étaient trop limitées. Cela s'explique notamment par le fait que, lors du transfert de l'ancien Service d'analyse et de prévention (SAP) du DFJP au DDPS et de son intégration à ce qui est désormais le SRC, on a largement renoncé à transférer des collaborateurs et tout particulièrement dans les domaines du personnel, de la sécurité et de l'informatique. Le 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'ont, elles, pas évolué. Le SRC a régulièrement soulevé ce problème par le passé, notamment dans le rapport final du 27 mai 2011 « Exploitation des synergies dans le domaine des services civils de renseignement » établi dans le cadre de l'examen des tâches de la Confédération.

Le SRC a annoncé, fin 2012, un besoin total de douze postes supplémentaires pour les domaines de l'informatique, de la sécurité et du personnel. Le DDPS a accordé onze postes destinés aux domaines de l'administration des banques de données, de la gestion et de la surveillance du réseau, de l'exploitation des systèmes de communication et d'application, de l'infrastructure du courrier, de la sécurité informatique et de la sécurité intégrale. Le poste demandé pour le domaine du personnel n'a pas été accordé.

Avec ces postes supplémentaires, des prestations critiques pour la sécurité peuvent être accomplies dans une plus large mesure par des collaborateurs internes. Les projets de migration qui s'étaient accumulés peuvent être réalisés. Des capacités manquantes au niveau de la sécurité informatique et de la sécurité d'exploitation ont pu être comblées et des postes redondants ont pu être créés. Le principe des quatre yeux peut être assuré de manière permanente et tout particulièrement lors d'activités spécialement sensibles durant les plages horaires élargies.

Les renforts en personnel accordés au SRC permettent d'accroître la qualité et la sécurité de l'informatique.

4.3 Gestion des risques

Le SRC dispose, depuis le mois de mars 2010 déjà, d'un document approuvé concernant la protection et la sécurité et qui constitue la base de la gestion des risques au SRC. Dans ce document sont identifiés les risques principaux ainsi que les méthodes, processus et structures à utiliser pour gérer ces risques. Des mesures visant à réduire les différents risques ont été identifiées et mises en œuvre déjà avant le vol de données. Après cet événement, les mesures et les processus ont été analysés en détail et des adaptations y ont été apportées. Outre l'introduction de mesures supplémentaires dans le but d'augmenter la sécurité, l'intégration de la gestion des risques au *controlling* du service a été améliorée. L'association de la gestion des risques aux différents échelons doit être formellement définie dans un document futur qui concernera la gestion des risques au SRC. En plus de cela, les contrôles ont été renforcés et leur fréquence augmentée.

4.4 Communication

La préparation de la communication interne et externe au sujet de cette affaire a immédiatement été une part essentielle de la collaboration entre le chef du DDPS et le directeur du SRC. Dans un premier temps, il a été délibérément décidé de renoncer à communiquer, étant donné qu'une procédure était en cours et que les dommages pour la Suisse avaient pu être évités, les données n'ayant pas été transmises à des tiers. L'objectif, fixé en accord avec les autorités de poursuite pénale et sur leur recommandation, était de ne pas rendre l'affaire publique.

Différentes variantes ont été évaluées en permanence pour la communication. Pour des raisons de confidentialité, et afin de prévenir toute indiscrétion, ces planifications n'ont pas été retenues par écrit ou enregistrées de quelque autre manière. Les mesures à prendre en cas de divulgation d'une source font partie des tâches essentielles de la gestion des sources. Une préparation spéciale n'est donc pas nécessaire. Jusqu'à ce jour, on a pu éviter que les données proprement dites soient rendues publiques.

Le DDPS a décidé de communiquer activement après avoir eu connaissance d'enquêtes de médias en cours. Il a publié, le 26 septembre 2012, un communiqué de presse dans lequel sont indiqués le vol de données, la réaction rapide du DDPS, le fait que l'ensemble des données a été retrouvé et que l'on a pu empêcher une fuite des données. A la demande de la Délégation des Commissions de gestion, le communiqué lui a été soumis avant la publication, afin qu'elle puisse prendre position. Le DDPS a ensuite modifié le communiqué conformément aux observations de la Délégation des Commissions de gestion.

5. Résultats des examens mandatés

5.1 Surveillance des services de renseignement DDPS

La Surveillance des services de renseignement (NDA) est un service interne à l'administration qui contrôle les activités du SRC en vérifiant le respect des prescriptions constitutionnelles et légales (légalité), la qualité et le bien-fondé des actions effectuées (opportunité) ainsi que l'atteinte des objectifs (efficacité). Ce service travaille sous l'autorité directe du chef du DDPS et est rattaché au Secrétariat général du DDPS.

Après avoir pris connaissance d'un rapport du SRC concernant le vol de données, le chef du DDPS a chargé, le 24 août 2012, la Surveillance des services de renseignement de rédiger un rapport afin d'éclaircir les points suivants : respect des directives et ordonnances importantes, appréciation des actions du SRC avant, pendant et après que le vol de données ait été commis, évaluation des mesures prises et planifiées ainsi que de la gestion des risques du SRC. La Surveillance des services de renseignement devait également recommander, le cas échéant, d'autres mesures permettant de réduire les risques.

La sécurité n'est pas l'élément principal

La Surveillance des services de renseignement a, par la suite, informé par oral et à plusieurs reprises le chef du DDPS sur les résultats intermédiaires de ses travaux. Dans son rapport final du 30 novembre 2012, elle constate que le problème n'est, en l'occurrence, pas principalement lié à la sécurité technique de l'information, mais à la réaction hésitante au niveau de la conduite du personnel. Il était toutefois difficile d'évaluer les intentions de X et la marge de manœuvre au niveau du droit du personnel était limitée. Elle relève des lacunes dans la gestion des risques au sein du SRC et l'absence de liens transversaux entre les risques stratégiques et les risques opérationnels. Elle indique de même que les personnes responsables pour la gestion des risques et des contrôles ne sont pas formellement désignées. Le rapport souligne l'importance d'une conduite coordonnée des processus transversaux de gestion des risques afin d'identifier ces derniers et trouver des solutions. Il note que les contrôles physiques, tels que l'inspection des bureaux sous la forme de contrôles ponctuels n'étaient jusqu'à maintenant effectués que de manière sporadique. Pour combler ces lacunes, le rapport conseille de renforcer les domaines de la sécurité et de l'informatique du SRC en augmentant le personnel.

La Surveillance des services de renseignement a présenté cinq recommandations au chef du DDPS concernant le SRC :

- Développer le dispositif dans le domaine de la gestion des risques (analyse et évaluation cohérentes des risques pertinents, intégration des différents niveaux de risques et formulation des contre-mesures correspondantes, développement de la sécurité et de l'informatique au SRC).
- Vérifier le positionnement de l'unité organisationnelle Sécurité au sein de la hiérarchie du SRC. Celle-ci doit pouvoir assumer sa fonction essentielle dans tout le service, de manière efficace et indépendante.
- Agir à temps et de manière résolue lors de difficultés avec le personnel, notamment en renforçant la collaboration avec le service du personnel et le service juridique.

- Augmenter la sécurité physique.
- Introduire des modifications formelles pour l'adaptation d'applications logicielles existantes et l'introduction de nouvelles applications.

Le chef du DDPS a transmis ces recommandations au SRC. Elles sont en train d'être mises en œuvre.

5.2 Protection des informations et des objets DDPS (PIO DDPS)

La Protection des informations et des objets est une unité organisationnelle du DDPS chargée de garantir la sécurité (des personnes, des informations, des biens et de l'environnement). Par conséquent, elle édicte également la majeure partie des directives de sécurité informatique au sein du DDPS.

Le 23 octobre 2012, le chef du DDPS a chargé la PIO d'élaborer des propositions concrètes concernant le renfort en personnel du domaine de la sécurité TIC au SRC, l'amélioration de la capacité de réaction du SRC et des solutions techniques supplémentaires visant à accroître la sécurité au SRC.

La PIO a relevé que les directives départementales en matière de sécurité informatique n'étaient pas mise en œuvre de manière optimale au SRC. Les systèmes qu'utilisait l'ancien SAP, et qui ont été repris lors du transfert du DFJP au DDPS, n'ont pas été suffisamment sécurisés. Dans le domaine TIC, le SRC ne dispose pas des ressources suffisantes, ce qui l'empêche d'assurer efficacement la sécurité. Afin d'améliorer cette situation, le SRC a engagé un responsable de la sécurité informatique (100 %) qui est entré en fonction au 1er novembre 2012 déjà. La PIO a en outre critiqué l'état de la mise en œuvre des bases juridiques de la Confédération par le SRC, appelant à une amélioration immédiate. Elle constate aussi que le SRC a déjà pris des mesures immédiates pour pallier cette lacune.

La PIO relève des besoins supplémentaires au niveau du personnel

Selon l'estimation de la PIO, le besoin supplémentaire en personnel dans les domaines de la sécurité et de l'informatique au SRC se monte à 7-12 postes à plein temps. Ceci doit permettre d'aménager des redondances pour les fonctions-clés, donnant ainsi les moyens de réagir immédiatement en cas d'irrégularités et d'instaurer le principe des quatre yeux. De plus, des adaptations devraient être apportées au niveau du droit du travail afin d'ouvrir la possibilité d'écarter, au besoin, des personnes exposées à des risques en les déliant immédiatement des tâches sensibles pour la sécurité. Finalement, des conditions de travail concurrentielles sont nécessaires. Il s'agirait d'apporter des améliorations aux structures de conduite et à la culture d'entreprise par une sensibilisation périodique aux questions de sécurité ainsi que d'améliorer l'instruction à ce niveau. La PIO constate également que le potentiel de solutions techniques n'est pas entièrement exploité, mais que si on voulait le faire, ce ne serait quasiment pas finançable.

Selon la PIO, il n'est pas totalement exclu qu'un tel vol puisse à nouveau avoir lieu à l'avenir. Elle retient toutefois qu'avec un investissement de moyens raisonnable, la probabilité que

cela se reproduise peut être réduite. Il faut cependant éviter que, par des contrôles de sécurité effectués de manière disproportionnée, une culture de la méfiance ne s'installe au SRC. Les mesures de sécurité doivent être adaptées à la menace ; elles doivent demeurer compréhensibles et transparentes, être soutenues et revues en permanence par la direction.

5.3 Nouvelle loi fédérale sur la sécurité des informations

Le 12 mai 2010, le Conseil fédéral a chargé le DDPS de rédiger, dans le cadre d'un groupe de travail interdépartemental incluant notamment le DFJP, le DFAE, le DFF et la ChF, un concept normatif ainsi que les bases formelles d'une loi fédérale sur la sécurité des informations. Le champ d'application des règles visant à assurer la sécurité des informations doit ainsi être élargi et concerner toutes les personnes qui, travaillant à la Confédération, se voient confier des informations classifiées. Un autre objectif est de donner un cadre légal uniforme pour l'application de la procédure concernant la sauvegarde du secret, valable dans les domaines militaire et civil. Le Conseil fédéral a lancé ce mandat après avoir constaté que le manque de cohérence actuel des bases légales présente un réel problème à l'application coordonnée de la sécurité des informations.

Afin de remplir le mandat et d'élaborer les bases de la nouvelle loi fédérale sur la sécurité des informations, le DDPS a réuni un groupe d'experts sous la direction de Markus Müller, professeur ordinaire en droit constitutionnel et administratif à l'Université de Berne. Suite au vol de données, le Conseil fédéral a apporté, le 24 octobre 2012, quelques modifications au mandat : outre l'élargissement du groupe d'experts existant à l'ensemble des départements et à la Chancellerie fédérale, il demande également une analyse des dangers ainsi que des propositions de mesures immédiates et de bases légales en vue d'améliorer la sécurité des informations au sein de la Confédération.

Rapport intermédiaire du groupe d'experts

Le 27 février 2013, le DDPS a présenté un rapport intermédiaire du groupe d'experts au Conseil fédéral. Ce document se réfère à l'ensemble de l'administration fédérale et ne se prononce donc pas spécifiquement sur le SRC. Il estime qu'il y a besoin d'agir dans les domaines de la conduite, de l'organisation, du personnel et de la technique. Les experts mettent en évidence le besoin immédiat d'instruire et de sensibiliser les cadres de l'administration (y compris au sommet de la hiérarchie) à la problématique de la sécurité des informations. Ils notent que des cadres bien formés et conscients du problème ainsi que des collaborateurs loyaux et satisfaits de leurs conditions de travail constituent le meilleur moyen de prévenir les dangers internes.

Compte tenu de ces remarques, le Conseil fédéral a chargé, le 15 mars 2013, le DFF, en sa qualité de département responsable des questions du personnel, de prendre des mesures de formation et d'information adaptées à l'échelon et de sensibiliser les cadres de l'administration fédérale aux questions de la sécurité des informations.

D'autres améliorations relatives à la sécurité entreront en vigueur avec la nouvelle loi fédérale sur la sécurité des informations.

5.4 Examen externe de la Surveillance des services de renseignement

Suite au vol de données et afin d'avoir un examen si possible complet de tous les acteurs concernés, le chef du DDPS a demandé qu'un examen externe des tâches, de l'organisation et des prestations de la Surveillance des services de renseignement soit effectué. Ce mandat a été confié au professeur Heinrich Koller, ancien directeur de l'Office fédéral de la justice. Son enquête avait pour but de mettre en évidence les tâches de la Surveillance des services de renseignement prescrites par le cadre légal et les directives du chef du DDPS, de présenter les tâches effectuées dans la pratique et d'évaluer les prestations de ce service. Elle devait également identifier si, en rapport à ces tâches, des changements étaient nécessaires au niveau des compétences et de l'organisation du service, ainsi qu'au niveau du nombre de collaborateurs, de leur profil ou du cahier des charges. Finalement, le professeur Koller devait aussi se prononcer sur une éventuelle nécessité d'adapter les bases légales.

Le professeur Koller a rendu son expertise début avril 2013 au chef du DDPS. Il est parvenu à la conclusion que la Surveillance des services de renseignement effectue ses tâches consciencieusement. Les trois collaborateurs sont des experts dans leur domaine respectif. Il n'y a pas de changement urgent à apporter à ce niveau. Les bases légales actuelles sont en principe suffisantes ; la nouvelle loi fédérale sur la sécurité des informations y apportera les précisions et compléments pertinents. Il note toutefois qu'il serait souhaitable d'apporter un complément aux fondements juridiques de l'indépendance de la Surveillance des services de renseignement. Parmi les points restreignant l'efficacité, le professeur Koller constate que l'action de ce service n'est pas toujours orientée vers un but précis et qu'elle manque parfois, en raison des ressources limitées, de la profondeur souhaitée.

Renfort en personnel de la Surveillance des services de renseignement

L'expertise du professeur Koller recommande au DDPS de renforcer immédiatement le service avec un quatrième poste occupé par un spécialiste TIC et/ou un spécialiste éprouvé des services de renseignement. La méthode du contrôle doit être améliorée, y compris le contrôle des certifications correspondantes. Elle préconise de développer une stratégie à long terme, d'identifier les risques politiques, de définir les lignes directrices stratégiques et de se concentrer sur les intérêts du mandant et des clients. La qualité du service peut être augmentée par la sensibilisation des personnes concernées aux problèmes et risques de l'activité de renseignement ainsi que par une formation continue méthodique.

Les contacts du service de Surveillance des services de renseignement et du chef du DDPS doivent être entretenus de manière régulière (au minimum toutes les deux semaines) et il s'agit de vérifier les concordances avec les points abordés lors des entretiens de conduite réguliers entre le chef du DDPS et le directeur du SRC. Les rapports établis par la Surveillance des services de renseignement doivent être complétés par une information régulière et permanente du chef du DDPS. La mise en œuvre des recommandations émises par le service doit être ordonnée à temps, avec une échéance fixée, ou être rejetée sur la base d'une motivation. La compréhension mutuelle des examinateurs et des personnes dont les tâches, les rôles et les processus sont examinés doit être améliorée, de même que la manière d'utiliser les résultats. Finalement, le professeur Koller suggère qu'un service permettant le *whistleblowing* soit aménagé pour les collaborateurs du SRC.

Les recommandations de l’expertise du professeur Koller ont été examinées à l’interne et un plan de mesures a été présenté au chef du DDPS. Il s’agit principalement de renforcer la fonction de la Surveillance des services de renseignement en tant qu’organe de contrôle et d’alerte du chef du DDPS, d’améliorer le contenu des rapports au chef du DDPS et d’en intensifier le rythme, d’optimiser la méthode du contrôle (en proposant notamment des formations ciblées) et d’augmenter le nombre de collaborateurs affectés aux tâches de surveillance. Le chef du DDPS discutera de ce rapport et des différentes mesures avec la Délégation des Commissions de gestion, à la demande de cette dernière, avant de prendre des décisions définitives.

6. Conclusion et prochaines étapes

Par son action rapide et ferme, le SRC a pu empêcher que les données volées soient transmises plus loin. Les mesures nécessaires pour analyser les circonstances du vol de données et accroître la sécurité intégrale ont été mises en œuvre sans attendre aussi bien à l'échelon du SRC, qu'à celui du département et du Conseil fédéral.

Une partie des quarante mesures que le SRC a édictées dans les domaines relevant de sa compétence se trouve actuellement encore en cours de mise en œuvre. L'affectation des nouveaux postes au SRC et à la Surveillance des services de renseignement est aussi un processus toujours en cours, de même que l'application des recommandations de la Surveillance des services de renseignement et du rapport Koller. La nouvelle loi fédérale sur la sécurité des informations, un projet ouvert déjà avant le vol de données, sera complétée par plusieurs éléments et les travaux vont être accélérés. Le projet de mise en consultation de cette loi doit être remis d'ici à la fin avril 2013. Les mesures mandatées par le Conseil fédéral concernant la formation et l'information des cadres de la Confédération relatives à la sécurité des informations seront mises en œuvre dès octobre 2013.

Il faut tenir compte du fait que le présent rapport reflète l'état des connaissances du DDPS au début du mois d'avril 2013. Une appréciation définitive ne pourra avoir lieu qu'après la remise du rapport de la Délégation des Commissions de gestion.

Il reste en outre à voir comment centrer davantage la gestion des risques à la Confédération sur les dangers relatifs à l'administration de données sensibles. Le SRC n'est, de loin, pas le seul service de l'administration fédérale à conserver des données particulièrement sensibles et à les traiter. Un vol de données au SRC a peut-être un côté plus spectaculaire, mais si des données venaient à disparaître dans un autre service, le potentiel de dommage serait aussi très important. Il est indiqué d'analyser ces dangers systématiquement et de prendre les mesures nécessaires partout dans l'administration fédérale. Avec ses 40 mesures édictées suite au vol, le SRC a effectué, en la matière, un travail de base qui pourrait s'avérer utile à l'ensemble de l'administration. On pourrait notamment examiner dans quelle mesure il serait judicieux de mettre en œuvre ces dispositions également à l'extérieur du SRC.

Concernant les contrôles de sécurité relatifs aux personnes, il est également nécessaire de procéder à certaines vérifications. Il s'agit notamment de se poser la question si les personnes ayant accès à des données personnelles particulièrement sensibles devraient subir un contrôle plus élargi et s'il est nécessaire d'introduire un rythme de contrôle plus serré. Même si dans le cas du vol de données présent rien ne prouve qu'un contrôle de sécurité relatif à la personne élargi avec audition aurait permis de formuler des réserves quant à la poursuite de l'activité de X, il ne fait aucun doute que l'intensification de tels contrôles contribue à augmenter la sécurité et à réduire largement les risques.

Du point de vue du DDPS, on peut conclure que le SRC a réagi rapidement et fermement suite au vol de données, qu'il a pris les mesures nécessaires, que celles-ci ont été mises en œuvre ou sont en train de l'être. Il s'agit d'examiner dans quelle mesure les autres services de l'administration fédérale devraient également développer leur gestion des risques et prendre les dispositions correspondantes.