Inspection de l'AS-Rens 22-18
Collecte de données par l'unité Cyber du SRC

Résumé

Rappel des faits et déroulement de l'inspection

En traitant de possibles cyberattaques, le SRC a collecté, entre 2015 et 2020, des renseignements protégés par le secret des télécommunications. Ces mesures de recherche sont soumises à autorisation et ne peuvent donc être mises en œuvre qu'après obtention de l'autorisation du Tribunal administratif fédéral.

En avril 2021, le directeur du SRC de l'époque a appelé l'AS-Rens pour l'avertir de possibles irrégularités commises par l'unité Cyber du SRC dans la recherche d'informations et de l'ouverture d'une enquête interne. L'AS-Rens a suivi l'enquête interne du SRC concernant ces évènements et le SRC l'a régulièrement informée de l'avancement des investigations. En outre, l'AS-Rens a reçu des informations complémentaires sur le fond de l'affaire.

À la suite de l'enquête interne, le DDPS a mandaté l'ancien juge fédéral Niklaus Oberholzer en 2022 pour conduire une enquête administrative. C'est pourquoi l'AS-Rens- à cette époque, a renoncé à lancer une propre inspection.

Une fois l'enquête administrative du DDPS conclue, l'AS-Rens a estimé que les incidents survenus dans l'unité Cyber avaient été largement éclaircis concernant la légalité de la recherche d'informations.

Par contre, de l'avis de l'AS-Rens, ni l'enquête interne du SRC, ni l'enquête administrative du DDPS n'avait éclairci des questions encore en suspens, comme les contacts et les informations échangées avec des entreprises privées.

En juin 2022, l'AS-Rens a donc lancé une inspection **visant à répondre aux questions encore en suspens concernant les événements survenus entre 2015 et 2020 au sein de l'unité Cyber du SRC. En outre, l'AS-Rens a également vérifié si les mesures prises par le SRC sous la forme d'ajustements des processus et de l'organisation de l'unité Cyber étaient appropriées et suffisantes pour garantir à l'avenir une collecte de données conforme au droit et appropriée.**

À cette fin, l'AS-Rens a notamment analysé un grand jeu de données (concernant les contacts et les informations échangées avec des entreprises privées) que ni l'enquête interne du SRC

ni l'enquête administrative du DDPS n'avaient examiné. Le SRC avait procédé à une sauvegarde forensique de ces données dans le cadre de l'enquête interne en 2021, mais avait décidé de ne pas les évaluer lui-même, principalement pour des raisons liées au droit du personnel. L'AS-Rens se considérait en revanche habilitée, en tant qu'autorité de surveillance, à analyser ce jeu de données.

L'inspection de l'AS-Rens a porté sur les faits concernant les événements dans le domaine cyber qui se sont produits jusqu'en 2021, ainsi que sur les mesures organisationnelles prises dans le même domaine jusqu'en mars 2023. Les entretiens avec le personnel et les cadres concernés ont eu lieu jusqu'en décembre 2022. L'AS-Rens a demandé des informations spécifiques sur certaines questions concrètes jusqu'au printemps 2024. Enfin, le SRC a eu la possibilité de commenter les résultats de l'inspection entre décembre 2024 et janvier 2025.

Résultats de l'analyse

Concrètement, l'AS-Rens a répondu aux questions suivantes.

1. Les faits pertinents pour l'évaluation des incidents survenus dans l'unité Cyber ont-ils été entièrement saisis ?
2. Comment le SRC assurera-t-il la légalité de l'analyse du trafic de données des fournisseurs à l'avenir ?
3. Les mesures organisationnelles prises par le SRC et les contrôles mis en place sont-ils adéquats et efficaces pour éviter que de tels incidents se produisent à l'avenir ?

1. Les faits pertinents pour l'évaluation des incidents survenus dans l'unité Cyber ont-ils été entièrement saisis ?

Tant l'enquête interne que l'enquête administrative ont conclu que les données traitées par l'unité Cyber dans le cadre de l'analyse des cyber incidents étaient presque exclusivement de nature technique et ne présentaient aucun lien avec des personnes. L'unité Cyber n'a pas besoin de rechercher des données personnelles ; ce qui l'intéresse, ce sont les procédures et les indicateurs techniques, qui sont totalement indépendants des personnes. Les données évaluées à la suite de cyberattaques ne peuvent pas être associées à une personne en particulier.

L'analyse par l'AS-Rens des données sauvegardées de manière forensique a toutefois également révélé que des données personnelles avaient été traitées et peut-être même échangées avec des services externes. Le jeu de données contenait entre autres des adresses IP[1], qui sont considérées comme des données personnelles du point de vue juridique. Selon l'art. 5, let. a, de la loi fédérale du 25 septembre 2020 sur la protection des

[1] Une adresse IP (adresse de protocole internet) est une suite de chiffres attribuée à chaque appareil connecté à un réseau informatique ou à internet.

données (LPD)[2], les données personnelles sont toutes les informations concernant une personne physique identifiée ou identifiable. Déjà dans son message de 1988 sur la LPD, le Conseil fédéral avait précisé que « […], si l'identification nécessite des moyens tels que, selon le cours ordinaire des choses, aucun intéressé ne les mettra en œuvre (p. ex. parce qu'il lui faudrait procéder à une analyse sophistiquée d'une statistique), on ne peut guère parler de possibilité d'identification »[3]. Conformément aux art. 37 et 38 de l'ordonnance du 15 novembre 2017 sur la surveillance de la correspondance par poste et télécommunication (OSCPT)[4], par exemple, le SRC a la possibilité d'obtenir des informations sur l'identification des utilisateurs d'adresses IP attribuées en Suisse de manière univoque ou non. Il ne doit donc pas déployer de gros efforts pour identifier les personnes concernées, du moins pour une partie des adresses IP traitées en Suisse. C'est pourquoi l'AS-Rens estime que ces adresses IP doivent être considérées comme des données personnelles dans l'environnement de travail du SRC.

Dans le cadre de ses activités de contrôle, l'AS-Rens a trouvé quelques rares indices d'une éventuelle transmission d'informations. L'analyse des données n'a cependant pas permis de clarifier cette question de manière approfondie et définitive. L'AS-Rens a **formulé une recommandation** visant à examiner les risques liés à la collaboration avec des services externes dans le domaine cyber.

2. Comment le SRC assurera-t-il la légalité de l'analyse du trafic de données des fournisseurs à l'avenir ?

Sur la base des conclusions de l'enquête interne, le SRC a pris diverses mesures d'urgence le 20 mai 2022. Pendant l'enquête, il avait déjà révisé les directives du 1er octobre 2021 concernant ses activités de renseignement dans le domaine cyber, lesquelles sont entrées en vigueur le 23 mai 2022. Contrairement à ce que prévoit le contenu révisé, le SRC n'a toutefois pas encore mis hors service le système de stockage dans lequel les données obtenues lors de cyberattaques étaient sauvegardées et traitées. Selon le SRC, le domaine Analyse technique cyber ne pourrait plus du tout faire son travail sans cette infrastructure, et l'unité Cyber ne pourrait plus que très partiellement s'acquitter de ses tâches. Le SRC a toujours l'intention de mettre cette infrastructure hors service, mais il faut d'abord trouver une nouvelle solution technique. Déjà le 15 décembre 2022, l'AS-Rens a adressé un courrier au SRC pour lui signaler que les mesures communiquées n'étaient toujours pas mises en œuvre. Le système utilisé pour le traitement des données cyber n'étant qu'une solution temporaire, il convenait de le remplacer par un système définitif. Dans ce contexte, l'AS-Rens a enfin formulée une **recommandation** au SRC pour qu'il traite cette question de toute urgence.

---

[2] RS 235.1
[3] FF 1988 II 421
[4] RS 780.11

Les actes d'inspection effectués par l'AS-Rens ont montré que les mesures d'urgence décidées et annoncées par le SRC n'étaient pas toutes mises en œuvre. Pour pallier les manquements dans la conduite de l'unité Cyber, constatés tant dans l'enquête interne que dans l'enquête administrative, il a fallu attendre 2024 pour que le SRC mette en place des instruments de conduite adéquats.

Le SRC n'a pas mis en place de nouveaux contrôles. Le principe de la double vérification n'est toujours pas appliqué en dehors de l'unité Cyber du SRC. Sur ce point, également, l'AS-Rens a **formulé une recommandation.**

L'AS-Rens a remarqué qu'il n'existait aucun règlement du personnel du SRC précisant les droits et les devoirs pour l'utilisation des appareils professionnels. Elle a **recommandé** au SRC de réglementer la distinction entre l'usage privé et l'usage professionnel et d'informer son personnel que les appareils du SRC, en cas de soupçon, pouvaient être mis en sécurité et faire l'objet d'une enquête.

3. Les mesures organisationnelles prises par le SRC et les contrôles mis en place sont-ils adéquats et efficaces pour éviter que de tels incidents se produisent à l'avenir ?

De manière générale, la recherche d'informations par le biais de mesures soumises à autorisation n'était pas au centre de cette inspection. D'après les actes d'inspection effectués dans le domaine Cyber, rien ne suggère que des informations sont encore obtenues illégalement auprès de fournisseurs d'accès.

Le SRC n'a pas toujours respecté les mesures qu'il s'était lui-même imposées, comme la mise en œuvre rapide des points soulevés dans le rapport d'échantillonnage de son propre service d'assurance qualité.

Compte tenu de l'ampleur de la recherche illégale d'informations par l'unité Cyber, constatée et analysée après plusieurs années, il était surprenant de constater que le SRC a renoncé à tout nouveau contrôle et s'appuie uniquement sur de nouveaux processus. Bien que ces derniers soient incontestablement nécessaires, il importe tout autant d'accorder une attention suffisante à leur respect. Jusqu'à la fin des actes d'inspection de l'AS-Rens en février 2024, tout portait à conclure que la direction de l'unité Cyber, dans le contexte très tendu du renseignement, n'aurait toujours pas su détecter à temps d'éventuels dysfonctionnements. Entre-temps, le SRC a procédé à une transformation et en janvier 2025 a pu montrer plausiblement les améliorations dans la conduite de l'unité Cyber. C'est pourquoi l'AS-Rens a décidé enfin de ne pas émettre de recommandation à ce sujet.