Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

Centre national pour la cybersécurité NCSC
Sécurité informatique de la Confédération

9 juin 2023

Rapport sur la sécurité informatique de la Confédération en 2022

Table des matières

1 Organisation de la sécurité informatique dans l'administration fédérale 3
2 État actuel de la sécurité informatique dans l'administration fédérale ... 3
3 Garantie de la sécurité informatique – facteur humain ... 4
4 Incidents de sécurité et vulnérabilités ... 5
4.1 Incidents de sécurité ... 5
4.2 Vulnérabilités ... 6
4.3 Systèmes et protocoles de réseau obsolètes ... 8
5 Synthèse des fournisseurs de prestations internes ... 9
6 Renforcement de la sécurité informatique ... 10
6.1 Mesures prises en 2022 ... 10
6.2 Mesures prévues pour 2023 ... 11

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 à gérer rapidement ceux qui surviennent néanmoins. On entend par cyberincident tout événement pouvant compromettre la confidentialité, l'intégrité, la disponibilité ou la traçabilité des données ou occasionner des dysfonctionnements, qu'il soit accidentel ou provoqué intentionnellement par un tiers non autorisé[1].
Le Conseil fédéral édicte les ordonnances et directives propres à assurer l'application des mesures qui s'imposent pour assurer la sécurité informatique dans l'ensemble de l'administration fédérale. Il a en outre octroyé au délégué à la cybersécurité la compétence d'édicter des directives informatiques[2]. Les directives sont élaborées par le Centre national pour la cybersécurité (NCSC) avec le soutien du Comité pour la sécurité informatique (C-SI), l'organe consultatif pour les questions de sécurité informatique dans l'administration fédérale.
Les unités administratives sont responsables de la sécurité de leurs objets informatiques à protéger[3]. À cet effet, elles examinent régulièrement les objets sensibles et prennent les mesures de sécurité requises. 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, OPCy, le délégué à la cybersécurité informe régulièrement le Département fédéral des finances (DFF), à l'intention du Conseil fédéral, de l'état de la sécurité informatique au sein des départements et de la Chancellerie fédérale. À cet effet, il rédige chaque année un rapport sur la sécurité informatique de la Confédération.
Ce rapport s'appuie sur les informations que les départements et la Chancellerie fédérale transmettent au NCSC concernant l'état de leur sécurité informatique. Pour récolter les données dont il a besoin, le NCSC réalise une enquête structurée auprès de tous les délégués à la sécurité informatique des départements et de la Chancellerie fédérale. Le rapport prend également en considération l'expérience du NCSC et les constatations faites par ce dernier, ainsi que les signalements et rapports sur la sécurité établis par les fournisseurs de prestations internes de la Confédération.
Sur la base de ces informations, le NCSC conclut que le dispositif de sécurité actuel mis en place par l'administration fédérale est, dans l'ensemble, adapté aux menaces. Lors d'incidents, les mesures qui s'imposaient ont toujours pu être appliquées immédiatement. Cependant, même si elle a déployé un train de mesures de sécurité informatique, toute entreprise doit s'attendre à subir une cyberattaque. L'administration fédérale n'échappe pas à la règle.
Le NCSC a totalement remanié et restructuré la directive informatique «Si001 – Protection informatique de base dans l'administration fédérale», dont la nouvelle version est en vigueur depuis le 1er mars 2022. Compte tenu de l'expérience accumulée jusqu'à présent et des modifications escomptées en lien avec l'entrée en vigueur de la loi sur la sécurité de

[1] Ordonnance du 27 mai 2020 sur les cyberrisques (OPCy; RS **120.73**)

[2] Art. 11 OPCy

[3] 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).

l'information (LSI)[4], les processus P041 «Analyse des besoins de protection» et P042 «Concept de sécurité de l'information et de protection des données (concept SIPD)» sont également en cours de révision.
Pour que les mesures de sécurité prescrites dans la directive sur la protection informatique de base ou dans les concepts SIPD puissent être appliquées, les documents de sécurité nécessaires doivent être à jour (ne pas remonter à plus de 5 ans). Cette exigence est remplie pour 80 % des objets à protéger de l'administration fédérale. Par rapport à l'année précédente, cela représente un recul de 10 points de pourcentage, qui s'explique par l'augmentation du nombre d'objets à protéger identifiés dans le cadre de contrôles d'inventaire au sein de différentes unités administratives, objets pour lesquels il faut maintenant rédiger les documents de sécurité adéquats. Des fluctuations du degré de couverture des documents de sécurité sont inévitables en raison de l'évolution constante des inventaires. Le taux de 80 % montre cependant que les unités administratives continuent d'observer l'obligation de tenir à jour les documents de sécurité. La mise en œuvre des mesures de sécurité et leur contrôle (mesures prévues dans la directive sur la protection informatique de base et les concepts SIPD) étaient en outre garantis en 2022 pour 73 % des objets à protéger (année précédente: 70 %). Cette légère amélioration tient à la multiplication des contrôles effectués par les départements et les unités administratives.

3 Garantie de la sécurité informatique – facteur humain

Les collaborateurs de tous les niveaux hiérarchiques jouent un rôle clé dans le domaine de la sécurité informatique. Ils sont donc régulièrement sensibilisés et formés à cette question.
Les formations organisées par le NCSC ont rencontré un large succès. Proposées par le Centre de formation de l'administration fédérale, elles ont de nouveau pu se dérouler en présence en 2022, contrairement à l'année précédente, où elles avaient dû être réalisées exclusivement en ligne. En raison de la forte demande, il est prévu d'organiser 4 cours au lieu de 3 en 2023.
Par ailleurs, le NCSC a régulièrement mené des cours et des campagnes de sensibilisation pour permettre aux délégués à la sécurité informatique des départements et des unités administratives ainsi qu'aux autres membres du personnel de l'administration fédérale d'approfondir et de consolider leurs connaissances dans le domaine de la cybersécurité. Ainsi, plusieurs cours avancés ont été proposés en ligne en 2022 sur les thèmes de la cryptographie (avec 100 participants en moyenne), du bitcoin et de la blockchain (90 participants en moyenne), de la forensique numérique (140 participants en moyenne), de Tor et du Darknet (140 participants en moyenne) et de Kubernetes (130 participants en moyenne).

[4] Loi du 18 décembre 2020 sur la sécurité de l'information (LSI), FF **2020** 9665

En 2021 et 2022, le NCSC et la Prévention Suisse de la Criminalité ont mené ensemble une campagne nationale de sensibilisation auprès de la population. Les informations données à cette occasion étaient également à la disposition du personnel fédéral. En 2022, la campagne était axée sur la vigilance sur Internet, mettant l'accent sur l'hameçonnage et les arnaques, des thèmes essentiels aussi au sein de l'administration fédérale. Elle a été diffusée par 40 offices fédéraux au total, dépendant du Département fédéral de la défense, de la protection de la population et des sports (DDPS), du Département fédéral de l'économie, de la formation et de la recherche (DEFR), du Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC), du Département fédéral des affaires étrangères (DFAE), du DFF, du Département fédéral de l'intérieur (DFI) et du Département fédéral de justice et police (DFJP).
Afin de continuer à promouvoir les connaissances sur les risques, les menaces et l'utilisation prudente des outils numériques et mobiles, l'administration fédérale a en outre mis sur pied en 2022 une offre de formation en ligne sur le thème de la sécurité informatique. Initialement conçu sous la forme d'un programme pilote, ce cours est, à partir de 2023, obligatoire pour tous les nouveaux collaborateurs. Le module permettra à l'ensemble du personnel fédéral, toutes fonctions et positions confondues, d'approfondir le thème de la sécurité informatique.
Pour répondre directement aux questions du personnel liées à la sécurité informatique au sein des unités administratives, l'administration fédérale s'appuie en outre sur 8 délégués à la sécurité informatique au niveau des départements et de la Chancellerie fédérale (DSID) et sur plus de 80 délégués à la sécurité informatique au niveau des offices (DSIO).
Sous la direction des DSID et des DSIO, quelque 94 % des nouveaux collaborateurs ont suivi une initiation à la sécurité informatique en 2022 (contre 95 % en 2021).
Dans le contexte actuel, le personnel fédéral a bien plus souvent recours aux formes de travail mobiles qu'avant la pandémie de COVID-19. C'est pourquoi le nombre d'outils numériques utilisés dans l'informatique de la Confédération augmente sans cesse, et de nombreuses sources de danger doivent être écartées en amont au moyen de connexions VPN sécurisées aux systèmes de l'administration.

4 Incidents de sécurité et vulnérabilités

4.1 Incidents de sécurité

L'infrastructure informatique de l'administration fédérale est exposée en permanence à des cyberattaques de nature très différente. Durant l'année sous revue, aucun incident n'a toutefois compromis le bon fonctionnement de l'administration fédérale. Les équipes de sécurité des fournisseurs de prestations de l'administration fédérale ont réussi à prévenir les cyberattaques au moyen de diverses mesures. À titre d'illustration, l'équipe d'intervention en cas d'urgence informatique (*computer security incident response team*, CSIRT) de l'Office fédéral de l'informatique et de la télécommunication (OFIT) et le Cyber Fusion Center (CFC) de la Base d'aide au commandement (BAC) ont protégé leurs systèmes contre les cyberattaques en agissant comme suit:

- Dans l'ensemble, la CSIRT de l'OFIT a demandé le blocage de domaines à 116 reprises, invoquant presque toujours le piratage de sites Internet à des fins de diffusion de maliciels ou d'hameçonnage. Elle a procédé à ces blocages en collaboration avec l'équipe d'intervention de la Confédération en cas d'urgence informatique (*computer emergency response team*, GovCERT), rattachée au NCSC. En outre, l'OFIT a signalé que pour certains réseaux, plusieurs pare-feu autorisaient une connexion directe à Internet. Les règles concernées du pare-feu ont été rapidement modifiées après l'identification du problème, et les failles de sécurité ont ainsi pu être comblées immédiatement. Par ailleurs, des lacunes ont été constatées

sur certains serveurs (principalement Linux) pour ce qui concerne la protection contre les maliciels. Les exploitants en ont été informés, et le problème a pu être résolu rapidement.

- En 2022, le CFC de la BAC a traité 559 incidents de sécurité au total, allant du soupçon de maliciel aux tentatives d'hameçonnage. Ces incidents n'étant toutefois jamais critiques, la situation générale peut être décrite comme plutôt calme. Ce calme ressort également du nombre d'incidents signalés et semble durer.

Durant la période sous revue, quelques attaques par déni de service distribué (*distributed denial of services*, DDoS[5]) se sont produites, montrant aux délégués à la sécurité informatique de la Confédération que ce problème restait actuel. Les attaques DDoS consistent à lancer simultanément un grand nombre d'attaques dans le but de créer une surcharge et de provoquer l'indisponibilité de serveurs Web, de services en ligne ou de réseaux tout entiers. À des fins de contre-attaque, un nouveau pare-feu d'application Web (*web application firewall*, WAF) a été déployé et assorti d'une limitation des accès (*rate limiting*). En restreignant le nombre de demandes par adresse IP, il protège l'administration fédérale d'attaques DDoS.

4.2 Vulnérabilités

Le 29 septembre 2021, le NCSC a obtenu la reconnaissance de l'organisation américaine MITRE[6] en tant que service d'autorisation habilité à attribuer un numéro d'identification unique aux vulnérabilités qui lui sont signalées (*common vulnerabilities and exposures*, CVE[7]). À ce titre, le NCSC est responsable de l'élaboration et de la publication d'informations sur les vulnérabilités signalées et de la gestion des numéros correspondants dans le système CVE. Il est ainsi non seulement le service officiel pour les signalements de failles de sécurité en Suisse, mais il est aussi chargé de définir les numéros CVE utilisés dans les échanges internationaux. Depuis sa reconnaissance officielle, le NCSC a publié 30 CVE, dont 15 au cours de l'année 2022.
Hormis la publication de CVE, le NCSC traite aussi les signalements de vulnérabilités pour le compte de l'administration fédérale et d'autres acteurs (cantons, communes, exploitants d'infrastructures critiques et entreprises suisses). Les vulnérabilités des applications et des systèmes comptent parmi les causes principales des incidents de sécurité. C'est pourquoi leur identification et leur élimination rapides revêtent aussi une très grande importance pour l'administration fédérale. En 2022, le NCSC a publié au total 27 avertissements concernant des vulnérabilités importantes ou critiques. Il a également traité les vulnérabilités suivantes, qui présentaient un degré de criticité élevé:

Analyse d'applications pour smartphone
Dans le cadre de la Coupe du monde de football qui s'est déroulée au Qatar, le domaine Transformation numérique et gouvernance de l'informatique (TNI) de la Chancellerie fédérale a, en accord avec le NCSC et l'OFIT, bloqué deux applications sur les téléphones portables professionnels, afin de protéger les collaborateurs et les données de la Confédération.
Requises pour l'entrée au Qatar, les applications «Ehteraz» et «Hayya to Qatar 2022» exigeaient un accès étendu aux données, ce qui a conduit le NCSC à faire une analyse technique des applications, en collaboration avec des services spécialisés de la Confédération. Il a été décidé, à titre préventif, de bloquer ces deux applications sur les

[5] Dans le domaine de la technique de l'information, *denial of service* (DoS) désigne l'indisponibilité d'un service Internet due la plupart du temps à une surcharge du réseau de données. La principale différence entre les attaques DDoS et DoS est que dans le cas des premières, plusieurs systèmes sont utilisés, ce qui permet de surcharger les réseaux et les systèmes avec des volumes de données plus importants.

[6] La MITRE Corporation est une organisation à but non lucratif exploitant des instituts de recherche sur mandat des États-Unis. Elle est née de la scission du Massachusetts Institute of Technology (MIT).

[7] Système de référence servant à nommer les vulnérabilités des systèmes informatiques et à en décrire la criticité

téléphones portables professionnels.

Atlassian Confluence Server
Peu après avoir été identifiée au début de juin 2022, une vulnérabilité critique du produit Atlassian Confluence Server[8] a pu être éliminée au sein de l'administration fédérale grâce à des mises à jour. Un cybercriminel aurait pu exploiter cette faille et exécuter n'importe quel code sur les serveurs Confluence en tant qu'utilisateur non identifié. Après la mise à jour, les systèmes ont fait l'objet d'une analyse visant à identifier d'éventuels signes de compromission. En l'absence de signes de ce genre, les serveurs ont pu être remis en service immédiatement.

Microsoft Exchange Server
À la fin de septembre 2022, une entreprise de cybersécurité vietnamienne[9] a pour la première fois rapporté deux vulnérabilités critiques de type *zero day*[10] dans Microsoft Exchange Server. Pouvant être associées et désignées ensemble par «ProxyNotSchell», ces vulnérabilités ont déjà été exploitées activement dans le monde entier, avant même qu'un correctif officiel ne soit disponible. Dans ce genre de cas, il est particulièrement important de réagir vite et de suivre les recommandations, qui peuvent aller jusqu'à l'arrêt du système concerné, en attendant qu'un correctif officiel soit mis à disposition.
S'ils avaient exploité simultanément les deux failles de sécurité[11], des cybercriminels auraient par exemple pu accéder à des systèmes vulnérables et déployer à distance un code malveillant au moyen d'Internet. Il était donc urgent d'agir, tant dans l'administration fédérale que dans d'autres entreprises.
Selon les informations du fabricant, ces failles de sécurité ne peuvent être exploitées qu'en présence d'un compte déjà authentifié sur le serveur, ce qui réduit la probabilité d'une attaque. Le 8 novembre 2022, Microsoft a publié les mises à jour nécessaires pour supprimer les vulnérabilités. L'administration fédérale les a installées sans délai. Tous les systèmes vulnérables ont en outre été soumis à un examen approfondi, qui n'a cependant révélé aucun signe de compromission.

Vulnérabilité de FortiOS VPN
Le 13 décembre 2022, le fabricant de produits de sécurité Fortinet a signalé une faille de sécurité critique[12] dans le produit FortiOS VPN. L'exploitation de cette vulnérabilité permettait à des utilisateurs non identifiés de bloquer à distance des appareils et éventuellement d'exécuter des codes malveillants. L'administration fédérale a réagi immédiatement après la communication de cette faille en actualisant les systèmes concernés dans les deux jours suivants et en cherchant des indices de compromission. Aucun système compromis n'a toutefois été trouvé.

Failles de sécurité possibles dans les outils de vidéoconférence
Le télétravail s'est durablement fait une place dans le monde professionnel, et des séances et ateliers sont souvent organisés en ligne. L'administration fédérale détermine les «solutions de vidéoconférence» autorisées. Cependant, lors de vidéoconférences, des outils disponibles gratuitement sur Internet sont aussi utilisés (p. ex. des tableaux virtuels ou des outils de sondage ou de planification).
Ces outils peuvent faire courir un risque aux appareils de l'administration fédérale, car les cybercriminels peuvent s'en servir pour lancer des attaques.

[8] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26134

[9] https://ncsgroup.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html

[10] On appelle failles *zero day* des vulnérabilités pour lesquelles il n'existe encore aucun correctif permettant d'empêcher leur exploitation.

[11] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41040
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41082

[12] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42475

Pour écarter ce risque, le secteur TNI de la Chancellerie fédérale est en train d'élaborer, dans le cadre de l'initiative stratégique 2 «Orientation client», un guide ayant caractère de directive pour les outils destinés à la collaboration agile. Les DSIO et DSID sont en outre chargés de sensibiliser les collaborateurs à ce sujet.

Vulnérabilité critique chez Citrix

Le 13 décembre 2022, le fabricant Citrix a signalé une vulnérabilité critique[13] dans ses produits Citrix ADC et Citrix Gateway. Il s'agissait d'une faille d'authentification qui aurait aussi pu permettre l'exécution d'un code malveillant au moyen d'Internet. Étant donné la criticité de cette vulnérabilité, l'administration fédérale a appliqué les correctifs requis à ses systèmes en l'espace de quelques jours. Le système Mobile Device Management (MDM) était notamment concerné.

4.3 Systèmes et protocoles de réseau obsolètes

Le NCSC constate que des systèmes et protocoles de réseau obsolètes sont encore et toujours utilisés dans l'administration fédérale, ce qui augmente considérablement le risque de failles de sécurité.

Leur remplacement ressortit aux responsables des applications des bénéficiaires de prestations au sein des offices et des départements. Or, compte tenu des priorités définies, ces personnes n'ont pas toujours les ressources nécessaires pour remplacer les protocoles et, même après l'évaluation du NCSC, elles ne sont pas forcément conscientes des risques encourus sur le plan de la sécurité. Ceux-ci sont certes mentionnés dans les rapports sur la sécurité des unités administratives et assumés par les différentes directions, mais compte tenu de leur complexité technique, seul un nombre infime de responsables sont conscients des risques informatiques qu'ils acceptent en réalité. Cette méconnaissance peut entraîner un cumul des risques de sécurité. Le NCSC suivra ce problème de près conformément à son mandat de conduite et de coordination en matière de cybersécurité.

Notons toutefois que certains systèmes obsolètes, présents surtout dans les environnements de laboratoires, sont déjà hébergés sur des réseaux isolés et n'échangent pas de données avec les réseaux de la Confédération.

Suppression des versions de protocole obsolètes TLS 1.0 / 1.1

Un sondage de l'OFIT a permis d'identifier différentes interfaces utilisant les versions obsolètes des protocoles d'authentification et de chiffrement TLS 1.0 et TLS 1.1. TLS[14] est un protocole visant à garantir la confidentialité et l'intégrité des données transmises sur des réseaux. Étant donné que les versions TLS 1.0 et TLS 1.1 sont obsolètes et comportent des vulnérabilités, l'exploitation de systèmes utilisant ces versions de protocole n'est plus autorisée dans l'administration fédérale. La plupart de ces protocoles ne se trouvent toutefois pas dans les liaisons https[15] ordinaires, mais sont présents dans des protocoles propriétaires qui utilisent également TLS. La large diffusion de TLS dans les produits les plus divers représente un défi de taille, et la résolution de cette situation est à la fois compliquée et chronophage (elle pourrait durer jusqu'à la fin de 2026).
En résumé, 1786 systèmes équipés d'une version obsolète du protocole sont encore utilisés activement au sein de l'administration fédérale. On peut en revanche se réjouir que durant l'année 2022, le nombre de versions obsolètes TLS 1.0 et 1.1 qui ont été mises à jour est quasiment égal à celui des versions obsolètes encore en usage. Le risque peut être

[13] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27518

[14] Acronyme de *transport layer security*

[15] Acronyme de *hypertext transfer protocol secure*, qui désigne un protocole de communication sur le Web grâce auquel les données peuvent être transmises confidentiellement

considéré comme limité tant que les versions obsolètes de TLS ne servent qu'à la communication interne et que les systèmes concernés ne sont pas accessibles par Internet.

Recommandations concernant la gestion des versions de protocole obsolètes
Le NCSC recommande aux fournisseurs de prestations d'agir comme suit:
Pour procéder à une élimination systématique et généralisée, il convient, au besoin, de bloquer toutes les versions de protocole obsolètes et de les autoriser ensuite de façon contrôlée et individuelle pour les systèmes qui sont indispensables, en se fondant sur un plan de migration conçu à cet effet. Une solution pourrait par exemple être de déplacer ces systèmes dans un environnement réseau isolé, de manière à éviter tout échange de données avec d'autres systèmes informatiques de l'administration fédérale.

5 Synthèse des fournisseurs de prestations internes

D'une manière générale, les fournisseurs de prestations informatiques internes de la Confédération considèrent que l'année 2022 a été plutôt calme sur le front des cybermenaces. Du point de vue global, la cybersécurité est toutefois une préoccupation de plus en plus essentielle. Les thèmes abordés en 2021 revêtent toujours la même importance et restent d'actualité. Il est en outre apparu une nouvelle fois que le respect des cycles de vie et la gestion des correctifs étaient indispensables à la protection des systèmes informatiques. Un très grand nombre d'attaques visent des composants pour lesquels il n'y a pas eu de correctif ou de solution de rechange depuis quelque temps.
Les fournisseurs de prestations estiment qu'il est primordial de vérifier les droits d'accès aux systèmes et garantir la sécurité informatique dans les environnements de développement pour éviter que les failles de sécurité ne se retrouvent dans l'environnement de production.
Les services en nuage faisant l'objet d'une utilisation accrue, l'exigence d'une collaboration sûre et efficace s'impose de plus en plus, notamment lors des clarifications menées après un incident avec différents fournisseurs de nuages. Compte tenu des tensions actuelles sur la scène internationale, les fournisseurs de prestations s'inquiètent des conséquences d'une pénurie d'électricité et, le cas échéant, de la disponibilité de leurs systèmes informatiques.
Dans le cadre du déploiement de DevSecOps[16], plusieurs fournisseurs de prestations ont commencé à engager des *security champions* pour la mise en œuvre de projets agiles intégrant la sécurité informatique. Les *security champions* assistent les *product owners* et les chefs de projets et veillent à ce que la sécurité soit prise en compte dès le développement des projets et devienne ainsi automatiquement un composant du produit (approche *security by design*). Dans les projets agiles, l'importance de la sécurité est croissante, car le développement des produits est réalisé en continu. Au lieu d'être associée à des étapes ordinaires du projet, la sécurité informatique devient un processus de développement qui nécessite une surveillance permanente.
Durant l'année sous revue, les fournisseurs de prestations ont commencé la mise en œuvre du programme «Mitigation Credential Theft – MCT», qui vise principalement à empêcher l'installation de logiciels indésirables.
Dans ce contexte, le déploiement d'un logiciel permettant une gestion privilégiée des accès (*privileged access manager*, PAM) a été prescrit sur tous les systèmes bureautiques, conformément à la nouvelle directive sur la protection informatique de base (version 5) et à la directive d'application E033 sur la protection de l'identité. En 2022, un outil de gestion a donc été déployé sur cette infrastructure, et son exploitation productive a démarré pour l'administration des serveurs Windows. Une démonstration de faisabilité (*proof of concept*, PoC) a en outre été réalisée pour les systèmes Linux, de sorte que l'exploitation productive

[16] Acronyme de *development*, *security* et *operations*

puisse aussi être lancée en 2023 pour la gestion de ces systèmes.

6 Renforcement de la sécurité informatique

L'administration fédérale prend les mesures de sécurité qui s'imposent sur la base des évaluations de la situation et des incidents de sécurité qu'elle réalise en permanence. Outre les éventuelles mesures immédiates, des mesures d'ordre juridique, organisationnel et technique sont élaborées et appliquées durablement et de façon proportionnée.

6.1 Mesures prises en 2022

En 2022, tous les départements et la Chancellerie fédérale ont arrêté des mesures et entrepris des actions pour renforcer leur sécurité informatique.

Ces mesures et actions ont notamment revêtu les formes suivantes:

- Les collaborateurs ont été informés des différentes mesures par plusieurs voies (campagne nationale de sensibilisation S-U-P-E-R[17], campagnes contre l'hameçonnage, publication d'informations sur l'intranet concernant des thèmes comme le télétravail, les voyages à l'étranger et la protection des données – des mesures parfois interdépartementales) et sensibilisés à la cybersécurité en général.
- Le projet Endpoint Detection and Response (EDR)[18] a été lancé au sein du DFAE. Son objectif consiste en l'installation d'une solution EDR sur le plus grand nombre possible de systèmes de l'administration fédérale.
- Le programme Security Champions a débuté. Il porte sur la réalisation de projets agiles.
- Le projet DigiSec a été lancé. Il a pour objet la production d'une application destinée à la mise en œuvre d'un système de gestion de la sécurité de l'information (ISMS) dans toute l'administration fédérale.
- Le déploiement d'ISMS s'est poursuivi dans différentes unités administratives.
- La certification externe selon la norme ISO 27001, qui vise à garantir la sécurité informatique, a suivi son cours dans certaines unités administratives.
- Le NCSC a lancé un programme de primes aux bogues au sein de l'administration fédérale[19].
- La norme «securitxt.txt» a commencé à être introduite dans les pages Internet de l'administration fédérale. Elle a pour objectif d'améliorer le signalement de vulnérabilités[20].
- Les ressources humaines dédiées à la sécurité informatique ont été renforcées.
- Le programme de prévention de l'usurpation d'identité «Mitigation Credential Theft – MCT» s'est poursuivi.
- Le service de signature de macros, qui réduit considérablement les risques liés aux macros de MS Office, a été mis sur pied.

[17] https://www.s-u-p-e-r.ch/fr/

[18] L'expression *endpoint detection and response* (EDR) désigne une catégorie d'outils et de techniques qui permettent d'identifier rapidement les menaces actives sur les terminaux et d'y réagir au mieux.

[19] Programmes de primes aux bogues visant à augmenter la cyberrésilience de l'administration fédérale (admin.ch)
https://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/medienmitteilungen/newslist.msg-id-89868.html

[20] https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-behoerden/aktuelle-themen/security-txt.html

6.2 Mesures prévues pour 2023

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

- extension des analyses mensuelles (*Web scans*) de toutes les pages Web exposées à des risques afin d'éliminer les vulnérabilités identifiées;
- reprise d'autres applications essentielles dans le programme de primes aux bogues et, en parallèle, vérification proactive des éventuelles vulnérabilités touchant ces applications;
- formations et campagnes de sensibilisation aux risques;
- réalisation de tests de pénétration sur les systèmes accessibles par Internet et exécution des mesures qui s'imposent;
- établissement d'un ISMS répondant aux exigences de la LSI et de la norme ISO 27001;
- remplacement du logiciel de chiffrement de la Confédération «SecureCenter» par son successeur «CHCrypt».

Le NCSC devient un office fédéral

La cybersécurité est devenue une préoccupation majeure ces dernières années à tous les échelons et, par conséquent, une tâche indispensable de la Confédération. Compte tenu de l'importance croissante du NCSC, le Conseil fédéral a décidé, le 2 décembre 2022, de transformer ce centre en un office fédéral et de le rattacher au DDPS. Le NCSC continuera à assumer les tâches clés en matière de cybersécurité, dont l'assistance des infrastructures critiques dans la gestion des cyberincidents, la mise à disposition d'un service national de liaison pour la population et les entreprises, la diffusion d'informations et d'avertissements concernant les cybermenaces et les mesures à appliquer pour s'en protéger, la sensibilisation de la population, la gestion des vulnérabilités et la protection des systèmes de l'administration fédérale[21].

[21] Le NCSC devient un office fédéral: https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-92048.html