Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

Centre national pour la cybersécurité NCSC
Sécurité informatique de la Confédération

13 avril 2022

Rapport sur la sécurité informatique de la Confédération 2021

Table des matières

1 Organisation de la sécurité informatique dans l'administration fédérale

La sécurité informatique dans l'administration fédérale comprend toutes les mesures visant à prévenir un cyberincident. Il s'agit d'éviter tout événement nuisant à la confidentialité, à l'intégrité, à la disponibilité ou à la traçabilité des données ou pouvant occasionner des dysfonctionnements, qu'il soit accidentel ou provoqué intentionnellement par un tiers non autorisé[1].
Le Conseil fédéral édicte à cet effet des ordonnances et des instructions sur la protection de l'administration fédérale contre les cyberrisques. Le délégué à la cybersécurité édicte de son côté des directives en matière de sécurité informatique.
Par ailleurs, le Comité pour la sécurité informatique (C-SI) est l'organe consultatif du Centre national pour la cybersécurité (NCSC) pour les questions de sécurité informatique dans l'administration fédérale.

Les unités administratives sont responsables de la protection de leurs systèmes et applications informatiques et des données à protéger (objets à placer sous protection). Elles examinent régulièrement les éléments protégés et prennent les mesures de sécurité nécessaires. En outre, elles sont responsables du respect et de la mise en œuvre des directives informatiques, des procédures de sécurité et des décisions du Conseil fédéral, du NCSC et des départements ou de la Chancellerie fédérale dans leurs domaines de compétences respectifs.

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

Conformément à l'art. 11, al. 2, de l'ordonnance du 27 mai 2020 sur les cyberrisques (OPCy), le délégué à la cybersécurité informe régulièrement le Département fédéral des finances, à l'intention du Conseil fédéral, de l'état de la sécurité informatique au sein des départements et de la Chancellerie fédérale. Il rédige chaque année un rapport sur la sécurité informatique de la Confédération à cette fin.
Ce document s'appuie sur les rapports des départements, des Services du Parlement et de la Chancellerie fédérale (art. 13, al. 1, OPCy – déclaration basée sur une enquête structurée), sur l'expérience du NCSC et sur les constatations faites par ce dernier, ainsi que sur les annonces et rapports sur la sécurité établis par les fournisseurs de prestations (FP) internes de la Confédération.

Au vu des informations fournies en 2021, le NCSC conclut que l'état actuel de la sécurité informatique dans l'administration fédérale est dans l'ensemble adapté aux menaces et que les mesures nécessaires sont prises immédiatement en cas d'incidents.
Or même après avoir déployé un arsenal de mesures de sécurité informatique, toute entreprise doit encore s'attendre à subir une cyberattaque (selon le paradigme *assume breach*[2]).
L'administration fédérale n'échappe pas à la règle.

Pour que les mesures de sécurité prescrites dans la protection informatique de base ou dans les concepts de sécurité soient correctement mises en œuvre, les documents de sécurité nécessaires doivent être actuels (et donc ne pas remonter à plus de cinq ans). Tel est le cas en

[1] Ordonnance du 27 mai 2020 sur la protection contre les cyberrisques dans l'administration fédérale (ordonnance sur les cyberrisques, OPCy; RS **120.73**)

[2] Le paradigme *assume breach* (s'attendre à l'intrusion) se compose des termes anglais *assume* (= supposer, présumer) et *breach* (= faille, lacune – source: www.digitalacademy.de).

moyenne pour 90 % des objets à placer sous protection (même valeur que l'année précédente). Il s'agit fondamentalement d'un pourcentage tout à fait satisfaisant.
La validité des documents de sécurité disponibles à l'échelon de l'administration fédérale atteint un score de 95 % en moyenne (année précédente: 96 %). Les documents de sécurité manquants sont rédigés en continu et mis à jour en cas de besoin.

La mise en œuvre des mesures de sécurité et de leur contrôle (mesures de protection de base et mesures des concepts SIPD) était garantie en 2021 pour 70 % des objets à protéger (année précédente: 57 %). Cette amélioration découle des efforts consentis par les départements afin de mettre à jour les documents sur la sécurité et de rédiger les documents manquants, ainsi que du contrôle de la mise en œuvre des mesures.

La mise en œuvre des mesures de sécurité informatique relève de la responsabilité des chefs des unités administratives, qui mandatent à leur tour les délégués à la sécurité informatique des départements (DSID) et des unités administratives (DSIO).
Tous les postes des DSID et des DSIO sont pourvus. En revanche, les postes des DSID au Département fédéral de l'intérieur, au Département fédéral de l'économie, de la formation et de la recherche et au Département fédéral de l'environnement, des transports, de l'énergie et de la communication ne sont pourvus qu'à 60 %, alors qu'ils devraient l'être à 80 % au niveau de chaque département.

Le télétravail instauré dans le cadre des mesures de lutte contre le coronavirus a entraîné une multiplication des problèmes de disponibilité du réseau en janvier 2021 (largeur de la bande passante au niveau de la connexion Internet au réseau de la Confédération). Les utilisateurs en télétravail ont sollicité davantage la connexion Internet à ce réseau, ce qui a occasionné divers problèmes de performance, notamment lors des appels par Skype et des vidéoconférences.
De concert avec le secteur Transformation numérique et gouvernance de l'informatique de la Chancellerie fédérale, l'Office fédéral de l'informatique et de la télécommunication (OFIT) a augmenté la bande passante du réseau tout en bloquant certains services de streaming. Ces mesures ont permis de décharger ce dernier et d'améliorer à nouveau la qualité des vidéoconférences, mais en contrepartie il n'était plus possible de regarder des vidéos sur Internet. D'autres mesures ont toutefois permis de résoudre aussi ce problème.
On peut retenir que le télétravail a globalement bien fonctionné jusqu'ici et qu'aucun incident de sécurité imputable à ce dernier n'a été signalé à ce jour.

3 Garantie de la sécurité informatique – facteur humain

Les collaborateurs de tous les niveaux hiérarchiques jouent un rôle capital dans le domaine de la sécurité informatique. Ils sont donc régulièrement sensibilisés et formés à la sécurité informatique.
Sous la direction des DSID et des DSIO, quelque 95 % des nouveaux collaborateurs ont suivi un cours introductif sur la sécurité informatique en 2021 (contre 87 % en 2020). Cette amélioration découle de la numérisation accrue des formations pendant la pandémie.
Dans le cadre d'un «kit de bienvenue» fourni à tous les nouveaux collaborateurs de l'administration fédérale, le NCSC élabore actuellement un module sur la sécurité informatique, qui devrait être mis à la disposition de l'ensemble de l'administration fédérale au milieu de l'année 2022.

Plusieurs départements et unités administratives ont pris des mesures de sensibilisation individuelles, notamment dans le domaine de l'hameçonnage par courriel.

Les formations organisées par le NCSC dans le domaine de la sécurité informatique ont rencontré un large succès. Ces formations proposées dans le cadre du Centre de formation de l'administration fédérale ont été dispensées pour la plupart en ligne pendant l'année 2021 et ont reçu un accueil très positif de la part des participants.

En outre, le NCSC propose désormais des cours d'expert visant l'acquisition et le développement de connaissances spécialisées dans le domaine de la cybersécurité, qui s'adressent aux collaborateurs du NCSC, aux DSID et DSIO, ainsi qu'à d'autres personnes intéressées de l'administration fédérale qui travaillent sur les questions de cybersécurité.

Soulignons par ailleurs que de nombreux collaborateurs réagissent de manière appropriée aux pourriels et aux courriels d'hameçonnage en les supprimant immédiatement ou en cliquant sur le bouton «Spam» du programme de messagerie Outlook afin de les transmettre au FP pour analyse.
Les tentatives ciblées d'hameçonnage (tout comme les autres tentatives d'escroquerie) proviennent souvent d'adresses électroniques de services externes (fournisseurs par ex.) qui ont été piratées, ce qui les rend d'autant plus difficiles à identifier pour les destinataires de ces courriels. Dans la mesure où plusieurs cybercriminels sont arrivés à leurs fins dans un premier temps, les campagnes de sensibilisation restent nécessaires.

4 Incidents de sécurité et vulnérabilités

4.1 Synthèses des fournisseurs de prestations internes

En 2021, le principal fournisseur de prestations interne de la Confédération, l'OFIT, a traité environ 434 incidents de sécurité[3] (année précédente: 834). Il convient de souligner que les incidents de sécurité n'entraînent pas tous des dommages directs pour l'administration fédérale. Les vulnérabilités critiques sont par exemple aussi examinées à titre préventif lors du traitement de ces incidents.
La surveillance des réseaux – à l'exception de quelques réseaux très spécifiques[4] – relève de la responsabilité de l'équipe d'intervention en cas d'urgence informatique (*Computer Security Incident Response Team*, ou CSIRT) de l'OFIT, qui est le fournisseur du service standard de transmission des données. Les incidents décrits dans les rapports du CSIRT de l'OFIT peuvent donc être considérés comme représentatifs de l'ensemble de l'administration fédérale civile.
En outre, le Cyber Fusion Center du FP du Département fédéral de la défense, de la protection de la population et des sports (DDPS) a traité plus de 400 notifications internes en 2021, dont la plupart ont été considérées comme non critiques.
Les autres FP n'ont mentionné aucun incident particulier.

[3] Toutes les annonces de sécurité reçues sont comptabilisées comme incidents de sécurité. En font aussi partie les cas suspects qui, après analyse, s'avèrent être inoffensifs ou constituer une fausse alarme, ainsi que les cas d'hameçonnage qui ne concernent pas directement l'administration fédérale.

[4] En est entre autres exclue la transmission de données garantie sur les réseaux centraux de l'armée (notamment sur des réseaux destinés au groupe Défense), qui doit être fournie dans le cadre de l'infrastructure fédérale et en interne par la Base d'aide au commandement du fait des exigences visant à assurer la disponibilité et à éviter la dégradation des services (modèle de marché relatif au service standard Transmission de données du 19 juin 2020).

4.2 Incidents de sécurité

L'administration fédérale subit constamment des attaques. Il peut s'agir d'attaques par courriels à très grande échelle, ou d'attaques ciblées contre l'infrastructure informatique de la Confédération ou contre certains collaborateurs.
Les agresseurs vont des distributeurs de pourriels en masse aux acteurs probablement étatiques, en passant par la criminalité organisée et les «hacktivistes».

Courriels entrants
L'OFIT analyse tous les courriels entrants et veille à ce que les courriels potentiellement dangereux ne parviennent pas à leurs destinataires.

En 2021, 34,5 % des courriels entrants (année précédente: 48 %) ont été **effacés** avant de parvenir à leur destinataire:

Courriels entrants dans l'administration fédérale	138 872 079 (année précédente: env. 160 millions de courriels)
Dont courriels supprimés de manière centrale[5]	47 955 038
Courriels transmis aux destinataires	90 917 041

Ce recul bienvenu du nombre de courriels supprimés s'explique surtout par le démantèlement de l'infrastructure Emotet[6] (voir la section «Blocage d'adresses URL et de domaines» ci-dessous pour de plus amples informations à ce sujet).

En analysant et en triant les courriels entrants, l'OFIT contribue largement à la sécurité dans toute l'administration fédérale.

Hameçonnage
L'hameçonnage est une tentative, par le biais de sites web, de courriels ou de messages instantanés falsifiés, d'accéder à des données personnelles d'un utilisateur afin d'usurper son identité ou de télécharger sur son système un logiciel malveillant au moyen d'une pièce jointe.
Ce phénomène n'épargne pas les collaborateurs de l'administration fédérale puisqu'en 2021, l'OFIT a traité onze cyberattaques par hameçonnage qui avaient abouti (contre 34 l'année précédente).
Le nombre élevé de notifications relatives à des pourriels témoigne de l'intérêt que revêt toujours cette méthode aux yeux des cybercriminels.
Les efforts de sensibilisation des collaborateurs aux attaques par hameçonnage se poursuivent dans l'ensemble de l'administration fédérale et mettent notamment en avant le raffinement croissant des méthodes utilisées par les cybercriminels.

Maliciels
Il est particulièrement réjouissant de constater qu'**un** seul incident impliquant un logiciel malveillant (maliciel) a infecté **un** seul appareil de la Confédération en 2021 (contre 15 en 2020). Malgré la nature ciblée de cette cyberattaque, l'intervention immédiate du FP responsable a permis d'éviter des dommages plus importants.
Le caractère isolé de cet incident en 2021 ne dispense toutefois pas d'améliorer encore la protection de la Confédération contre les maliciels.

[5] Sont supprimés de manière centrale – et donc neutralisés – les courriels émanant de distributeurs connus de pourriels et de maliciels ainsi que les courriels dans lesquels des virus ou des maliciels ont été détectés.

[6] Emotet est un maliciel qui circule principalement par le biais de pourriels. À l'origine, il s'agissait d'un simple cheval de Troie bancaire. L'objectif des pirates était de s'introduire dans le système informatique de leurs cibles pour se saisir des données d'accès à leurs comptes bancaires. Emotet a ensuite été employé comme injecteur (*dropper*), un type de moyen qui est souvent utilisé pour répandre des maliciels supplémentaires.

Skype for Business
En octobre 2021, des tentatives de cyberattaques visant le programme Skype for Business d'un département ont été détectées. En l'occurrence, les cyberpirates ont testé une foule de mots de passe pour essayer de se connecter à de nombreux comptes Skype et ont réussi à accéder à trois d'entre eux. Les collaborateurs concernés ont été contactés immédiatement et leur mot de passe a été modifié. D'autres mesures à effet immédiat ont également été prises.

Système de gestion de l'apprentissage (*learning management system*, LMS) de l'Armée suisse
Des problèmes de disponibilité du système LMS de l'Armée suisse sont apparus lorsque l'école de recrues a débuté en télétravail à cause de la pandémie. Un service externe a également découvert une vulnérabilité au niveau de la protection des données. Ces deux problèmes ont pu être résolus rapidement.

Blocage d'adresses URL et de domaines (sites Internet externes)
Onze mandats ont conduit au blocage de 90 domaines[7] (contre 217 en 2020). Si, comme dans le passé, la plupart de ces domaines ont été bloqués en raison de la présence de maliciels, ce nombre peu élevé s'explique également par le démantèlement, annoncé fin janvier, de l'infrastructure Emotet par Europol et d'autres autorités de poursuite pénale. Le nombre de cyberattaques menées à l'aide de pourriels renfermant des maliciels a alors considérablement chuté jusqu'en mars. Puis de nouvelles attaques conduites au moyen du maliciel IcedID, qui a remplacé Emotet, ont été constatées, mais malgré ces vagues d'attaques, seul un appareil client a été infecté (voir la section «Maliciels» ci-dessus).

Incidents de sécurité externes ayant un impact direct sur l'administration fédérale
Quatre failles de sécurité critiques de Microsoft Exchange[8] ont permis la réalisation d'attaques à distance avec exécution de code. Les systèmes Exchange ont été corrigés en l'espace de quelques jours au moyen d'un patch d'urgence mis en œuvre par les FP.

Microsoft a en outre annoncé une vulnérabilité critique appelée PrintNightmare, qui aurait permis à des utilisateurs pouvant installer un pilote d'imprimante mais n'ayant pas de privilèges élevés de mettre en péril l'ensemble du système. L'installation de logiciels par les utilisateurs présente en général un grand risque. Cette activité étant interdite sur les appareils clients de la Confédération, ce risque est fortement réduit.

Une vulnérabilité très critique qui affectait le sous-logiciel Log4j[9] et qui a été publiée le 10 décembre 2021 s'est vu attribuer le niveau de gravité maximal de 10 par l'Apache Software Foundation. Cette vulnérabilité permet à des cyberattaquants d'exécuter un code malveillant à distance sur l'ordinateur touché et de prendre le contrôle complet du système dans certaines circonstances.
Une mise à jour du sous-logiciel Log4j – permettant de combler cette faille de sécurité – a été publiée quelques jours après l'annonce de cette vulnérabilité. D'autres mises à jour de Log4j ont suivi en rapport avec cette faille car les mises à jour précédentes ne l'avaient pas complètement comblée, de sorte qu'elle pouvait éventuellement être encore exploitée dans certaines configurations non standard. Le sous-programme Log4j est intégré dans de nombreuses solutions logicielles et, dans certains cas, il faut attendre la mise à jour fournie par le

[7] Un domaine est un nom unique dans le monde entier d'un site Internet.

[8] Microsoft Exchange est un logiciel de groupe de travail et de transmission de courrier électronique de l'entreprise Microsoft, qui permet de stocker et de gérer de façon centralisée les courriers électroniques, les rendez-vous, les contacts, les tâches et d'autres éléments pour plusieurs utilisateurs, facilitant ainsi la collaboration dans un groupe de travail ou dans une entreprise.

[9] Appelé également Log4Shell.

fabricant du programme car il n'est pas possible de l'effectuer soi-même. En installant immédiatement les mises à jour disponibles et en surveillant étroitement les répercussions de cette vulnérabilité, les FP ont pu déjouer les tentatives des cybercriminels d'exploiter cette vulnérabilité dans l'administration fédérale.

Les réactions immédiates des FP – coordonnées par le NCSC – ont permis d'éviter que les incidents de sécurité susmentionnés ne portent préjudice à l'administration fédérale.

Vulnérabilités dans les départements
Les départements indiquent que la plupart des vulnérabilités identifiées n'ont eu que des conséquences mineures ou modérées[10].
Seule la défaillance de prestations transversales a eu des conséquences majeures en ce sens qu'elle a entravé la disponibilité de tâches importantes qui n'ont plus pu être effectuées temporairement.

4.3 Systèmes et protocoles de réseau obsolètes

À l'exception des Services du Parlement et du Département fédéral de l'environnement, des transports, de l'énergie et de la communication, les départements ont signalé qu'ils utilisaient encore certains systèmes et protocoles de réseau obsolètes.

Ce sont les responsables des applications des bénéficiaires des prestations dans les offices et départements qui supportent la responsabilité de l'utilisation des systèmes et protocoles obsolètes. Mais faute de financement ou de ressources humaines suffisantes, ces responsables n'ont que peu de possibilités de remplacer ces protocoles et sont contraints de continuer à accepter les risques inhérents à des failles de sécurité parfois majeures.

Ces failles sont certes mentionnées dans les rapports sur la sécurité et assumées par les différentes directions, mais dans les faits, compte tenu de leur complexité technique, seuls quelques responsables sont conscients des risques informatiques qu'ils acceptent en réalité. Cette situation pouvant générer une accumulation de risques pour la sécurité, le NCSC suivra cette problématique en tant que responsable de la conduite et de la coordination dans le domaine de la cybersécurité.
La plupart de ces systèmes et protocoles seront remplacés ou mis à jour (d'ici à fin 2024 pour certains).
En outre, certains systèmes obsolètes – installés dans des laboratoires pour la plupart – sont déjà hébergés sur des réseaux isolés et ne génèrent ainsi aucun trafic avec le réseau de la Confédération.

5 Renforcement de la sécurité informatique

5.1 Mesures prises en 2021

Tous les départements, les Services du Parlement et la Chancellerie fédérale ont instauré

[10] Conséquences majeures = fuite de données; des personnes non autorisées peuvent accéder à des informations ou données à protéger, de sorte que le respect des prescriptions légales est fortement compromis voire impossible, que certaines prestations ne peuvent être fournies, qu'un département entier et/ou des services externes sont touchés.

Conséquences modérées = le respect des prescriptions légales est compromis ou entravé, les prestations sont restreintes, les conséquences pour les services externes sont supportables.

Conséquences mineures = le respect des prescriptions légales n'est ni compromis ni entravé, les prestations sont restreintes au sein de l'UA, aucune répercussion sur les services externes.

des mesures et entrepris des actions appropriées afin de renforcer leur sécurité informatique.

Voici quelques-unes des actions menées:
- organisation de campagnes de sensibilisation régulières (menées pour certaines de façon transversale dans plusieurs départements);
- vérification périodique des droits d'accès;
- contrôle des téléphones mobiles afin de détecter des maliciels ou le logiciel d'espionnage Pegasus;
- entretiens entre directeurs sur la question de la sécurité informatique notamment;
- formations, à l'instar de la Security Academy du DDPS (semaine de formation du DDPS);
- renforcement des ressources humaines dédiées à la sécurité informatique;
- organisation de programmes «Bug Bounty»[11] et de tests publics de la sécurité;
- poursuite du développement des systèmes de gestion de la sécurité de l'information (ISMS);
- création de zones techniques spéciales pour les systèmes de domotique en particulier (technique des bâtiments);
- réalisation d'audits;
- connexion permanente par VPN («VPN Always On») des postes de travail;
- initialisation de projets comme la signature numérique des macros.

5.2 Mesures prévues à court et à moyen terme

Afin de renforcer la sécurité informatique à court et à moyen terme, les départements, les Services du Parlement et la Chancellerie fédérale ont prévu de prendre notamment les mesures suivantes:

- mise en place d'une stratégie numérique;
- campagnes de sensibilisation;
- formation sur le traitement des informations classifiées;
- création de systèmes ISMS au sein des départements;
- renforcement des ressources humaines;
- réalisation d'audits techniques;
- mise à jour des consignes internes en matière de sécurité de l'information;
- poursuite et clôture du programme destiné à lutter contre le vol de données d'accès intitulé «Credential Theft Mitigation», de la signature numérique des macros, et du remplacement du logiciel de chiffrement «SecureCenter» de la Confédération.

Quant au NCSC, en sus de l'appui qu'il fournit aux DSID et aux DSIO dans tous les domaines de la sécurité informatique, il s'attache surtout à poursuivre l'élaboration des consignes de sécurité, à améliorer la prise en charge des vulnérabilités, ainsi qu'à définir des mesures pour assurer la formation continue des collaborateurs de la Confédération et l'exécution de la loi sur la sécurité de l'information.

[11] Ces programmes font appel au «piratage éthique», donc à des pirates informatiques qui recherchent légalement des failles dans un cadre déterminé, afin de déceler les éventuelles lacunes dans la sécurité des systèmes informatiques d'une organisation. Pour chaque bogue découvert et confirmé, le pirate reçoit une prime (*bounty*), dont le montant est fixé en fonction de la gravité de la faille détectée.