Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

Unité de pilotage informatique de la Confédération UPIC
Sécurité informatique

État de la sécurité informatique dans l'administration fédérale en 2019

1 La sécurité informatique dans l'administration fédérale

La sécurité informatique dans l'administration fédérale comprend des mesures visant à protéger l'intégrité et la disponibilité des systèmes de technologies de l'information et de la communication (TIC), de même que la confidentialité, l'intégrité, la disponibilité et la traçabilité des données sauvegardées, traitées et transférées dans ces systèmes[1]. Le Conseil fédéral édicte les directives concernant la sécurité informatique dans l'administration fédérale[2].
Sur la base de ces directives, l'Unité de pilotage informatique de la Confédération (UPIC) édicte des directives informatiques pour l'administration fédérale.
Les mesures de sécurité informatique s'appuient sur les normes internationales en vigueur, notamment les normes ISO concernant les processus de sécurité informatique, ainsi que sur l'évaluation des menaces.

Les unités administratives sont responsables de la protection de leurs systèmes et applications en matière de TIC et des données à protéger (objets à placer sous protection). Elles examinent régulièrement les objets à placer sous protection et prennent les mesures de sécurité nécessaires.

Pour évaluer la situation actuelle et édicter si nécessaire des mesures d'urgence, le domaine Sécurité informatique de la Confédération de l'UPIC collabore étroitement avec la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) ainsi qu'avec d'autres organes compétents pour la sécurité informatique[3].

En matière de sécurité informatique, l'administration fédérale ne se distingue pas fondamentalement des autres autorités, des entreprises ou des particuliers: les attaques sont constantes et il faut se protéger en conséquence. Force est toutefois de constater que les organisations étatiques comme l'administration fédérale sont davantage que les particuliers et les

[1] Ordonnance du 9 décembre 2011 sur l'informatique et la télécommunication dans l'administration fédérale (ordonnance sur l'informatique dans l'administration fédérale, OIAF), RS *172.010.58*

[2] https://www.isb.admin.ch/isb/fr/home/ikt-vorgaben/grundlagen/w002-weisungen_bundesrat_ikt-sicherheit_bundesverwaltung_wisb.html

[3] Par ex. Computer Emergency Response Team de l'UPIC (GovCERT.ch), Computer Security Incident Response Team (CSIRT) de l'OFIT ou Computer Emergency Response Team du DDPS (BAC MilCERT).

PME la cible d'attaques commises par d'autres organisations étatiques.

Le présent document ne fournit aucune information sur des attaques ou failles de sécurité spécifiques. Si un agresseur potentiel en prenait connaissance, c'est toute l'informatique de l'administration fédérale qui pourrait en pâtir. Par conséquent, le présent rapport ne fournit pas non plus d'indications concernant des départements ou des offices individuels.

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

En fin d'année, les départements, la Chancellerie fédérale et les services du Parlement font rapport à l'UPIC sur la mise en œuvre des mesures de sécurité (déclaration basée sur une enquête structurée). L'UPIC vérifie la plausibilité des informations reçues, en particulier au moyen des résultats d'évaluation issus de l'audit de l'informatique visé à l'art. 28 de l'ordonnance sur l'informatique dans l'administration fédérale.
S'appuyant sur les informations fournies pour 2019, l'UPIC conclut que l'état actuel de la sécurité informatique dans l'administration fédérale est dans l'ensemble adapté aux menaces et se situe à un niveau comparable à celui d'organisations similaires et de l'économie privée.

Pour la mise en œuvre des mesures de sécurité requises, les documents de sécurité nécessaires doivent être disponibles et actuels.
En 2019, la mise en œuvre des mesures de sécurité était garantie pour environ 90 % des objets à placer sous protection. Il s'agit fondamentalement d'une bonne valeur, car il est courant qu'une partie des documents soient en cours de remaniement.
Cependant, le niveau requis n'est pas atteint en ce qui concerne les contrôles de la mise en œuvre, même si la situation s'est améliorée par rapport à l'année précédente (contrôle pour environ 70 % des objets à placer sous protection, contre 66 % l'année précédente).
La mise en œuvre et le contrôle des mesures de sécurité requises permettent de maintenir l'état de la sécurité et de le garantir durablement dans toute l'administration.

3 Facteur humain

Les collaborateurs de tous les niveaux hiérarchiques jouent un rôle capital dans le domaine de la sécurité informatique. Les collaborateurs de l'administration fédérale ont donc été formés à la sécurité informatique en 2019 également.
Sous la direction des délégués à la sécurité informatique des unités administratives, quasiment tous les nouveaux collaborateurs (env. 95 %) sont familiarisés aux aspects de la sécurité informatique. Un manque de formation existe encore en particulier chez les collaborateurs externes.
Au cours de l'année sous revue, 130 spécialistes, tels que chefs de projets, responsables de systèmes ou délégués à la sécurité informatique, ont été formés spécifiquement à la sécurité informatique et au processus de l'administration fédérale en la matière.
Les formations et perfectionnements sont proposés par l'UPIC au Centre de formation de l'administration fédérale. L'UPIC organise en outre des formations ciblées et sur mesure dans certaines unités administratives et mène des campagnes de sensibilisation générales destinées à l'ensemble de l'administration fédérale.
En complément aux campagnes de sensibilisation centrales de l'UPIC, de nombreuses unités administratives organisent leurs propres actions de sensibilisation (notamment dans le domaine de l'hameçonnage par courriel).

4 Incidents de sécurité

En 2019, le principal fournisseur de prestations interne de la Confédération, l'Office fédéral de l'informatique et de la télécommunication (OFIT), a traité environ 900 incidents de sécurité[4]. Tous les incidents de sécurité n'engendrent cependant pas des dommages directs pour l'administration fédérale. Les points faibles critiques sont par exemple recherchés à titre préventif dans le cadre du traitement de ces incidents.

Les incidents de sécurité se répartissent en trois catégories:

- les attaques dirigées contre l'administration fédérale;
- les incidents de sécurité externes qui ont un impact direct sur l'administration fédérale;
- les pannes et événements internes.

4.1 Attaques dirigées contre l'administration fédérale

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

Courriels contenant des maliciels
Des attaques ciblées sont par exemple menées par l'envoi à des destinataires de l'administration fédérale de courriels contenant un logiciel nuisible (maliciel) ou un lien renvoyant vers un tel logiciel.
L'OFIT analyse en permanence les courriels entrants et veille à ce que les courriels potentiellement dangereux ne parviennent pas à leurs destinataires.

En 2019, selon l'analyse de l'OFIT, 78 % des courriels entrants ont été supprimés avant de parvenir à leur destinataire:

Courriels entrants dans l'administration fédérale:	306 687 261 (100 %)
Dont courriels supprimés de manière centrale (non transmis aux destinataires):	238 548 362 (78 %)
Courriels transmis aux destinataires:	68 138 899 (22 %)

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.

Hameçonnage
L'hameçonnage est une tentative, passant par des sites web, des courriels ou des messages instantanés falsifiés, d'accéder à des données personnelles d'un utilisateur afin d'usurper son identité ou de charger sur le système un logiciel malveillant au moyen d'une pièce jointe.

Dans 58 attaques d'hameçonnage, des collaborateurs de l'administration fédérale ont donné

[4] 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. Étant donné que l'OFIT fournit de nombreuses prestations transversales et de base pour l'ensemble de l'administration fédérale, cette statistique fournit un tableau représentatif.

leurs données d'accès à des messageries privées. Ni perte de données ni menace pour l'infrastructure informatique de la Confédération n'ont été constatées dans ces cas. Les collaborateurs concernés sont à chaque fois informés par le délégué à la sécurité informatique de leur unité organisationnelle des attaques constatées et des mesures à prendre. Ils peuvent ainsi modifier les données d'accès (mots de passe) en question et améliorer leur comportement.

Les usurpations d'identité à l'aide de méthodes d'hameçonnage iront croissant. Ces méthodes étant de plus en plus subtiles et ciblées, elles constituent un danger important. Les événements actuels sont aussi directement exploités pour des attaques (par ex. la crise du coronavirus, les championnats du monde, etc.).
Si des mesures de sécurité d'ordre technique sont prises pour identifier les courriels d'hameçonnage et les sites web contenant des maliciels, le thème de l'hameçonnage est aussi largement abordé dans les campagnes de sécurité, avec de premiers résultats positifs: les collaborateurs ont identifié et annoncé à l'OFIT nettement plus de courriels d'hameçonnage.

Appareils infectés
En 2019, l'OFIT a découvert 107 appareils infectés au total. L'infection était avérée pour 19 postes de travail (année précédente: 84), qui ont dû être restaurés (l'OFIT assure le suivi de quelque 30 000 postes au total).
Même si le chiffre de 19 appareils infectés semble faible, il ne faut pas oublier que chaque appareil infecté peut être à l'origine d'une menace pour l'ensemble de l'administration fédérale.

Attaques contre la présence sur Internet de l'administration fédérale
En 2019, 30 agresseurs ayant lancé une attaque contre la présence sur Internet de l'administration fédérale[5] ont pu être bloqués. D'autres blocages ont été effectués à titre de protection contre le scanning intensif de l'infrastructure de l'administration fédérale.

4.2 Incidents de sécurité externes ayant un impact direct sur l'administration fédérale

Sites web infectés
Les sites web non sécurisés constituent une menace pour l'administration fédérale également. Ils présentent souvent des failles de sécurité grossières et peuvent donc être utilisés pour des attaques d'hameçonnage ou la propagation de maliciels. En 2019, la Confédération a bloqué l'accès à environ 715 sites web, soit à titre préventif soit dans une démarche réactive.

Failles de sécurité dans les composants matériels et les systèmes d'exploitation
Les failles de sécurité découvertes dans les composants matériels et les systèmes d'exploitation sont immédiatement corrigées. Si cela n'est pas possible, les domaines concernés sont surveillés étroitement et des mesures sont prises pour les protéger. Aucune exploitation de ce type de failles de sécurité n'a été constatée jusqu'ici.

[5] Ces sites web sont hébergés par la Confédération.

4.3 Pannes et événements internes

Les pannes internes concernent principalement la disponibilité des systèmes et des données. En 2019, aucune interruption grave mettant notablement en péril la disponibilité requise n'a été constatée.

Quelques postes de travail ont dû être restaurés en raison du comportement inapproprié de collaborateurs. Après chaque incident, les collaborateurs concernés sont formés spécifiquement par leur délégué à la sécurité informatique (voir ci-dessus: hameçonnage).

5 Autres mesures

L'administration fédérale s'appuie sur l'évaluation de la situation et sur les incidents de sécurité pour prendre les mesures de sécurité adéquates. Outre d'éventuelles mesures d'urgence, elle élabore des mesures d'ordre juridique, organisationnel et technique et les met en œuvre de manière durable et proportionnée.

Afin de renforcer la mise en œuvre de la sécurité informatique dans l'administration fédérale ainsi qu'en faveur du pays, le Conseil fédéral a décidé de mettre en place le Centre national pour la cybersécurité. Les travaux de mise en place du centre ont débuté en 2019 et conduiront à une amélioration substantielle dans le domaine de la sécurité informatique[6].

Afin de soutenir les collaborateurs de l'administration fédérale, l'UPIC a lancé en mai 2019 une campagne de sensibilisation à la sécurité informatique. Les PME et le grand public ont également accès aux contenus de cette campagne[7].

Unité de pilotage informatique de la Confédération

[6] https://www.melani.admin.ch/melani/fr/home/ueber_ncsc/das_ncsc.html

[7] www.securite-informatique.admin.ch