Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Office fédéral de la cybersécurité OFCS

26 juin 2024

Rapport sur la sécurité informatique de la Confédération en 2023

Sommaire

1 Introduction 3

2 État de la sécurité informatique dans l'administration fédérale 3

2.1 Organisation de la sécurité informatique dans l'administration fédérale 4
2.2 Résultats des exigences de conformité des documents de sécurité 5

3 Incidents de sécurité 5

3.1 Attaques DDoS 5
3.1.1 Attaque DDoS du groupe *NoName* contre l'administration fédérale 5

3.2 Attaques par rançongiciel 6
3.2.1 Attaque contre l'entreprise Xplain AG 6
3.2.2 Autres incidents de sécurité semblables 8

3.3 Problèmes de sécurité chez des fournisseurs de solutions en nuage 8
3.3.1 Diffusion de logiciels malveillants via Microsoft Teams 8
3.3.2 Attaque menée par le collectif Storm-0558 dans le Microsoft Cloud 9

4 Activités et mesures 9

4.1 Programmes de primes aux bogues 9
4.2 Mesures de formation 10
4.2.1 Campagne nationale de sensibilisation à la cybersécurité S-U-P-E-R 10
4.2.2 Cours pour les experts 10
4.2.3 Formation sur la sécurité informatique (compliance) 10

4.3 Défis en matière de formation 11
4.3.1 Formation des prestataires externes 11
4.3.2 Formation des responsables des objets protégés 11

5 Conclusions et perspectives 11

5.1 Recommandations 11
5.2 Perspectives 12
5.2.1 Mesures prévues pour 2024 12
5.2.2 Prochains rapports 12

1 Introduction

L'Office fédéral de la cybersécurité (OFCS) rend compte au Conseil fédéral de l'état de la sécurité de l'information de la Confédération à la fin 2023, conformément à l'art. 11, al. 2, de l'ordonnance sur les cyberrisques[1] en vigueur durant la période sous revue. Après l'entrée en vigueur de la nouvelle loi sur la sécurité de l'information, cette tâche sera confiée au Secrétariat d'État à la politique de sécurité (SEPOS) à partir de l'exercice 2024[2] (cf. chap. 5.2.2).

Le présent rapport s'appuie sur une enquête structurée portant sur l'état de la sécurité informatique réalisée auprès de tous les délégués à la sécurité de l'information des départements et de la Chancellerie fédérale. Il prend également en considération les signalements et rapports sur la sécurité établis par les fournisseurs de prestations internes à la Confédération. L'OFCS évalue la sécurité de l'information au sein de la Confédération sur la base de ces données.

L'année 2023 a été marquée par plusieurs cyberincidents qui ont mis l'administration fédérale à rude épreuve : attaques du groupe d'hacktivistes prorusses *NoName057(17)* pour limiter la disponibilité des moyens informatiques de l'administration fédérale, fuite de données chez des prestataires de la Confédération (notamment l'entreprise Xplain AG) et incidents de sécurité chez des fournisseurs de solutions en nuage. Pour traiter la fuite de données chez Xplain AG, le Conseil fédéral a ordonné une enquête administrative. Celle-ci comprend des recommandations pour éviter ce type d'incidents à l'avenir. Le présent document ne fournit pas une analyse des mesures potentielles dans ce domaine, car l'enquête administrative a été publiée avant le rapport.

Le deuxième chapitre présente l'état actuel de la sécurité informatique dans l'administration fédérale au cours de l'exercice 2023, l'organisation de la sécurité informatique dans l'administration fédérale et les résultats du sondage sur les exigences de conformité pour les documents de sécurité.

Le troisième chapitre aborde les incidents de sécurité les plus graves qui ont touché l'administration fédérale l'an dernier.

Le quatrième chapitre s'intéresse aux principales activités et mesures au sein et en dehors de l'administration fédérale.

Enfin, le cinquième chapitre comprend un résumé des principales conclusions du rapport et quelques perspectives.

2 État de la sécurité informatique dans l'administration fédérale

Les risques et les tentatives d'attaques contre l'informatique de l'administration fédérale et de ses prestataires externes ne cessent d'augmenter, notamment en raison des tensions géopolitiques actuelles.

Les incidents qui sont survenus au cours de l'année sous revue ont entre autres montré à quel point la gestion des fournisseurs était importante pour la cybersécurité. Des lacunes apparaissent au niveau de la gouvernance des données dans toute la Confédération et de la vue d'ensemble des relations d'affaires avec les partenaires externes. Autrefois, il était

[1] Ordonnance du 27 mai 2020 sur la protection contre les cyberrisques dans l'administration fédérale (ordonnance sur les cyberrisques, OPCy ; RS 120.73), remplacée le 1er janvier 2024 par l'ordonnance sur la sécurité de l'information (OSI ; RS 128.1).

[2] https://www.admin.ch/gov/fr/start/dokumentation/medienmitteilungen.msg-id-98807.html

difficilement possible de contrôler la cybersécurité chez les fournisseurs et sur les logiciels livrés. Dans les deux cas, la responsabilité est centralisée : c'est l'unité administrative qui effectue les achats qui répond de l'élaboration des contrats et de la réception des produits. Par conséquent, les normes de sécurité ne sont pas homogènes.

En outre, quand il s'agit de gérer un incident impliquant plusieurs niveaux étatiques, comme dans le cas de Xplain AG, il s'est avéré que si les processus requis étaient plus ou moins bien rodés au sein de l'administration fédérale, ceux avec les cantons n'étaient même pas encore définis.

Les incidents qui se sont produits en 2023 ont montré que la conformité ne suffisait pas pour garantir la cybersécurité. Par ailleurs, les responsables des objets protégés doivent améliorer leurs compétences en matière de cybersécurité pour être aussi capables d'évaluer et de mettre en œuvre correctement les mesures requises pour la conformité (cf. chap. 4.3.2).

2.1 Organisation de la sécurité informatique dans l'administration fédérale

La sécurité informatique dans l'administration fédérale comprend toutes les mesures destinées, d'une part, à prévenir les cyberincidents, d'autre part, à identifier et gérer rapidement ceux qui surviennent néanmoins. Conformément à l'art. 5, let. d, de la révision du 29 septembre 2023 de la loi sur la sécurité de l'information[3], on entend par cyberincident *un événement survenant lors de l'utilisation de moyens informatiques et ayant pour conséquence une atteinte à la confidentialité, à la disponibilité ou à l'intégrité d'informations ou à la traçabilité de leur traitement*.

Le Conseil fédéral édicte des ordonnances et des directives propres à assurer la mise en œuvre des mesures qui s'imposent pour garantir la sécurité informatique dans toute l'administration fédérale. Jusqu'à présent, les directives relatives à la sécurité informatique étaient élaborées par le Centre national pour la cybersécurité (NCSC), qui a été transformé en office fédéral et rattaché au Département fédéral de la défense, de la protection de la population et des sports (DDPS) au 1er janvier 2024. Le Secrétariat général du DDPS était quant à lui chargé jusqu'ici d'établir les directives relatives à la sécurité de l'information pour l'administration fédérale. Dorénavant, ces directives seront rassemblées et édictées par le service spécialisé chargé de la sécurité de l'information au sein du SEPOS[4].

Les unités administratives sont responsables du respect et de la mise en œuvre des directives de sécurité informatique qui relèvent de leur domaine de compétences. À cet effet, elles examinent régulièrement les objets informatiques à protéger[5] et prennent les mesures de sécurité requises.

[3] FF 2023 2296 (projet de référendum)

[4] https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-98807.html

[5] Applications, services, systèmes, réseaux, fichiers de données, infrastructures et produits relevant de l'informatique ; plusieurs objets identiques ou connexes peuvent être regroupés en un seul objet informatique à protéger (art. 3, let. h, OPCy).

2.2 Résultats des exigences de conformité pour les documents de sécurité

Sur les 2176 objets à protéger recensés au total, 81,8 % possèdent des documents de sécurité valables. Les mesures de sécurité qui en découlent et leur contrôle étaient en outre garantis pour 74,4 % de tous les objets à protéger (contre 72,5 % en 2022).

Pour que les mesures de sécurité puissent être mises en œuvre correctement, les documents de sécurité nécessaires doivent être à jour (ils doivent dater de moins de cinq ans). Cette exigence est remplie pour 92 % des documents de sécurité valables (sur les 81,8 % cités précédemment). En comparaison avec l'année précédente (92,6 %), le recul reste extrêmement faible et s'explique par le fait que de nombreux documents ont dépassé la durée de validité de cinq ans en 2023. Ces derniers étaient entrés en vigueur en 2018 et les départements ont maintenant des difficultés à les mettre à jour en même temps. Les chiffres montrent cependant à l'OFCS que le recensement des objets à protéger et la mise en œuvre des mesures de sécurité par les unités administratives sont restés à un niveau comparable à celui de 2022.

De manière générale, les chiffres annoncés sont trop bas et mettent en évidence un problème au niveau de la conformité. Ces chiffres ne permettent pas non plus de déterminer clairement si la qualité des documents de sécurité informatique a été vérifiée de manière approfondie ni s'ils ont fait l'objet d'un examen critique. Même des documents à jour ne garantissent pas que les mesures de sécurité ont été introduites et contrôlées correctement. L'OFCS ne dispose pas des outils nécessaires pour mener des audits. De nouvelles solutions doivent être examinées dans le cadre de la loi sur la protection de l'information.

3 Incidents de sécurité

Les incidents de sécurité peuvent avoir des conséquences graves, comme la divulgation d'informations confidentielles, des actes de sabotage, des tentatives de chantage ou la défaillance de systèmes critiques. Les incidents de sécurité qui ont eu des répercussions importantes pour l'administration fédérale au cours de l'exercice 2023 sont présentés dans les chapitres 3.1 à 3.3.2.

3.1 Attaques DDoS

Les attaques DDoS (*attaques par déni de service distribué*) sont dirigées contre les ressources du réseau jusqu'au serveur cible. Elles sont menées par des cybercriminels ou des acteurs étatiques qui profitent des limites de capacités qui touchent chaque ressource du réseau. Ces attaques ont pour but de paralyser les ressources ciblées en leur envoyant de très nombreuses requêtes, ce qui provoque une surcharge des capacités de traitement. Le nombre de requêtes dépasse la limite de capacité de la ressource visée. Les réponses sont beaucoup plus lentes que d'habitude et certaines requêtes des utilisateurs ne sont pas traitées.

3.1.1 Attaque DDoS du groupe *NoName056(16)* contre l'administration fédérale

À partir du 7 juin 2023, un groupe d'hacktivistes prorusses a lancé des attaques DDoS contre des cibles en Suisse sous le nom de *NoName057(16)*. Le site internet du Parlement (www.parlement.ch) a été le premier à être touché. Le collectif a justifié les attaques par l'annonce du discours du président ukrainien Volodymyr Zelensky et les discussions menées

au Parlement suisse sur les exportations d'armes.

Les attaques ont duré près de deux semaines et ont visé différentes cibles. Elles ont cessé le 19 juin lorsque les hackers se sont concentrés sur de nouveaux objectifs à l'étranger.

Cibles	Date						
	12.06.2023	13.06.2023	14.06.2023	15.06.2023	16.06.2023	17.06.2023	18.06.2023
Administration fédérale	4	1		1		2	
Cantons			2		3		
Villes			6				6
Service public	2		1	1			1
Aéroports		8				6	
Secteur financier				5		2	1
Autres				1	3		
Armement				1			
Total 57	**6**	**9**	**9**	**9**	**6**	**10**	**8**

Tableau : liste récapitulative des attaques DDoS menées avec succès

Les attaques étaient d'une telle ampleur qu'elles ont mis en difficulté toutes les organisations touchées et l'administration fédérale a dû engager d'importants moyens pour les combattre.

En cas d'attaque DDoS, l'administration met tout en œuvre pour garantir le fonctionnement des applications internes, même si les systèmes accessibles depuis l'extérieur sont surchargés et ne peuvent plus répondre correctement aux requêtes. Cela n'a pas été le cas lors de cette attaque. D'importants systèmes internes dépendaient des services de systèmes externes, ce qui a engendré des restrictions de travail pendant quelques heures. Le NCSC a publié un rapport d'analyse détaillé sur ces attaques DDoS en novembre 2023 (cf. annexe)[6].

Les conséquences des attaques par rançongiciel contre des entreprises ou les autorités ont quant à elles des conséquences beaucoup plus graves que les attaques DDoS. Elles sont expliquées en détail au chapitre 3.2.

3.2 Attaques par rançongiciel

L'attaque par rançongiciel consiste à voler et à chiffrer les données et les fichiers de la victime. Les cybercriminels exigent ensuite le paiement d'une rançon, d'une part pour déverrouiller les données et d'autre part pour empêcher leur divulgation (c'est ce qu'on appelle une *attaque par rançongiciel à double extorsion*). Si la victime ne paie pas la rançon, elle prend le risque que les données volées soient publiées sur le darknet. Les attaques par rançongiciel peuvent viser des entreprises ou des autorités, mais aussi des particuliers, dont les données font souvent partie des dommages collatéraux de ces attaques.

3.2.1 Attaque contre l'entreprise Xplain AG

L'attaque par rançongiciel menée contre l'entreprise Xplain AG, un prestataire important de différentes unités administratives et de plusieurs cantons, a conduit à la fuite de 431 GB de données : 146 623 fichiers et 19 863 dossiers étaient concernés. Il s'agissait entre autres de

[6] https://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/berichte/fachberichte/ddos-bericht-6-2023.html

données importantes pour la sécurité et de données personnelles provenant notamment du domaine de la sécurité intérieure. Les cybercriminels ont publié les données volées sur le darknet, les rendant ainsi accessibles à des tiers. La divulgation de données confidentielles ou liées à la sécurité a de graves conséquences et génère une grande charge de travail. Des mesures d'urgence ont dû être définies et mises en œuvre afin de limiter les risques immédiats et d'informer les personnes concernées. Il a également fallu évaluer si des systèmes ou des banques de données de l'administration fédérale étaient compromis.

Cet incident a entravé l'arrêté temporaire de systèmes primordiaux. De plus, d'importantes ressources en personnel ont été engagées pour déterminer quels offices étaient clients de l'entreprise Xplain AG et définir la nature de leurs relations contractuelles, les droits d'audit existants et la durée des contrats.

Il faut dans un premier temps examiner l'incident en détail. Le Conseil fédéral a publié les résultats de l'enquête administrative le 1er mai 2024. Le Préposé fédéral à la protection des données a rendu public son rapport le même jour.
Le rapport d'enquête établit qu'au cours des dernières années, des données productives de la Confédération ont été transmises activement à l'environnement informatique de Xplain AG dans de rares cas. Ces transmissions sont intervenues lors de phases de test et d'intégration d'un logiciel ou dans le cadre de services de maintenance ou d'assistance et ont été effectuées aussi bien par des employés de Xplain AG qui disposaient d'un compte de messagerie de la Confédération que par des collaborateurs de l'administration fédérale. En outre, une fonctionnalité d'assistance intégrée à certaines applications développées par Xplain et désactivée entre-temps a entraîné le transfert de grandes quantités de données de l'environnement informatique de la Confédération vers celui de Xplain AG. Le Conseil fédéral s'est basé sur ce rapport pour établir un train de mesures visant à éviter de futures fuites de données (cf. chap. 5.2.1).

Le NCSC a coordonné la gestion de l'incident, défini des mesures pour le rétablissement de la sécurité des systèmes et procédé à une analyse complète de toutes les données publiées, avec le soutien de ressources internes et externes. Afin de contribuer au traitement de l'incident et d'assurer la plus grande transparence possible, il a publié un rapport sur la procédure et les résultats de l'analyse des données[7].

L'attaque par rançongiciel contre l'entreprise Xplain AG illustre parfaitement à quel point déterminer l'ampleur des dommages après une fuite de données peut rapidement devenir très coûteux. Ces coûts auraient toutefois pu être évités si on connaissait dès le début les données détenues par le fournisseur et la liste des clients de l'entreprise Xplain AG. Cet incident a en outre permis de révéler que la gestion de l'incident à plusieurs niveaux étatiques n'était pas normalisée. Si les processus étaient plus ou moins rodés au sein de l'administration fédérale, ceux avec les cantons n'étaient même pas encore définis. Une procédure standard et une évaluation uniforme pour classer la gravité d'un incident seront définis sur la base de cette expérience. Par ailleurs, le contrôle effectué au moment de la réception des logiciels était insuffisant. En effet, personne n'avait par exemple remarqué que la fonction du rapport d'erreur envoyait des données sensibles à Xplain AG.

[7] https://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/berichte/fachberichte/bericht-datenanalyse-xplain.html

3.2.2 Autres incidents de sécurité semblables

3.2.2.1 Attaque par rançongiciel contre arb architectes SA

Le 21 juillet 2023, l'Office fédéral des constructions et de la logistique (OFCL) a été informé d'une attaque menée contre le sous-traitant arb architectes SA. Le groupe de hackers *Abyss* avait détourné près de 220 GB de données non compressés, dont des plans de construction d'ambassades suisses et de résidences à l'étranger, pour les publier sous forme chiffrée sur le darknet. L'entreprise a pu récupérer les données chiffrées et a déposé une plainte pénale. La clé permettant de déchiffrer les documents volés a été publiée après l'échéance du délai de paiement de la rançon le 1er septembre 2023.

3.2.2.2 Attaque contre l'entreprise Concevis AG

Le 14 novembre 2023, une autre entreprise informatique suisse, Concevis AG, a été la cible d'une attaque par rançongiciel. Les hackers ont chiffré tous les serveurs de l'entreprise et dérobé les données qu'ils contenaient, dont probablement des données opérationnelles de l'administration fédérale. Les services concernés ont été informés rapidement et ont pu prendre des mesures d'urgence pour minimiser les risques pour la sécurité de l'administration fédérale. Les applications développées par Concevis sont utilisées par des fournisseurs de prestations de l'administration fédérale. Une compromission des systèmes de la Confédération est actuellement peu probable. Les conséquences de cette attaque ne sont cependant pas encore toutes connues aujourd'hui.

3.3 Problèmes de sécurité chez des fournisseurs de solutions en nuage

Les erreurs de configuration et les lacunes de sécurité chez des fournisseurs de solutions en nuage peuvent entraîner des fuites de données et des attaques. En effet, les hackers peuvent profiter des failles de sécurité qui n'ont pas été corrigées et des erreurs de configuration dans les environnements en nuage pour s'introduire dans les systèmes. Les deux problèmes de sécurité concernant l'environnement en nuage dont il est question dans ce chapitre n'ont pas eu de conséquences directes pour l'administration fédérale. Ils sont toutefois susceptibles d'ébranler la confiance de la population à l'égard des solutions en nuage utilisées par la Confédération. Il faut tirer les enseignements de ces incidents et les prendre en compte dans le développement de mesures de sécurité relatives aux solutions en nuage.

3.3.1 Diffusion de logiciels malveillants via Microsoft Teams

L'administration fédérale s'est aperçue que des utilisateurs externes pouvaient envoyer des pièces jointes aux collaborateurs de l'administration fédérale via les messages de chat dans Microsoft Teams. Ces annexes ne font pas l'objet d'une recherche automatisée de code malveillant dans Microsoft Teams. Lors d'un test, le Computer Security Incident Response Team (CSIRT) de l'Office fédéral de l'informatique et de la télécommunication (OFIT) a constaté que les fichiers étaient identifiés et supprimés par la protection antivirus au moment de la sauvegarde seulement. Cela signifie que contrairement à la pratique actuelle, les collaborateurs de la Confédération n'ont pas de deuxième ligne de défense contre les logiciels malveillants lorsqu'ils utilisent Teams et que les appareils de la Confédération sont uniquement équipés d'une protection locale contre les logiciels malveillants.

3.3.2 Attaque menée par le collectif *Storm-0558* dans le nuage Microsoft

Le 11 juillet 2023, Microsoft a informé dans deux articles de blog qu'une autorité gouvernementale américaine avait découvert que des courriels dans Exchange Online et Outlook.com avaient été la cible d'attaques, mais que celles-ci avaient cependant pu être interrompues dans l'intervalle. Ces attaques ont probablement été menées par *Storm-0558*, un groupe de hackers étatiques chinois. À partir du 11 mai 2023, les pirates ont pu accéder aux courriels d'environ 25 autorités gouvernementales, pour la plupart européennes. Ils ont en outre eu accès aux comptes de messagerie privés de plusieurs collaborateurs de ces services. Les cybercriminels ont pu falsifier les jetons d'authentification[8] utilisés pour les accès à l'aide d'une clé de signature dérobée. Ils auraient pu employer le même procédé pour compromettre d'autres services du nuage M365[9]. Ces attaques ont été découvertes le 16 juin 2023 et Microsoft a rapidement corrigé les failles. L'administration fédérale n'a pas été touchée par cet incident.
Il démontre toutefois que la gestion sécurisée des clés constitue un défi de taille, même pour une grande entreprise. Il confirme en outre que l'administration fédérale a pris la bonne décision en renonçant à utiliser les possibilités de chiffrement du nuage Microsoft.

4 Activités et mesures

4.1 Programmes de primes aux bogues

Au cours de l'exercice 2023, le NCSC a organisé des programmes de primes aux bogues pour plusieurs services et applications dans différentes unités administratives. Le NCSC a par ailleurs lancé son propre programme de primes aux bogues à l'été 2023. Il l'a développé progressivement pour donner aux pirates éthiques la possibilité de chercher et de signaler des vulnérabilités dans tous les systèmes publics exposés de l'administration fédérale (*.admin.ch) à partir de septembre 2023.

Entre septembre et octobre 2023, le NCSC a reçu en l'espace de dix jours 134 annonces de vulnérabilités qui avaient été identifiées dans les systèmes publics exposés de l'administration fédérale. Après une analyse technique, 98 de ces annonces ont été effectivement classées comme étant des failles de sécurité. Elles concernaient tous les départements et la Chancellerie fédérale.

Les retours reçus jusqu'ici au sujet du programme prouvent que les mesures de sécurité conventionnelles ne permettent pas d'identifier toutes les failles de sécurité des systèmes et des applications. Avec plus d'une centaine d'annonces de failles de sécurité reçues en l'espace de dix jours, il est en outre évident que l'administration fédérale doit impérativement continuer d'investir dans le programme de primes aux bogues du NCSC (devenu l'OFCS) et poursuivre son développement. Cette démarche proactive a pour but de donner à la Confédération un moyen d'agir et d'éliminer les risques pour la sécurité dans ses systèmes informatiques avant que des cyberattaques ne ciblent des vulnérabilités. Le programme de l'OFCS contribue aussi grandement à renforcer la cyberrésilience de l'administration fédérale. Les conséquences de composantes informatiques mal ou insuffisamment configurées dans l'administration fédérale peuvent affecter considérablement la sécurité et l'intégrité des systèmes, des applications et des réseaux.

[8] Le jeton d'authentification permet de valider l'identité d'un utilisateur ou d'un appareil.

[9] Microsoft 365 (M365) est un service de Microsoft basé sur un nuage, qui offre toutes sortes d'applications de productivité et d'outils de collaboration pour les entreprises.

4.2 Mesures de formation

4.2.1 Campagne nationale de sensibilisation à la cybersécurité S-U-P-E-R

La Prévention Suisse de la Criminalité et le NCSC ont organisé en 2023 la troisième campagne nationale de sensibilisation S-U-P-E-R (www.s-u-p-e-r.ch) sur le thème de la cybersécurité, en collaboration avec les corps de police cantonaux et municipaux. Les messages de la campagne ont été diffusés par le DFI, le DFF, le DFAE et le DEFR, ainsi que par les corps de police susmentionnés. À l'interne des départements, la campagne a été annoncée sur intranet, par courriel et par voie d'affichage.

L'analyse de la campagne menée en novembre 2023 a montré que le concept avec un site web comprenant une rubrique spécifique pour chaque thème, des pages interactives[10] et un quiz était efficace. Le large soutien des corps de police, des différents départements de l'administration fédérale et des communes est réjouissant. Les résultats positifs de l'année 2023 seront pris en compte dans l'organisation de la campagne S-U-P-E-R de 2024.

4.2.2 Cours pour les experts

En 2023, le NCSC a organisé trois cours en ligne pour les experts de l'administration fédérale. Ils portaient sur les technologies en matière de sécurité pour le *cloud computing*, les messages cryptés de bout en bout (E2EE) et la sécurité DNS. Près de 140 personnes ont participé au premier cours et environ 110 personnes aux deux autres formations. Ces cours sont facultatifs et offrent aux participants et participantes la possibilité de mieux évaluer des problèmes spécifiques en lien avec la sécurité et de partager leurs nouvelles connaissances au sein de l'administration fédérale. Ils constituent un élément de formation essentiel pour renforcer les connaissances des spécialistes informatiques en matière de sécurité tout en réduisant les frais.

4.2.3 Formation sur la sécurité informatique (*compliance*)

Pour répondre directement aux questions du personnel liées à la sécurité informatique au sein des différentes unités administratives, l'administration fédérale fait appel aux délégués à la sécurité informatique des départements et de la Chancellerie fédérale (DSID) et aux délégués à la sécurité informatique de l'organisation (DSIO). Sous leur direction, quelque 94 % des nouveaux collaborateurs ont suivi une formation sur la sécurité informatique en 2023 (chiffres équivalents à ceux de 2022). Cette valeur n'atteint jamais 100 %, car les membres du personnel qui sont engagés à la fin de l'année n'ont pas tous le temps de suivre le module relatif à la sécurité de l'information au sein de l'administration fédérale. D'autres motifs entrent aussi en considération comme les absences pour cause de maladie ou les comptes d'utilisateurs pour les externes qui n'ont pas accès au module.

[10] Les pages web interactives sont particulièrement utiles pour améliorer l'expérience des utilisateurs.

4.3 Défis en matière de formation

4.3.1 Formation des prestataires externes

Plusieurs départements déclarent qu'ils ont des difficultés à sensibiliser correctement le personnel ou les prestataires externes à la sécurité informatique. Les nouveaux collaborateurs engagés à l'interne ont l'obligation de suivre des modules de formation en ligne sur la sécurité informatique avant la fin de la période d'essai. Cette règle ne s'applique pas aux collaborateurs et collaboratrices externes et ne peut parfois pas être mise en œuvre pour des raisons techniques : les personnes concernées ne possèdent pas d'appareil de la Confédération ou n'ont pas accès au *web-based training* (WBT). Quelques offices ont indiqué qu'ils introduisaient des processus qui permettaient d'offrir une formation ou une formation continue ciblée au personnel externe.

Les aspects de la formation ou de la formation continue doivent être ajoutés aux documents d'appel d'offres et aux conditions contractuelles des prestataires externes afin que l'administration fédérale puisse exiger que les collaborateurs externes disposent des connaissances requises en matière de sécurité informatique ou qu'ils suivent une formation ad hoc en lien avec la fonction ou l'échelon.

4.3.2 Formation des responsables des objets protégés

Il s'avère que les responsables des objets protégés[11] doivent parfois posséder des compétences techniques plus pointues en matière d'évaluation et de mise en œuvre des documents sur la sécurité informatique que celles dont ils disposent effectivement. Par conséquent, ils doivent être encadrés de près par les DSIO ou, lorsque cela est possible, être formés en conséquence ou remplacés.

5 Conclusions et perspectives

5.1 Recommandations

En plus des mesures pour garantir une gestion sûre des données et une bonne cyberhygiène, l'OFCS recommande de ne partager avec les tiers que le strict nécessaire et d'anonymiser si possible les données. Tous les domaines doivent examiner la criticité de leurs dépendances aux fournisseurs et aux prestations. En se fondant sur cette analyse, il faudrait fixer contractuellement, surtout en cas de criticité élevée, un droit d'auditer les fournisseurs et prestataires et une obligation d'annoncer les incidents. Le contrat doit aussi définir comment procéder avec les données auxquelles le prestataire n'aurait pas dû avoir accès.
Il est en outre très important de prévoir des mesures techniques supplémentaires pour la protection proactive et la surveillance des systèmes afin de pouvoir introduire des contre-mesures adéquates en cas d'irrégularités. Cela inclut la meilleure protection possible des canaux de communication entre les organisations et leurs fournisseurs. Le plan d'urgence doit être tenu à jour et testé régulièrement. Les scénarios des exercices devraient aussi prendre en compte les relations avec les fournisseurs et les effets indirects des fuites de données.

[11] Une personne doit être désignée comme responsable des objets protégés dans chaque unité administrative. Cette personne est chargée de la mise en œuvre de cette directive. Elle doit être consciente de ses responsabilités et posséder les compétences techniques pour assumer cette tâche.

5.2 Perspectives

5.2.1 Mesures prévues pour 2024

Pour 2024, le Conseil fédéral a défini un train de mesures visant à améliorer la sécurité de l'information et à renforcer les activités qui s'y rapportent.

Ces mesures s'articulent autour de trois axes principaux :

- Premièrement, la gestion de la sécurité sera renforcée, notamment par l'adoption de prescriptions de sécurité supplémentaires concernant la collaboration avec les fournisseurs d'ici à la fin de 2024. La capacité d'effectuer des contrôles et des audits devra être renforcée.
- Deuxièmement, un programme de formation lié à la fonction sera élaboré d'ici à la fin de 2024 pour former et sensibiliser les collaborateurs aux prescriptions de sécurité existantes.
- Troisièmement, une vue d'ensemble des moyens de communication existants pour les autorités fédérales sera établie d'ici à la fin de 2024.

L'administration réagit ainsi aux incidents de sécurité qui sont survenus en 2023.

Pour renforcer la sécurité informatique à court et à moyen terme, les départements et la Chancellerie fédérale continueront de tenir à jour les documents de sécurité et de mettre en œuvre les mesures requises en temps opportun. L'OFCS recommande notamment de mettre l'accent sur l'implémentation des mesures, car la documentation et la mise en œuvre effective diffèrent parfois.

5.2.2 Prochains rapports

À partir de 2024 et conformément à l'art. 83, al. 1, let. h, LSI[12], le service spécialisé de la Confédération pour la sécurité de l'information du SEPOS rendra compte chaque année au Conseil fédéral de la situation en matière de sécurité de l'information au sein de la Confédération.

[12] Loi fédérale du 18 décembre 2023 sur la sécurité de l'information au sein de la Confédération (RS 128)