Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

**Secrétariat d'État à la politique de sécurité SEPOS
Service spécialisé de la Confédération pour la sécurité de l'information**

**Train de mesures pour éviter de nouvelles fuites de données
Autres domaines où il convient d'agir**

Résultats de l'atelier du 20 mars 2024
sur les recommandations en matière de sécurité des informations

---

Sur la base des recommandations du rapport du 28 mars 2024 résultant de l'enquête administrative sur la fuite de données, les préposés à la sécurité de l'information de la Chancellerie fédérale (ChF) et des départements, les prestataires internes de l'administration fédérale et des représentants de l'Office fédéral de la cybersécurité, de l'Office fédéral des constructions et de la logistique (OFCL) et d'armasuisse ont évalué la nécessité d'agir, en particulier auprès des fournisseurs, pour éviter de nouvelles fuites de données et ont élaboré des mesures ensemble. C'est le service spécialisé de la Confédération pour la sécurité de l'information, rattaché au Secrétariat d'État à la politique de sécurité (SEPOS), qui a animé cet atelier.

Les départements et les unités administratives ont appliqué des mesures d'urgence immédiatement après l'incident qui a touché l'entreprise Xplain. En outre, le Conseil fédéral a mis en vigueur la nouvelle loi sur la sécurité de l'information (LSI) le 1er janvier 2024, introduisant ainsi de nombreuses dispositions pour améliorer la sécurité de façon systémique et durable. Les mesures décrites ci-après ciblent les autres aspects sur lesquels il convient d'agir, en complément des dispositions déjà prises ou prévues dans la LSI.

L'administration fédérale civile et l'armée œuvrent actuellement à la concrétisation de la nouvelle législation. Le travail requis dans la phase initiale est élevé, car il s'agit d'induire des changements fondamentaux dans la gestion de la sécurité au sein de la Confédération. En l'absence de ressources supplémentaires, la marge de manœuvre des départements et des offices pour introduire de nouvelles mesures est faible. Les préposés à la sécurité de l'information des départements et de la ChF estiment tous que la mise en œuvre de la LSI doit être prioritaire.

Les mesures sont réparties en trois catégories : gestion de la sécurité, formation et sensibilisation, communication sécurisée avec des tiers.

## 1 Gestion de la sécurité

### 1.1 Clauses standards dans les contrats avec les fournisseurs

Les conditions générales de la Confédération et les clauses standards relatives aux menaces contre la cybersécurité sont souvent trop vagues pour spécifier avec les fournisseurs les besoins concrets en matière de sécurité découlant d'un mandat. C'est pourquoi le Secrétariat général (SG) du Département fédéral de la défense, de la protection de la population et des sports (DDPS) a ordonné, en 2022 déjà, l'élaboration de clauses contractuelles détaillées concernant la sécurité de l'information. Certaines d'entre elles doivent s'appliquer à toutes les acquisitions du département (clauses obligatoires), d'autres à des mandats spécifiques en fonction des besoins en matière

de protection des données (clauses facultatives). Le SEPOS (et plus particulièrement le service spécialisé de la Confédération pour la sécurité de l'information) émettra des recommandations concernant ces clauses conformément à l'art. 10, al. 3, de l'ordonnance sur la sécurité de l'information (OSI).

La conception de clauses standards s'est révélée difficile, car certaines directives techniques de sécurité font actuellement défaut ou sont compliquées à mettre en œuvre pour des tiers (p. ex. protection informatique de base de la Confédération). Les nouvelles directives fédérales doivent permettre une application tant par les prestataires internes que par les fournisseurs de prestations externes tout en étant compatibles avec les contrats signés. Ces exigences concernent aussi les cantons, qui doivent respecter la protection informatique de base de la Confédération lorsqu'ils accèdent aux systèmes de cette dernière.

Mesure 1

Le DDPS (SEPOS) est chargé d'élaborer d'ici fin 2024 des clauses contractuelles standards concernant la sécurité de l'information conformément à l'art. 10, al. 3, OSI.

Mesure 2

Le DDPS (SEPOS) est chargé d'élaborer d'ici fin 2024 des directives de sécurité pour la collaboration avec les fournisseurs. Il s'agit notamment de régler les aspects liés à la remise d'un accusé de réception pour les données transférées à des services externes à la Confédération et la suppression régulière et documentée des données opérationnelles de la Confédération présentes chez les fournisseurs.

### 1.2 Inventaire des relations avec les fournisseurs

L'enquête administrative sur la fuite de données au sein de l'entreprise Xplain a montré qu'une gestion active et efficace des fournisseurs était nécessaire. À moyen terme, dans deux ans, les départements et les offices pourront relier leurs objets à protéger (informations et systèmes d'information) et leurs fournisseurs dans l'application de gestion de la sécurité de l'information (SMSI) afin d'évaluer les risques et les dépendances qui en découlent. Cependant, l'administration fédérale ne peut pas attendre aussi longtemps pour avoir une meilleure vue d'ensemble de ses relations avec ses fournisseurs. Sur demande, l'OFCL est déjà en mesure de fournir des listes des relations contractuelles et financières que les unités administratives ont avec des prestataires.

Mesure 3

Les unités administratives sont chargées de compléter d'ici fin 2024 leur inventaire des objets à protéger avec les fournisseurs concernés. Le Département fédéral des finances (DFF / OFCL) met à disposition les listes des fournisseurs.

Mesure 4

La ChF et les départements sont chargés d'informer le DDPS (SEPOS) dans le cadre du rapport ordinaire 2024 quant à la mise en œuvre de la mesure visant à dresser l'inventaire des relations avec les fournisseurs.

### 1.3 Contrôles et audits

Les préposés à la sécurité de l'information estiment tous qu'il est urgent d'agir dans le domaine des audits. Il s'agit non seulement de surveiller l'application de la sécurité des informations chez les fournisseurs, mais aussi de réaliser des audits de sécurité internes. L'art. 13 OSI exige de toutes les unités administratives qu'elles fixent dans une planification annuelle de contrôle et d'audit la manière dont elles entendent vérifier la mise en œuvre de la sécurité de l'information dans leur domaine de compétences et chez les tiers. Les responsables de la sécurité de l'information des offices décident de la réalisation des audits. En termes d'efficience, il serait préférable de centraliser l'achat des prestations plutôt que de demander à chaque unité administrative de se procurer elle-même un soutien externe pour les audits. Il convient de charger l'OFCL d'acquérir, sur demande, des prestations d'audit pour l'ensemble des unités administratives. Par ailleurs, l'OSI précise que le service spécialisé de la Confédération pour la sécurité de l'information (SEPOS) répertorie les besoins de l'ensemble de l'administration fédérale en matière d'audits et autorise ce service à exécuter lui-même des audits. L'objectif est de consolider selon certaines priorités à l'échelle de la Confédération les audits réalisés auprès des prestataires internes et externes. C'est particulièrement important pour les fournisseurs soumis à la procédure de sécurité relative aux entreprises. La LSI prévoit que le service spécialisé chargé de mener la procédure de sécurité relative aux entreprises (SEPOS) assume la fonction de service d'assistance centralisé.

Mesure 5

En collaboration avec les services d'achats de la Confédération et les préposés à la sécurité de l'information, le DDPS (SEPOS) est chargé d'élaborer un plan permettant de réaliser des contrôles et des audits auprès des fournisseurs sur la base des obligations légales découlant de la LSI, et mettre ce plan en œuvre selon une approche fondée sur les risques.

Mesure 6

Le DFF (OFCL) est chargé d'acquérir, sur demande, des prestations d'audit pour l'ensemble des unités administratives.

### 1.4 Application SMSI

Pour que les départements et les offices puissent mettre en œuvre de façon efficiente les nouvelles directives, en particulier les dispositions de l'OSI concernant le SMSI, le DFF (Office fédéral de l'informatique et de la télécommunication, OFIT) et le DDPS (SG) collaborent afin d'acquérir et d'introduire une application SMSI standard

permettant de numériser les tâches et les processus de l'OSI. Les offices pourront employer l'application SMSI dès 2025. L'adjudication correspondante a été publiée sur SIMAP le 20 mars 2024.

L'application SMSI permettra de systématiser et de standardiser le recensement des informations et des systèmes d'information (ce qu'on appelle les *objets à protéger*). Elle consignera la participation de tiers (fournisseurs ou cantons) de façon systématique, évaluera les risques et documentera les mesures de sécurité. À moyen terme, le DDPS et le DFF veilleront à ce que les données concernant les fournisseurs puissent être extraites de collections de données disponibles (principe *once only*). Dans l'intervalle, l'OFCL met des listes à disposition en cas de besoin.

Si toutes les unités administratives utilisent l'application SMSI standard pour gérer leur sécurité, les départements et le SEPOS pourront notamment, d'un clic, obtenir une vue d'ensemble des objets à protéger, des fournisseurs ayant un lien avec la sécurité des informations, et de la progression de la mise en œuvre des mesures et des directives. Les préposés à la sécurité de l'information préconisent donc d'obliger l'ensemble des unités administratives à utiliser l'application SMSI. Il convient de compléter la législation fédérale sur la sécurité de l'information de façon appropriée.

Mesure 7

Le DDPS (SEPOS) est chargé d'examiner d'ici l'été 2025 s'il convient d'obliger les unités administratives (ChF, départements et offices) à utiliser l'application SMSI standard, une fois qu'elle sera disponible, pour la gestion de leur sécurité.

## 2 Formation

### 2.1 Concept de formation axé sur les besoins des titulaires de fonction

L'analyse des incidents de sécurité montre régulièrement que le personnel, à tous les échelons, ne connaît pas les directives en vigueur ou ne les applique pas de façon systématique. À titre d'exemple, on peut citer l'art. 11 de l'ordonnance sur la transformation numérique et l'informatique, qui règle l'accès aux données pour les fournisseurs externes de prestations. Les actions ponctuelles de formation et de sensibilisation menées après un incident sont souvent coûteuses et n'entraînent généralement pas d'amélioration durable de la sécurité. C'est pourquoi les mesures de formation doivent faire partie d'un concept global et durable. De plus, leur mise en œuvre et leur efficacité doivent faire l'objet d'une évaluation.

Il convient de charger le DDPS d'élaborer d'ici fin 2024, en collaboration avec la ChF et les départements, un concept de formation axé sur les besoins de différentes catégories de personnel (p. ex. responsables d'application, chefs de projet, rôles de projet tels que responsables de la sûreté de l'information et de la protection des données, cadres, collaborateurs en général, responsables de la sécurité de l'information, préposés à la sécurité de l'information) et de définir un calendrier pour la concrétisation des mesures de formation. Le département veillera à ce que l'efficacité de ces mesures soit contrôlée.

Mesure 8

Le DDPS (SEPOS) est chargé d'élaborer d'ici fin 2024, en collaboration avec la ChF et les départements, un concept de formation axé sur les besoins des différents titulaires de fonction et de définir un calendrier pour la concrétisation des mesures de formation. Son service spécialisé veillera à ce que l'efficacité de ces mesures soit contrôlée.

## 3 Communication sécurisée avec des tiers

L'administration fédérale dispose d'un service standard de communication vocale chiffrée (Threema) pour communiquer de manière sûre au niveau CONFIDENTIEL. Cependant, elle n'a pas de système de vidéoconférence sécurisé pour les échanges de groupe entre départements ou avec des partenaires externes aux niveaux CONFIDENTIEL ou SECRET. Or la nécessité d'un tel système a par exemple été mise en exergue lors de la pandémie de coronavirus. Les autorités fédérales doivent pouvoir communiquer entre elles et avec les cantons, les milieux industriels et les partenaires internationaux de manière sûre (données, voix, images, vidéos). C'est pourquoi la ChF prévoit de mettre à disposition d'ici l'été 2024, dans le cadre des services standards, une solution sécurisée de vidéoconférence fondée sur Webex qui pourra être utilisée jusqu'au niveau des données personnelles sensibles (projet *Secure Video Conferencing Service*).

Mesure 9

La ChF est chargée, après avoir consulté la Conférence des préposés à la sécurité de l'information, de soumettre à la Conférence des secrétaires généraux d'ici fin 2024 une vue d'ensemble des moyens de communication disponibles et de leur utilisation en fonction des différents niveaux de classification, en particulier pour les interactions avec des tiers.

Berne, le 3 avril 2024