_swissprivacy.law

Les résultats et les suites de l'enquête administrative dans l'affaire Xplain

Michael Montavon, le 17 juin 2024

> L'affaire Xplain a mis en évidence toutes les difficultés liées à la gestion d'un projet informatique complexe mené entre différents acteurs publics et privés. Plusieurs leçons ont pu être tirées pouvant certainement s'appliquer à d'autres situations comparables, quels que soient les acteurs concernés. Tour d'horizon des lacunes constatées et des mesures correctives proposées.

Enquête administrative « Fuite de données », rapport du 28 mars 2024 rédigé par Oberson Abels SA sur mandat du Conseil fédéral

Train de mesures pour éviter de nouvelles fuites de données, Résultat de l'atelier du 20 mars 2024 sur les recommandations en matière de sécurité de l'information, Département fédéral de la défense, de la protection de la population et des sports / Secrétariat à la politique de sécurité / Service spécialisé de la Confédération pour la sécurité de l'information

L'affaire Xplain

Au printemps 2023 , l'entreprise Xplain SA, fournisseur de logiciels dans le domaine de la sécurité, se fait dérober de grandes quantités de données qui finissent sur le Darknet. Le volume de données publiées s'élève à environ 1,3 million d'objets. Parmi ceux-ci se trouvent des données productives de l'administration fédérale, notamment des données confidentielles, des données personnelles (sensibles), des informations techniques, des informations classifiées ou des mots de passe.

En juin 2023, le PFPDT annonce qu'il a débuté au mois d'avril 2023 une procédure d'enquête préalable ayant révélé des indices de violations potentiellement graves des dispositions sur la protection des données. Il déclare sur cette base l'ouverture d'une procédure d'enquête formelle. Les résultats de la procédure d'enquête formelle sont révélés le 1er mai 2024 avec la publication, en allemand, de trois rapports contre Xplain, l'Office fédérale de la police (fedpol) et l'Office fédéral de la douane et de la sécurité des frontières (OFDF), accompagnés de diverses recommandations visant à réduire le risque de nouvelles violations de la protection des données.

Le PFPDT constate, en particulier, que ni fedpol ni l'OFDF n'ont clairement convenu avec Xplain si, et à quelles conditions, des données personnelles pouvaient être conservées sur les serveurs d'Xplain. Le processus en place était organisé de manière à ce que des données personnelles soient transmises à Xplain dans le cadre de prestations de support. Mais aucune exigence précise n'a été définie pour la transmission et le respect de la sécurité de ces données. La quantité de données transmise était, en outre, disproportionnée du point de vue du PFPDT. Finalement, Xplain n'a pas respecté les obligations d'un sous-traitant en matière de protection des données, ni certains engagements contractuels ayant été pris. Ces trois rapports ont fait l'objet d'un commentaire de David Vasella.

Parallèlement à l'enquête menée par le PFPDT, le Conseil fédéral ordonne le 23 août 2023 une enquête administrative visant à éclaircir les circonstances qui, du côté de l'administration fédérale, ont permis à Xplain SA d'entrer en possession de données de la Confédération. La tenue de cette enquête est confiée à l'étude d'avocats genevoise Oberson Abels SA. Sa mission est de déterminer i) si des déficiences en matière technique, d'organisation ou de processus ont conduit à ce que des données productives de l'administration fédérale soient en possession d'Xplain et (ii) si l'administration fédérale a satisfait à ses devoirs de manière adéquate lors du choix, de l'instruction et de la surveillance d'Xplain ainsi que dans le cadre de la collaboration avec celle-ci.

Les conclusions de l'enquête administrative sont rendues le 28 mars 2024. Le 1er mai 2024, le Conseil fédéral annonce que l'enquête administrative est désormais clôturée et adopte un train de mesures visant à éviter de futures fuites de données. Les travaux de mise en œuvre peuvent dorénavant être poursuivis dans les structures ordinaires de l'administration fédérale conjointement avec la mise en œuvre de la nouvelle loi fédérale sur la sécurité de l'information (LSI ; RS 128).

Le rapport d'enquête Oberson Abels

Selon le rapport d'enquête d'Oberson Abels SA, cinq unités administratives de la Confédération ont été directement touchées dans le cadre de l'affaire Xplain. Il s'agit de fedpol, de l'OFDF, de l'Office fédéral de la justice (OFJ), de la Police militaire (PM) et du Secrétariat d'état aux migrations (SEM).

Les principaux évènements ayant conduit à ce que des données productives de la Confédération soient présentes dans l'environnement informatique d'Xplain sont les suivants :

- Des employés d'Xplain ont transféré des données de l'administration fédérale reçues d'employés de la Confédération depuis leur compte de messagerie @admin.ch vers leur compte de messagerie Xplain ou ceux de leurs collègues. Dans un cas, un employé d'Xplain a probablement extrait lui-même des données d'un système de production de fedpol, les intégrant ensuite dans l'environnement informatique d'Xplain.
- Des employés de la Confédération responsables du support informatique interne ont traité des demandes de leurs collègues contenant des données de l'administration fédérale et les ont transmises ou mises à disposition d'Xplain sur un serveur partagé, sans retirer, pseudonymiser ou caviarder ces données.
- Des employés de la Confédération impliqués dans des travaux de développement, de test ou de migration informatique ont transmis des données à Xplain dans ce cadre.

Le rapport d'enquête met ensuite en évidence 10 lacunes ayant été constatées en termes d'organisation et de gestion :

- *Processus* : Des employés de la Confédération et d'Xplain ont pu extraire et envoyer des données par courriels sans encadrement ni respect du principe des quatre yeux. Selon ce principe, toute action critique ou sensible devrait être supervisée et approuvée par au moins deux personnes indépendantes.
- *Mesures techniques* : Aucune mesure technique n'a empêché l'extraction et l'envoi de données productives vers Xplain.
- *Formation et sensibilisation* : Les employés de la Confédération n'ont pas été suffisamment sensibilisés et formés aux enjeux du traitement des données. En outre, une faille de sécurité avait, certes, à un moment bel et bien été identifiée, mais l'information n'a pas circulé entre les unités administratives concernées.
- *Sécurité de l'information* : La Confédération a partiellement rempli ses devoirs de choisir et d'instruire Xplain, mais ne l'a pas suffisamment surveillé. Un concept de sécurité de l'information et de protection des données (concept SIPD) a certes été établi dans chaque cas, mais l'administration fédérale n'a jamais obtenu de rapport sur la sécurité de l'information au sein d'Xplain avant la fuite de données. En outre, aucun des contrats conclus avant juillet 2020 ne contenait de clauses spécifiques sur la sécurité de l'information.
- *Protection des données personnelles* : La Confédération n'a pas rempli ses devoirs de choisir, d'instruire et de surveiller lors de la sous-traitance de données personnelles à Xplain. En particulier, aucun contrat de sous-traitance des données au sens de l'art. 9 LPD (art. 10a aLPD) n'a été passé entre les unités concernées de l'administration fédérale et Xplain.

- *Gestion des cybermenaces* : Les unités de l'administration fédérale ont sous-estimé les risques posés par des tiers, en particulier par les fournisseurs de logiciels tiers (« supply chain security » et « third party cyber risk management »).
- *Répartition des responsabilités* : Il existe des divergences de compréhension, voire des positions contradictoires, sur la répartition des responsabilités en matière de sécurité de l'information entre les différentes parties impliquées de la Confédération (service d'achat central, métiers, Départements concernés, Centre de service informatique [CSI-DFJP], Office fédérale de l'informatique et de la communication [OFIT], collaborateurs spécialisés). Cette absence de compréhension uniforme des responsabilités entraîne des risques de conflits de compétence négatif.
- *Ressources* : Les ressources allouées à la sécurité de l'information sont globalement insuffisantes. A titre d'exemple, au moment des faits, la personne occupant la fonction de délégué à la sécurité de l'information auprès de fedpol était surchargée et attendait depuis un certain temps le renfort de deux postes supplémentaires. A l'OFJ, la même fonction ne représentait que 10% environ du cahier des charges d'une seule personne, ce qui est largement insuffisant.
- *Dépendance à l'égard d'Xplain* : Les unités administratives concernées de la Confédération se trouvaient par rapport à Xplain dans une situation de lock-in (sur cette notion : swissprivacy.law/301/). Selon leur analyse, il n'existait pas d'alternative à Xplain. Tout changement de fournisseur aurait impliqué de changer de système, ce qui aurait entraîné des difficultés techniques, des coûts disproportionnés et des retards.
- *Excès de confiance* : La relation entre les unités concernées de l'administration fédérale et Xplain reposait essentiellement sur la confiance (plutôt que sur le principe des quatre yeux). Plusieurs employés d'Xplain étaient « *onboardés* » auprès de la Confédération. Ils disposaient de matériels, d'adresses de messagerie électronique et de droits d'accès de l'administration fédérale, tutoyaient presque sans exception ses employés et utilisaient dans leur correspondance avec ces derniers des expressions laissant apparaître une certaine familiarité.

Ces constats ont abouti à l'élaboration d'une série de recommandations d'ordre à la fois organisationnel et opérationnel.

Sur le plan organisationnel, le rapport d'enquête critique, en partie, le système de responsabilité éclaté au sein de la Confédération, selon lequel chaque unité administrative est responsable de la sécurité et de la protection des informations qu'elle traite. Les interrogatoires menés dans le cadre de l'enquête administrative ont, en effet, mis en lumière un décalage entre i) la responsabilité attribuée aux unités administratives dans le domaine de la sécurité

et de la protection des données et ii) les connaissances dont elles disposent effectivement pour assumer cette responsabilité. Le rapport d'enquête recommande à ce niveau de prévoir une responsabilité accrue des unités spécialisées de la Confédération lors d'acquisition de moyens informatiques.

Sur le plan opérationnel, le rapport d'enquête formule une série de 10 mesures plus pratiques. Elles concernent notamment l'augmentation des ressources allouées à la sécurité et à la protection des données, la connaissance et la gestion des fournisseurs de services informatiques, la sensibilisation du personnel, l'effacement des données, la prise en compte le plus tôt possibles des questions de sécurité et de protection des données, et la mise en place de limitations techniques.

Le train de mesures adopté par le Conseil fédéral

Sur la base du rapport d'enquête administrative, le Conseil fédéral a adopté un train de mesures proposées par les services et le personnel spécialisés de l'administration fédérale. Ces mesures doivent être appliquées en complément des obligations de la LSI qui restent cependant prioritaires. Elles s'articulent autour de trois axes : i) gestion de la sécurité, ii) formation et sensibilisation et iii) communication sécurisée avec des tiers.

Le premier axe porte sur quatre aspects :

- L'élaboration de clauses contractuelles standardisées en matière de sécurité de l'information. Certaines clauses doivent s'appliquer à toutes les acquisitions de services informatiques (clauses obligatoires), tandis que d'autres uniquement à des situations spécifiques en fonction des besoins (clauses facultatives). L'élaboration de ces clauses est une concrétisation de l'art. 10 al. 3 de l'ordonnance sur la sécurité de l'information (OSI ; RS 128.1).
- La réalisation d'un inventaire des relations avec les fournisseurs. Le but est que les départements et les offices fédéraux puissent aisément relier leurs objets à protéger et leurs fournisseurs, et évaluer les risques et les dépendances qui en découlent. Actuellement, un tel inventaire est réalisé au moyen de listes, mais il pourra être réalisé dans un délai de deux ans au moyen d'une application de gestion de la sécurité de l'information (SMSI).
- Une meilleure gestion des prestations de contrôle et d'audit. Selon l'art. 13 OSI, toutes les unités administratives doivent elles-mêmes fixer la manière dont elles entendent vérifier la mise en œuvre de la sécurité de l'information dans leur domaine de compétences et chez leurs fournisseurs. En termes d'efficience, il est néanmoins préférable de

centraliser l'achat de prestations d'audit. C'est pourquoi l'Office fédéral des constructions et de la logistique (OFCL) acquerra, sur demande, des prestations d'audit pour l'ensemble des unités administratives.
- L'utilisation élargie d'une application SMSI au sein des unités administratives de l'administration fédérale. Actuellement, l'art. 47 OSI prévoit uniquement la « possibilité » pour les unités administratives d'utiliser une application SMSI pour gérer la sécurité de leurs informations. L'introduction d'une obligation généralisée d'utiliser une application SMSI commune à toute l'administration fédérale permettrait de systématiser et de standardiser le recensement des informations et des systèmes d'information à protéger. C'est pourquoi, la Confédération analysera d'ici l'été 2025 si la LSI doit être modifiée afin de rendre obligatoire l'utilisation d'un SMSI standard.

Le deuxième axe se concentre sur l'élaboration d'un concept de formation spécifiquement axé sur les besoins de chaque fonction (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). Il est, en outre, prévu de procéder à une évaluation ultérieure de l'efficacité du concept de formation.

Le troisième axe traite finalement de la communication sécurisée avec des tiers. L'administration fédérale veut acquérir une solution sécurisée de vidéoconférence permettant d'échanger des données en fonction des différents niveaux de classification.

Commentaire

Les enquête du PFPDT sont prévues à l'art. 49 LPD. Le PFPDT ouvre d'office ou sur dénonciation une enquête contre un organe fédéral ou une personne privée si des indices suffisants font penser qu'un traitement de données pourrait être contraire à des dispositions de protection des données.

Prévue aux art. 27a ss de l'ordonnance fédérale sur l'organisation de gouvernement et de l'administration (OLOGA ; RS 172.010.1), l'enquête administrative n'est pas dirigée contre un office ou des personnes déterminées, mais vise uniquement à établir si un état de fait exige une intervention pour sauvegarder l'intérêt public.

Dans un cas, comme dans l'autre, les deux enquêtes mettent en évidence l'absence de contrat de sous-traitance des données en violation de l'art. 9 LPD (10a aLPD). Cette conclusion est toutefois critiquée par Xplain dans le rapport d'enquête du PFPDT. Cette dernière

conteste agir en qualité de sous-traitant, car son contrat ne consisterait pas à héberger ou à traiter des données de l'administration fédérale, mais uniquement à développer des logiciels destinés à être exploités par des organes de l'administration fédérale eux-mêmes. Dans le cadre de cette activité, Xplain ne traiterait pas directement des données personnelles pour le compte de la Confédération, mais offrirait simplement des services de maintenance, de soutien et de développement logiciel.

Comme l'indique justement le PFPDT, la transmission de données personnelles reste pertinente, même lorsqu'elle ne représente qu'un effet secondaire de l'exécution du contrat. La publication en masse sur le Darknet de données de la Confédération dérobées à Xplain parle d'elle-même. Sauf à admettre que ces données aient été collectées ou communiquées de manière illicite (ce qui soulèverait un autre problème), cela implique l'existence d'une relation de sous-traitance, laquelle aurait dû être réglée au moyen d'un contrat de sous-traitance des données. L'existence d'une responsabilité distincte, voire d'une responsabilité conjointe sur des données productives, semble difficile à argumenter dans un tel cas. Comme l'a souligné l'enquête administrative, la nature des prestations confiées à Xplain relève ici intégralement de l'administration auxiliaire (« Bedarfsverwaltung ») sans qu'il y ait transfert d'une tâche de l'administration à proprement parler. Une responsabilité distincte peut, en revanche, être admises s'agissant des données des employés de la Confédération qu'Xplain a pu récolter dans le cadre de l'exécution du contrat ou encore s'agissant des données techniques relatives à l'utilisation des logiciels fournis, ces données n'étant pas des données productives de la Confédération.

Même si l'enquête administrative a permis de mettre en évidence plusieurs éléments importants en termes de sécurité et de gouvernance des données, un des manquements le plus significatif dans cette affaire demeure certainement l'absence de contrat de sous-traitance des données. Un tel contrat n'aurait pas empêché l'attaque contre Xplain, mais il aurait facilité une meilleure gestion des risques. Si les autorités fédérales avaient considéré la transmission de données à Xplain et l'avaient encadrée par un contrat de sous-traitance, il est probable que : i) la quantité de données transmises à Xplain et ultérieurement divulguées sur le darknet aurait été réduite et ii) des mesures de sécurité accrues auraient été implémentées. La conclusion d'un contrat de sous-traitance des données n'est pas une exigence nouvelle, mais elle a parfois été négligée par le passé. Dorénavant, les responsables du traitement devraient penser à conclure un tel contrat systématiquement dans le cadre de toute acquisition de prestations informatiques où des données personnelles productives du responsable du traitement sont susceptibles d'être transmises au prestataire.

Proposition de citation : Michael Montavon, Les résultats et les suites de l'enquête administrative dans l'affaire Xplain, 17 juin 2024 *in* www.swissprivacy.law/306

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.