AFCDP

CORRESPONDANT INFORMATIQUE ET LIBERTÉS
BIEN PLUS QU'UN MÉTIER

AFCDP

CORRESPONDANT INFORMATIQUE ET LIBERTÉS

BIEN PLUS QU'UN MÉTIER

www.afcdp.net

Ce texte est l'un des chapitres du livre « Correspondant Informatique et Libertés : bien plus qu'un métier », publié par l'AFCDP en 2015.

SÉSAME, OUVRE-TOI !

par Bruno RASLE

Et si, en termes de sécurité des données à caractère personnel, on commençait par la base, c'est-à-dire le mot de passe ? Le couple identifiant-mot de passe (login-password) est de loin la solution de contrôle d'accès logique la plus répandue. Pourtant nous avons tous connaissance des imperfections de ce dispositif simple et ancien : mots de passe notés sur un petit bout de papier ou sur un tableau blanc, mots de passe identiques pour accéder à plusieurs services, mots de passe faibles et jamais changés, mots de passe transmis en clair avec l'identifiant, mot de passe communiqué à des collègues… Dans son principe même, le mot de passe présente de multiples défauts : il est difficile d'en retenir plusieurs, il est facile à deviner si faible et difficile à retenir si fort, il est facile à espionner lors de la saisie, il peut être intercepté, aucun signal ne nous alerte si quelqu'un se l'est approprié … et pourtant, malgré tous ces inconvénients, la plupart des contrôles d'accès logiques l'utilise, bien que certains annoncent régulièrement sa mort prochaine. Au-delà de ces annonces pas toujours désintéressées, ce chapitre vise à donner à un Correspondant Informatique et Libertés les connaissances élémentaires lui permettant de se faire sa propre opinion quant à la pertinence de ce mode de protection d'accès[1], à l'heure où une série de délibérations de la CNIL met l'emphase sur des défauts de sécurité. Ce texte a aussi pour ambition de responsabiliser les utilisateurs, car, comme le rappelle Bernard Foray dans son ouvrage « La Fonction RSSI, Guide des pratiques et retours d'expérience » (Dunod, 2007), « Le mot de passe, c'est la première pierre de la construction d'une culture sécurité ».

Pas une semaine ne se passe désormais sans qu'une décision de justice, une délibération de la CNIL où une actualité ne montre que les enjeux liés à la protection des données à caractère personnel et à la conformité à la loi Informatique et Libertés méritent désormais d'être considérés à leur juste mesure par les directions des entreprises.

Ainsi, au détour de la nouvelle loi Consommation[2], la Commission Nationale Informatique et Libertés s'est vue dotée d'un nouveau pouvoir de contrôle, à distance. Ses agents peuvent constater les non-conformités, de leurs bureaux, par la simple visite d'un site Web[3]. La constatation des indexations de données personnelles « sensibles » par les moteurs de recherche ne nécessitera plus de mission de contrôle sur place (on pense ici, par exemple, aux données de patients qui avaient été indexées par le moteur de recherche Google car librement accessibles[4], ce qui a donné lieu, courant 2013, à plusieurs contrôles de la CNIL). La Commission pourra ainsi rapidement constater et agir en cas d'incident de

---

[1] Ce texte est focalisé sur l'identification d'utilisateurs, mais il convient de ne pas oublier les mots de passe « applicatifs », par exemple utilisés par les applications pour accéder aux bases de données. Optimiser la gestion de ses mots de passe « humains » sans se pencher sur celle des mots de passe embarqués dans les applications équivaut à renforcer sa porte d'entrée et laisser une fenêtre ouverte à l'arrière de sa maison. Maintes applications ont accès aux bases de données qui hébergent les données les plus stratégiques pour les entreprises. Logiquement, ces mots de passe doivent être protégés, modifiés régulièrement et rester inconnus des développeurs. La réalité est malheureusement souvent autre.

[2] Loi n° 2014-344 du 17 mars 2014 relative à la consommation

[3] *CNIL, Un pouvoir d'investigation renforcé grâce aux contrôles en ligne*, disponible sur http://www.cnil.fr/linstitution/actualite/article/article/un-pouvoir-dinvestigation-renforce-grace-aux-controles-en-ligne/, mars 2014

[4] T. Duvernoy et L. Minano, *Enquête : des données médicales confidentielles accessibles sur le web*, Actusoins, 1er mars 2013

sécurité sur Internet exposant des données personnelles. Elle pourra aussi vérifier la conformité des mentions d'information figurant sur les formulaires en ligne ou les modalités de recueil de consentement des internautes en matière de prospection électronique. On peut imaginer que ses agents en profiteront pour s'intéresser aux processus d'identification et d'authentification[5], et de constater, par exemple, qu'un site adresse à l'utilisateur, dans un seul courriel en clair l'ensemble des informations : nom, prénom, identifiant et mot de passe. La CNIL précise toutefois qu'il n'est pas question qu'elle tente des intrusions aux systèmes d'information, dans le respect de la loi Godfrain[6].

Une décision du Tribunal de grande instance de Paris[7] a également été remarquée : le juge a estimé que la société victime a participé à la réalisation de son propre préjudice. Certes, le pirate a été puni... mais la sanction financière qui devait être de 100.000 € à son encontre a été « allégée » par le juge à hauteur de 30.000 € car, pour ce dernier, la société avait participé à la réalisation de son propre préjudice en sécurisant de façon insuffisante l'accès aux adresses électroniques de ses clients et prospects. Cette décision est sans doute à marquer d'une pierre blanche, comme l'avait été en son temps celle de la Cour de cassation (chambre criminelle) en octobre 2001[8]. La Cour « a condamné le premier à 50.000 francs d'amende et le deuxième à 30.000 francs d'amende… que le système informatique mis en place n'assurait pas une protection suffisante de la confidentialité des données enregistrées ; Jean C., président du SIMTPA et Jean-Claude D. directeur de ce syndicat …que le fait qu'à un moment donné, la mauvaise utilisation des mots de passe ait pu permettre à des administratifs de prendre connaissance des données médicales recueillies dans le système, constitue en l'espèce le seul délit de l'article 42 de la loi du 6 janvier 1978 devenu 226-16 du Code pénal. »

Ce jugement est ancien. Les choses ont-elles évolué depuis ? Lors de son intervention donnée dans le cadre des JSSI 2013 de l'OSSIR et intitulée « Retours d'expérience sur des campagnes d'audit de sécurité[9] », Patrick Chambet, RSSI de C2S, a présenté les dix vulnérabilités les plus fréquemment relevées au sein du Groupe Bouygues (ce qu'il appelle le *Wall of shame*). En premier vient « Mots de passe par défaut / triviaux », l'on trouve « Stockage non sécurisé de mots de passe » en huitième position et « Post-it® trouvés dans des endroits inattendus » vient en dixième position. Dans les leçons à en tirer et les bonnes pratiques à faire progresser figure « Définir et mettre en œuvre des politiques de mots de passe… encore et toujours ». Et c'est probablement une telle situation que les agents de la CNIL ont relevée lors des contrôles qu'ils ont effectués courant 2012 au sein de la Fédération Française d'Athlétisme (FFA). La délibération de la formation restreinte n° 2014-293 du 17 juillet 2014 – qui formalise une sanction de 3.000 € avec publicité – indique que « la sécurité du système d'information de la FFA, qui comprend environ un million de personnes, et de l'espace de l'athlète sur le site Web FFA était insuffisante », épingle « la robustesse des mots de passe permettant d'accéder au système d'information » et estime « que la modification des paramètres afin d'imposer une robustesse et un renouvellement des mots de passe permettant l'accès aux systèmes d'information sont des mesures de sécurité élémentaires ».

---

[5] Par convention et dans le cadre de ce texte, le contrôle d'accès logique par simple mot de passe est dénommé identification, et non authentification. Cette dernière suppose que l'utilisateur fasse la « preuve » de son identité, et la fourniture d'un simple mot de passe ne répond pas à cette exigence. Pour justifier l'utilisation du vocable « authentification », ne faudrait-il pas un procédé plus robuste ? À titre d'exemple, le contrôle d'accès logique mis en place par l'ASIP Santé (par identification puis *One Time Password*), est qualifié par la CNIL d'authentification dans sa délibération n° 2013-096 du 25 avril 2013, autorisant la mise en œuvre, à titre expérimental, du service national de messagerie sécurisée de santé : « les mesures mises en place apparaissent conformes aux dispositions de l'article L110-4 du code de la santé publique, [et] sont de nature à garantir une authentification fiable des émetteurs et destinataires des messages ».

[6] Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique

[7] Tribunal de grande instance de Paris 3e section, 4 e chambre Jugement du 21 février 2013

[8] Cour de cassation, chambre criminelle, Audience publique du mardi 30 octobre 2001, n° de pourvoi: 99-82136, Le Syndicat National Professionnel des Médecins du Travail, partie civile

[9] www.ossir.org/jssi/jssi2013/1A.pdf

« Tu m'aimes, je t'aime : partageons notre mot de passe ! »

Le mot « secret » est étrange… D'après sa définition, une chose secrète doit rester strictement confidentielle, ne doit jamais être partagée avec un tiers, ne doit jamais être divulguée… Pourtant, trop souvent, les utilisateurs n'hésitent pas à communiquer leurs mots de passe à un ami, un collègue, voire à un supérieur hiérarchique. Ainsi, selon une étude menée fin 2011, 30 % des adolescents américains partageraient leurs mots de passe avec leur petit(e) ami(e)[10]. Par ailleurs, certains employeurs américains exigent des candidats l'accès total à leur compte personnel MySpace ou Facebook, notamment pour vérifier s'ils ne sont pas liés à des gangs. Des États envisagent de légiférer pour mettre le holà à cette pratique. Les administrateurs informatiques n'ont pas non plus à connaître les mots de passe des utilisateurs. En temps normal, ils n'ont aucunement besoin de ces droits et ne doivent pas commettre d'usurpation de personnalité[11]. Les administrateurs doivent résister à d'éventuelles injonctions hiérarchiques à violer le secret des mots de passe des utilisateurs.

Voici quelques affaires qui se sont déroulées plus près de chez nous. En 2012, une brigadière de police a été écrouée. Elle renseignait son amant, un dealer présumé de Seine-Saint-Denis, grâce à des consultations du fichier STIC (Système de Traitement des Infractions Constatées) et des cartes grises. Pour détourner les soupçons, elle prenait soin d'utiliser le mot de passe que lui avait confié une collègue naïve[12]. Trois ans auparavant, la CNIL avait pourtant formulé des constats à ce sujet, qu'elle avait formalisés dans son document « Contrôle du STIC : Les propositions de la CNIL pour une utilisation du fichier plus respectueuse du droit des personnes ». Au sein du chapitre « Définir une politique de gestion des habilitations et des mots de passe plus stricte » on relève le passage suivant : « La CNIL constate que si la traçabilité des accès et des connexions au STIC est techniquement possible, cette fonction de contrôle n'est pratiquement jamais utilisée (seulement 120 contrôles en 2008). Aucun système d'alerte en temps ne permet de détecter des utilisations anormales de cet énorme fichier auquel 100.000 fonctionnaires peuvent accéder et qui donne lieu à 20 millions de consultations par an. »

En 2001, l'adjoint du directeur technique d'une régie publicitaire, avait été licencié pour faute grave pour avoir tenté, par emprunt du mot de passe d'un autre salarié, de se connecter sur le poste informatique du directeur de la société. La Cour de cassation a rejeté son pourvoi et l'a condamné aux dépens[13]. En 2006, une secrétaire commerciale avait été également licenciée pour faute grave. Devant partir à son cours de gymnastique, elle avait transmis son mot de passe à un collègue, en infraction de la charte informatique de l'entreprise. Contestant son licenciement, elle a saisi la juridiction prud'homale de demandes indemnitaires. La Cour de cassation a considéré que le non-respect volontaire par un salarié de la charte informatique rend impossible son maintien dans l'entreprise et justifie un licenciement pour faute grave[14].

Par un arrêt du 25 mars 2014[15], la Cour d'appel de Versailles a condamné une société de maintenance à la suite du piratage du système de téléphonie d'une de ses clientes et de nombreux appels émis vers le Timor Oriental. La société de maintenance qui avait pourtant, une fois informée du piratage, mis en

---

[10] *Young, in Love and Sharing Everything, Including a Password*, The New York Times, par Matt Richtel, 17 janvier 2012.

[11] Pour cette même raison, durant un contrôle sur place de la CNIL, il est sain de créer des droits spécifiques aux agents effectuant la mission, pour leur permettre d'accéder aux ressources et pour ne pas « polluer » la traçabilité des accès et des actions.

[12] Le Nouvel Observateur, *La policière et le dealer, couple improbable dans une affaire de stup*, 26 octobre 2012

[13] Cassation sociale 21 décembre 2006 n° 0541165

[14] Cour de cassation, chambre sociale, Audience publique du mardi 5 juillet 2011, n° de pourvoi : 10-14685

[15] www.legalis.net/spip.php?page=jurisprudence-decision&id_article=4083

œuvre un plan d'intervention rapide permettant de sécuriser les lignes, a été condamnée pour manquement à ses obligations contractuelles. La Cour conclut qu'il appartenait à la société de maintenance « de vérifier l'état de sécurisation de l'installation téléphonique de sa cliente et de vérifier que celle-ci utilisait l'installation dans des conditions optimales de sécurité et d'efficacité qu'elle devait s'assurer qu'elle était informée de la nécessité de modifier son mot de passe régulièrement ». Les constatations montraient que l'installation téléphonique n'avait jamais été valablement sécurisée puisqu'elle comportait toujours le mot de passe par défaut…00000.

On rappellera que l'utilisation des mots de passe peut servir à des fins de preuve. C'est une pratique insérée dans le code civil à l'article 1316-2 par la loi 2000-230 du 13 mars 2000, article 1 : « Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous les moyens le titre le plus vraisemblable, quel qu'en soit le support ». C'est la raison pour laquelle on relève fréquemment ce type de clause au sein des contrats de service ou au sein des chartes « la saisie du mot de passe confidentiel remis à l'utilisateur, vaudra preuve de l'utilisation du système entre les parties ». Ceci a été confirmé par l'arrêt de la Cour de cassation, Chambre civile 1 du 8 janvier 2009 (06-17.630, Inédit) et au niveau européen par l'arrêt T-333/99 du 18 octobre 2001 (X c. Banque Centrale Européenne).

Le choix judicieux de l'identifiant

On trouve peu de littérature sur ce sujet. Pourtant l'identifiant (encore appelé login ou compte) est l'un des éléments qui doivent être fournis par l'utilisateur pour « montrer patte blanche ». Soit l'identifiant est une valeur « publique » - le cas le plus fréquent est l'adresse email, mais on pense aussi au numéro de téléphone portable souvent utilisé pour se connecter à son compte personnel chez son opérateur de téléphonie mobile[16] - soit il s'agit d'un élément arbitraire fourni par l'organisme qui gère la ressource[17]. Cette dernière approche est illustrée par les banques, mais aussi par le ministère des Finances : toute personne qui souhaitait déclarer ses revenus de l'année 2013 en ligne devait commencer, pour obtenir un mot de passe, par saisir non pas un seul identifiant mais trois : son numéro fiscal, son numéro de télédéclarant et son revenu fiscal de référence. Ce dernier numéro se trouvant sur le dernier avis d'impôt, on conçoit la difficulté pour un cybercriminel de prendre connaissance de l'ensemble de ces différentes composantes. Dans ce dernier cas, il ne lui suffit pas de deviner le mot de passe, mais bien le couple identifiant et mot de passe. En première approche la CNIL s'était montrée réservée sur ce procédé. Dans un avis rendu public en 2006, elle craignait que ce dispositif entraîne un affaiblissement du niveau de sécurité du dispositif et avait demandé que cela reste exceptionnel et ponctuel dans le cadre de la télédéclaration des revenus. Le bilan présenté par le ministère des finances a dû être convaincant et la méthode permet d'alléger considérablement les serveurs de la direction générale des impôts, qui n'ont plus à gérer de certificats électroniques. Compte tenu de sa sensibilité et de la doctrine de la CNIL, on écartera bien sûr la possibilité d'utiliser le NIR comme identifiant de connexion (login).

[16] Certains comptes clients des opérateurs de téléphone mobiles sont protégés par un identifiant qui correspond au numéro de téléphone, et par un mot de passe composé seulement de quatre chiffres. Une intrusion permet à un pirate de lire le journal des appels et des SMS, de changer le téléphone associé au compte (et donc recevoir les appels/SMS du compte), d'acheter un nouveau téléphone avec la carte bancaire associée au compte, de changer le mot de passe ainsi que l'adresse mail du compte. Ce type de faille est utilisé par les pirates pour récupérer les mots de passe à usage unique (*One Time Password*) envoyés sur les téléphones mobiles de leurs victimes.

[17] Et dans ce cas, la confidentialité de cet identifiant doit également être préservée. On remarque ainsi que la saisie de cet élément, sur la page d'identification des clients de Free afin d'accéder à leur espace personnel, se fait par un clavier virtuel, alors que la saisie du mot de passe se fait de façon traditionnelle.

Le mot de passe, pierre angulaire de la majorité des dispositifs d'identification

Un mot de passe est un moyen d'identification qui permet d'utiliser une ressource ou un service – ou de prendre connaissance d'une information – dont l'accès logique est limité et protégé[18]. Le mot de passe est le secret[19] qui permet à la ressource de vérifier que l'utilisateur qui vient de saisir son identifiant est bien légitime à accéder. Une bonne analyse ne doit donc pas se limiter à l'étude du mot de passe, mais bien au couple « identifiant + mot de passe » (ces éléments sont appelés « crédentiels »).

Pour cette étude, nous prenons pour postulat qu'une analyse de risques préalable et une analyse de valeurs ont été menées, et que leurs conclusions ont permis de mettre en place un contrôle d'accès logique par identification par simple saisie d'un identifiant et d'un mot de passe. En présence de risques d'un niveau supérieur, d'autres approches doivent être étudiées, comme la possession, en sus, d'un élément physique (par exemple, dans le domaine de la santé, la CPS – Carte du Professionnel de Santé), l'ajout d'un OTP[20], voire le recours à la biométrie.

Il peut arriver que le « mot » de passe soit en fait une véritable phrase : les Anglo-Saxons utilisent alors le terme de *passphrase*[21] (phrase de passe – mais ce terme n'est pas usité en français). La plus célèbre des *passphrase* est celle utilisée dans le conte Ali Baba et les Quarante Voleurs : « Sésame, ouvre-toi ! ».

La composition et la longueur du mot de passe sont des éléments cruciaux pour la sécurité[22]. Un mot de passe trop court[23] ou constitué uniquement de lettres peut s'avérer facile à découvrir par un cybercriminel[24], comme nous le verrons plus loin. Dans son document « Recommandations de sécurité relatives aux mots de passe[25] », l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) indique deux approches permettant de se créer un mot de passe résistant ET facile à retenir. La méthode phonétique consiste à utiliser les sons de chaque syllabe pour fabriquer une phrase facile à retenir. La phrase « J'ai acheté huit cd pour cent euros cette après-midi » deviendra ght8CD%E7am[26]. La méthode des premières lettres consiste à garder les premières lettres d'une phrase (citation, paroles de chanson...) : la citation « un tiens vaut mieux que deux tu l'auras » donnera 1tvmQ2tl'A.

---

[18] Les parents d'une jeune américaine de sept ans ont posté la photo de la note que leur fille avait déposée à leur attention sur l'ordinateur familial. Le couple avait osé annoncer qu'il comptait restreindre son accès à Internet. Le mot disait : « Si vous mettez un mot de passe, je ferais de votre vie un enfer ! ». Disponible sur www.huffingtonpost.com/2012/05/16/girl-leaves-parents-note-computer-password_n_1522528.html

[19] Trois types de secret peuvent être produits pour « montrer patte blanche » : ce que l'on sait (comme le mot de passe), ce que l'on a (un badge, une clé physique, une carte à puce), ce que l'on est (biométrie). L'identification par mot de passe est faible, car elle ne met en œuvre qu'un seul type de secret.

[20] *One-time password* : Mot de passe à usage unique, valable pour une seule identification, généralement transmis via SMS.

[21] On imagine que c'est la méthode appliquée par les utilisateurs qui doivent s'identifier grâce à un mot de passe comportant ...24 caractères mis en place en 2014 à la suite de la demande de la CNIL dans le cadre d''un dispositif de *whistleblowing* (dispositif d'alerte) qui était soumis à son autorisation.

[22] Concernant la « résistance » des différentes structures de mots de passe, on se reportera utilement à l'article *Password strength* de Wikipedia dans sa version en langue anglaise.

[23] Dans sa délibération du 5 juillet 1988, la CNIL jugeait insuffisantes les mesures de sécurité qu'avait prises le syndicat hôtelier qui permettait à ses membres de mettre en commun, via Minitel, le signalement des clients qui partaient à la cloche de bois. Le service vidéotex était protégé par un mot de passe composé de quatre caractères : la Commission préconisait, à l'époque, le recours à des mots de passe d'au moins 6 caractères. Nostalgie…

[24] Jusqu'en 2010 (apparition de la version Oracle 11g), les mots de passe acceptés par Oracle n'étaient constitués que de lettre majuscules. Source : www.oracle-base.com/articles/11g/case-sensitive-passwords-11gr1.php

[25] La version du 5 juin 2012 est disponible sur http://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf

[26] Dans son guide pratique Sécurité, la CNIL donne pour exemple « un Chef d'Entreprise averti en vaut deux » pour mémoriser 1Cd'Eaev2.

Mais ces critères ne sont pas les seuls à prendre en compte : ainsi, le code PIN associé aux cartes bancaires ne comporte que quatre chiffres, ce qui, isolé, correspond à une faiblesse extrême mais que d'autres dispositions viennent équilibrer. La durée de vie est l'un des autres paramètres qui influe sur sa résistance (un mot de passe est d'autant plus robuste qu'il est changé régulièrement), de même que les modalités de transmission, de connexions et de gestion de ces mots de passe.

Il peut être intéressant, au moment où l'utilisateur crée son mot de passe personnel, de vérifier la complexité du mot de passe et d'afficher une indication de sa résistance. Le vérificateur peut alors valider que le mot de passe comprend bien le nombre minimal requis de caractères (par exemple huit), qu'il est constitué à partir de caractères de types différents (lettres minuscules, lettres majuscules, chiffres et caractères spéciaux[27]), qu'il n'a aucune correspondance avec le nom du compte (l'identifiant) ni l'appellation de la ressource protégée et qu'il diffère des précédents mots de passe.

Faut-il interdire certaines combinaisons ?

Dans les cas où le choix du mot de passe est laissé à l'utilisateur[28] (mot de passe personnel), il convient de rendre impossible certaines combinaisons trop évidentes, qui pourraient être facilement trouvées par un cybercriminel[29]. Fréquentes sont les études qui montrent que les mots de passe les plus populaires sont « 123456 », « password », « azerty », ou tout simplement l'identifiant, voire même un blanc[30].

Le magazine Capital, dans son édition d'avril 2007[31], a épinglé plusieurs sites Web insuffisamment protégés : « Pas très imaginatifs les administrateurs du Web des Deux-Alpes ! Ils ont choisi, comme code secret, le mot « admin », à l'image de bien de milliers d'autres gestionnaires de sites. Une fois la place investie, nous avons modifié le prix des forfaits… ». Selon une étude parue en 2006[32], 13 % des mots de passe serveurs et routeurs n'ont jamais été modifiés et possèdent encore le mot de passe par défaut qui figure dans le manuel d'installation[33]. Ainsi, toutes les bases de données Oracle sont livrées avec plusieurs comptes par défaut. L'un d'entre eux, baptisé « Scott » a pour mot de passe « tiger » ... ce qui correspond au nom du chat de la sœur de Bruce Scott, l'un des tout premiers développeurs de la base de données. Ceci explique que l'une des premières tentatives d'un pirate essayant de s'introduire dans une base de données Oracle pour en prendre le contrôle ou en exfiltrer le contenu, est de tenter tout simplement de se connecter sur le compte *Scott* avec le mot de passe *tiger*. Comme l'indique Marc Gavini[34], « Il ne faut pas créer cet utilisateur en production... changez au moins son mot de passe. Inutile de faciliter la tâche des hackers ».

---

[27] L'expert Jesper M.Johansson fait plaisamment remarquer que le mot de passe « Mot 2 passe » respecte scrupuleusement cette contrainte, tout en présentant une faiblesse conceptuelle.

[28] Mot de passe imposé ou personnel ? La tendance est actuellement de laisser l'utilisateur composer son propre mot de passe. Cela n'a pas toujours été le cas. Ainsi, dans l'une de ses délibérations datant du 5 juillet 1988 (relative à une liste noire mise en place par le syndicat hôtelier), la CNIL avait suggéré de préférer des mots de passe générés à partir de chaînes de caractères aléatoires, plutôt que de laisser les utilisateurs les choisir eux-mêmes.

[29] Les informations postées par les utilisateurs sur les réseaux sociaux sont mises à profit par les pirates, qui y trouvent facilement des éléments liés au vécu de la personne (date et lieu de naissance, hobby, etc.) que celle-ci aurait pu utiliser pour concevoir son mot de passe.

[30] En mars 2014, la CNIL a posté une page spécifique intitulée « Comment construire un mot de passe sûr et gérer la liste de ses codes de sécurité ? ». Cette page cite une étude selon laquelle 17 % des internautes utilisent leur date de naissance comme mot de passe, alors que le secret ne devrait pas avoir de lien avec son détenteur.

[31] « Comment je suis entré par effraction chez… » par Damien Bancal

[32] *US Privileged Password Survey*, septembre 2006, Cyber-Ark

[33] Et sur plusieurs sites Web, dont www.phenoelit.org/dpl/dpl.html

[34] *Oracle: Exploitation de bases de données en environnement de production sous Unix*, par Marc Gavini, Editions ENI, 2011

Dans un papier intitulé *Why Your Data Breach Is My Problem*[35], les chercheurs Stefan Frei et Bob Walder indiquent qu'à force d'être exposées lors de *Data Breach*, certaines données très personnelles – et ne pouvant pas être changées –, comme la date de naissance et le numéro de sécurité sociale[36], seraient condamnées à moyen terme à être considérées comme « publiques » : ces données ne pourraient donc plus être utilisées comme des éléments fiables d'identification, les cybercriminels ayant pris l'habitude de collecter soigneusement et de « croiser » les informations obtenues[37].

Enfin, il faut en finir avec le dogme des « mots de passe de 8 caractères » : comme l'a montré une étude publiée en 2011[38], un mot de passe de 16 lettres présente un bien meilleur ratio résistance/ergonomie[39] qu'un mot de passe de 8 caractères, composé avec des lettres minuscules et majuscules, des chiffres et des signes spéciaux. Avec une résistance quasiment identique, la seconde approche fait peser une charge bien moins lourde sur l'utilisateur. Il ne faut donc pas hésiter à sortir du postulat du mot de passe de 8 caractères complexes, mais plutôt chercher à trouver le « bon équilibre » et une solution qui apporte le niveau de sécurité adéquat et suffisant sans créer de frustration pour le détenteur du mot de passe. Des tests ergonomiques s'imposent pour mesurer les oublis de mots de passe, les erreurs dans leur saisie, voire les abandons au moment de leur création.

Cette étude indique aussi la distribution de l'utilisation des caractères spéciaux dans les mots de passe[40]. Au lieu d'être égales, les fréquences vont d'un rapport de 1 pour le signe « > » à 362 pour le signe « @ » en passant par 345 pour le signe « ! ». La troisième position est détenue par le signe « $ » (mais les répondants étaient américains). Cette même étude cite une idée déjà exprimée l'année précédente par S.Schechter, C.Herley et M. Misenmacher dans leur article *Popularity is everything: A new approach to protecting passwords from statistical-guessing attacks* : lors de la création du mot de passe, il conviendrait de refuser ceux qui sont déjà trop souvent utilisés par d'autres personnes (sur le modèle de ce qui est fait pour les identifiants : il est impossible à deux utilisateurs d'avoir le même).

Pour sourire, signalons deux anecdotes qui illustrent notre propos : en juin 2010, la chaîne de télévision TF1 diffuse un reportage sur la correction de l'épreuve du baccalauréat. A l'écran, une représentante de l'académie de Versailles insiste sur les précautions de sécurité qui sont prises par le ministère pour empêcher toute tentative de fraude. Derrière elle, sur un tableau blanc, on relève l'inscription suivante : « identifiant : vpc2010 mot de passe : m151307 », ainsi que l'URL de la ressource sensible[41]... En 2010 également, on a appris que l'équipe du Président Bill Clinton avait perdu les codes déclenchant le feu nucléaire à la fin des années 90[42]. Ces codes sont supposés être en permanence à la disposition du locataire de la Maison-Blanche. C'est au moment de leur remplacement que le collaborateur en charge de leur sécurité a avoué n'avoir aucune idée de l'endroit

---

[35] https://www.nsslabs.com/reports/why-your-data-breach-my-problem

[36] Concernant spécifiquement le numéro de sécurité sociale, il est fortement déconseillé aux USA de l'utiliser comme identifiant. Les auteurs de l'étude recommandent d'ailleurs aux entreprises américaines « de se préparer à la promulgation éventuelle d'une loi fédérale qui interdirait aux entreprises d'utiliser cette donnée comme moyen de vérification de l'identité ». La page Web *State laws restricting private use of Social Security numbers* liste les états américains qui interdisent déjà l'utilisation du numéro de sécurité sociale pour accéder à des ressources.

[37] Voir KrebsOnSecurity, *How Much Is Your Identity Worth?,* 8 novembre 2011

[38] *Of passwords and people: Measuring the effect of password-composition policies*, Komanduri, Shay, Gage Kelley, Mazurek, Bauer, Christin, Faith Cranor, Egelman.

[39] La quasi-totalité des faiblesses que l'on peut reprocher aux mots de passe proviennent des êtres humains qui doivent les créer, les mémoriser et les utiliser. Il faut donc impérativement intégrer un volet ergonomie dans tout projet d'identification.

[40] Certains experts évoquent la possibilité d'utiliser des caractères issus des alphabets grec, hébreux ou cyrillique.

[41] *Correction du Bac, TF1 diffuse login et mot de passe d´un espace privatif de l´académie de Versailles* dans un reportage du JT de 13 heures, Zataz.com, 25 juin 2010.

[42] *President Bill Clinton Lost Nuclear Codes While in Office*, par John Donvan, abcNews, 20 octobre 2010

où ils se trouvaient. Si l'on en croit les services officiels, les procédures ont été modifiées après l'incident.

Le cœur qui saigne

On vous l'a dit, on vous l'a répété… Il ne faut jamais saisir son numéro de carte bancaire si le cadenas n'est pas fermé. Il devrait en être de même lors de toute saisie de mot de passe, car celui-ci est transmis en clair à la ressource à laquelle vous voulez accéder. Le CIL doit donc vérifier ou faire vérifier que toute saisie en ligne d'informations critiques se fait bien sous la protection du protocole HTTPS[43]. Cette belle certitude a été ébranlée en avril 2014, à la découverte d'une faille de sécurité dans certaines versions du logiciel OpenSSL, sur lequel s'appuie une grande partie de la sécurité du Web. Baptisée du nom de *Heartbleed* (« cœur qui saigne »), cette faille permet à un attaquant de provoquer un contournement de la politique de sécurité d'un serveur Web et une atteinte à la confidentialité des données qu'il héberge. Des chercheurs ont montré que la vulnérabilité pouvait être exploitée pour compromettre les certificats utilisés par les serveurs Web pour réaliser le chiffrement de la connexion avec les internautes : les mots de passe auraient donc pu être écoutés par un tiers, et ceci depuis deux ans. Très rapidement la CNIL a recommandé à tout responsable de traitement mettant en œuvre une version vulnérable d'OpenSSL de mettre à jour les serveurs concernés, de révoquer et renouveler les clés de chiffrement et les certificats utilisés, mais aussi d'inviter les utilisateurs à renouveler leurs mots de passe[44]. La CNIL précisait qu'elle comptait vérifier la bonne prise en compte de ces mesures dans le cadre des contrôles qu'elle opère régulièrement[45]. Parmi les sites français, Darty a confirmé à la presse avoir utilisé une version vulnérable d'OpenSSL, et avoir corrigé le problème le 9 avril : les utilisateurs du site de commerce ont été « vivement invités » à changer de mot de passe[46].

Le 14 avril 2014, la CAR (*Canada Revenue Agency*) a préféré suspendre son site. Son responsable a indiqué disposer d'éléments indiquant que « la vulnérabilité a été exploitée pour extraire, des bases de données personnelles relatives aux assujettis, environ 900 numéros de sécurité sociale ». Un mois après la découverte de la faille dans la librairie OpenSSL, des chercheurs ont constaté qu'il restait encore près de 320.000 serveurs vulnérables sur la Toile[47]. Là encore, les Correspondants Informatique et Libertés doivent s'assurer que le nécessaire a été fait, bien fait et à temps.

Comment s'y prennent les cybercriminels ?

Lors de la conception d'un procédé d'identification à base de mot de passe, il convient d'essayer d'adopter le point de vue de l'assaillant. Quelles sont les principales techniques utilisées par le cybercriminel pour réussir à prendre connaissance des mots de passe ?

Il peut l'obtenir par *social engineering* (ingénierie sociale), directement auprès du détenteur du compte ou bien auprès de tiers qui ont connaissance du secret. La pratique consiste à exploiter la naïveté des individus pour obtenir des informations. Avec beaucoup d'aplomb, le pirate peut ainsi obtenir le mot de passe d'un individu en se faisant passer pour un administrateur technique, ou, à l'inverse contacter

---

[43] Popularisé par le symbole du cadenas fermé, l'HyperText Transfer Protocol Secure — littéralement « protocole de transfert hypertexte sécurisé » — est la combinaison du protocole HTTP avec une couche de chiffrement et garantit en théorie la confidentialité des données envoyées par l'utilisateur et reçues du serveur.

[44] Il convient de prévoir aussi la rotation des mots de passe embarqués dans les applications se connectant en Webservice sur les ressources concernées.

[45] *Faille de sécurité Heartbleed : comment réagir ?*, page mise en ligne le 16 avril 2014 sur le site Web de la CNIL.

[46] Le Monde, *Faille Heartbleed : les sites pour lesquels il est conseillé de changer son mot de passe*, le 11 avril 2014, par Michaël Szadkowski

[47] http://blog.erratasec.com/2014/05/300k-servers-vulnerable-to-heartbleed.html#.U2z4T1eS68A

l'équipe de *help-desk* en demandant de réinitialiser le mot de passe en prétextant un caractère d'urgence. C'est ainsi que Kevin Mitnick[48] a pu accéder aux systèmes informatiques de Fujitsu, Motorola, Nokia, Sun Microsystems et du Pentagone.

Le pirate peut aussi arriver à ses fins auprès du détenteur du compte par une opération de *phishing*[49]. Dans ses conseils publiés à la suite de la faille *Heartbleed*, la CNPD (Commission Nationale pour la Protection des Données) luxembourgeoise recommande aux utilisateurs particuliers « d'être vigilant dans les prochains jours quant aux courriels qui leur sont destinés. En effet, la situation actuelle est propice à des tentatives de *phishing* (hameçonnage), dans lesquelles il leur est demandé de changer leur mot de passe et où ils sont incités à se connecter sur de faux sites (par exemple, on leur fait croire qu'ils accèdent au site de leur banque mais il s'agit d'un site pirate). En cas de doute, la CNPD recommande de contacter par téléphone la société qui leur aurait envoyé le courriel pour demander la confirmation de l'authenticité de la communication. ».

Il peut l'obtenir également par une opération de *pharming*. Ne devant pas être confondue avec le *phishing*, cette technique d'escroquerie consiste à rediriger le trafic Internet d'un site Web vers un autre site lui ressemblant à s'y méprendre afin d'inciter les internautes (en confiance) à saisir leur nom d'utilisateur et mot de passe dans la base de données[50]. Généralement dirigées contre les sites bancaires ou financiers, ces attaques visent à obtenir les données confidentielles des internautes afin d'accéder à leur compte, d'usurper leur identité ou de commettre des délits en se faisant passer pour eux. Pour réaliser cette attaque, les pirates utilisent une méthode appelée « empoisonnement DNS » (*Domaine Name System*[51]*Poisoning*) : l'attaquant exploite une vulnérabilité du serveur DNS qui accepte alors des informations incorrectes qu'il transmet par la suite aux utilisateurs qui effectuent la requête visée par l'attaque[52]. Plus le procédé d'identification sera techniquement résistant, plus ces différentes techniques seront mises en œuvre par les pirates pour obtenir ce qu'ils recherchent.

Le cybercriminel peut essayer d'espionner la frappe au clavier de la personne qui saisit son mot de passe par la mise en place d'un enregistreur de frappes (*keylogger*), qui saisit tout texte tapé par un utilisateur à son insu. Le CIL veillera à l'affichage de conseils de sécurité à l'attention des utilisateurs afin de les aider à assurer une bonne « hygiène » de leurs ordinateurs[53]. Le pirate peut aussi essayer de « casser » le mot de passe, soit en ligne (en se connectant sur la ressource, comme le fait un utilisateur légitime), soit en mode déconnecté après avoir exfiltré de l'organisme cible la liste des empreintes des mots de passe[54] : il convient de sécuriser l'accès à celle-ci et de placer une alerte en cas de tentatives de copie. Les bases de données abritant des données sensibles – dont les empreintes des

---

[48] Kevin Mitnick est un pirate informatique qui se faisait appeler « Le Condor ». Il est le premier cybercriminel à avoir figuré sur la liste des dix fugitifs les plus recherchés du FBI. En 1995, il est condamné à cinq ans de prison pour délit informatique. En 2002, il coécrit un livre traitant de l'ingénierie sociale et basé sur ses expériences personnelles : L'Art de la supercherie.

[49] Appelée aussi hameçonnage ou filoutage, le *phishing* est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité ou un détournement de fonds. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, scan haute définition de pièces d'identité, etc.

[50] Dans le *phishing*, la victime a cliqué sur un lien qui mène vers un faux site. Dans le *pharming*, la victime a bel et bien saisi la bonne URL dans son navigateur, mais elle a été « aiguillée » par le DNS « empoisonné » vers un faux site.

[51] Le DNS est un service permettant de traduire un nom de domaine (par exemple afcdp.net) en l'adresse IP de la machine portant ce nom. Vu le peu de soin apporté à ce dispositif en termes de sécurité (alors qu'il est crucial), on aurait pu croire que l'acronyme signifie « Dernier de Nos Soucis ».

[52] Voir http://fr.wikipedia.org/wiki/DNS_poisoning

[53] C'est également dans cette page que l'on peut placer une mention relative à la Loi Godfrain n° 88-19 du 5 Janvier 1988, qui punit les accès et le maintien frauduleux dans les systèmes de traitement automatisé de données, de même que les tentatives pour fausser ou entraver leur fonctionnement. On peut aussi inviter l'utilisateur à ne pas mémoriser les mots de passe dans son navigateur Internet. Si une personne mal intentionnée prend le contrôle de l'ordinateur d'un utilisateur, il lui suffit alors de récupérer le fichier contenant la liste des mots de passe enregistrés pour pouvoir se connecter sur des sites à accès protégé.

[54] Nous verrons plus loin qu'il s'agit en fait de la base des empreintes/hash des mots de passe, ces derniers de devant jamais être conservés en clair.

mots de passe – sont plus souvent qu'on l'imagine accessibles par Internet, à l'insu des informaticiens. En 2007, l'expert sécurité David Litchfield a révélé avoir trouvé 492.000 bases de données accessibles librement sur Internet, sans aucune protection[55] : « Il n'est pas possible de dire combien de ses ressources sont intégrées dans des chaînes de commandes en ligne, mais un demi-million de serveurs accessibles, c'est largement plus que suffisant pour permettre aux criminels de récupérer des données sensibles ». De plus, il suffit de la présence au sein de l'organisme d'un seul PC infecté et sous le contrôle d'un pirate pour que soient exfiltrées des informations de grande valeur.

Si l'extraction a été détectée mais n'a pu être empêchée, il est recommandé de procéder à la rotation (au renouvellement) des mots de passe, le cybercriminel risquant de parvenir plus ou moins rapidement à surmonter la protection mise en place. L'absence d'un tel dispositif en cas de violation de données à caractère personnel, dans l'hypothèse d'une généralisation de la notification à laquelle sont déjà soumis certains acteurs au titre de l'ordonnance n° 2011-1012 du 24 août 2011, pourrait être amèrement regrettée dans un futur proche[56].

L'attaque par force brute consiste à tester, de manière exhaustive et « idiote », les différentes possibilités de mots de passe. Tous les caractères étant testés, ce mode est, à la longue, infaillible. Afin d'augmenter la pertinence de l'algorithme, les tentatives sont d'abord effectuées pour les caractères les plus utilisés statistiquement. Combien de temps faut-il à un attaquant pour parvenir à ses fins ? Sans tenir aucun compte de la latence due au réseau de communication, il faut, par exemple, 35 minutes à un simple ordinateur de bureau pour trouver un mot de passe composé de huit lettres minuscules, 253 jours en cas d'utilisation des lettres minuscules et majuscules et des chiffres, 23 ans si on y ajoute tous les caractères spéciaux[57]. Si le pirate utilise un réseau d'ordinateurs, il ne lui faudrait, en revanche, « que » 83 jours pour parvenir à ses fins dans cette dernière configuration. Certaines sondes réseau sont capables de détecter ces attaques, surtout quand elles sont menées sans discrétion (encore faut-il exploiter les alarmes). Un mot de passe « robuste » prendra plus de temps pour être cassé par cette méthode, surtout si un « gel » est imposé en cas d'échecs d'identification répétés. Pour réduire le temps nécessaire pour découvrir le mot de passe, les cybercriminels segmentent-ils l'attaque et confient-ils à des PC zombis[58] la tâche de tester – chacun – une partie du dictionnaire[59], permettant ainsi à une attaque qui aurait dû, en théorie, prendre plusieurs années, d'être couronnée de succès en quelques semaines ?

L'attaque par dictionnaire consiste à tester une série de mots de passe potentiels, les uns à la suite des autres, en espérant que le mot de passe soit contenu dans le dictionnaire. Cette méthode repose sur le fait que de nombreuses personnes utilisent des mots de passe courants (par exemple : un prénom, une couleur ou le nom d'un animal[60]). C'est pour cette raison qu'il est toujours conseillé de ne pas utiliser de mot de passe comprenant un mot ou un nom. Les cybercriminels se sont constitué des dictionnaires comprenant les mots de passe les plus fréquemment choisis par les utilisateurs, les prénoms, les noms de pays et de ville, les noms propres de personnages illustres (mais aussi de héros de cinéma, de BD, etc.). Les mots peuvent être « déclinés » dans leurs différentes variantes (en changeant par exemple la

---

[55] SearchSecurity, *Survey finds thousands of database servers open to attack*, par Robert Westervelt, 14 novembre 2007

[56] La fonction de gestion des mots de passé doit pouvoir permettre à l'exploitant de déclencher la modification des mots de passe associés à une liste ou un bloc d'utilisateurs, voire à leur totalité.

[57] *Password recovery speed – How long will your password stand up*, disponible sur www.lockdown.co.uk

[58] Ordinateur contrôlé à l'insu de son utilisateur par un pirate, suite à une infection par un malware (virus ou cheval de Troie). Certains cybercriminels gèrent des « parcs » de plusieurs centaines de milliers PC zombies (les « botnets »), qu'ils louent à des tiers peu scrupuleux pour réaliser des opérations de déni de service ou diffuser des pourriels (spams).

[59] La version *Distributed John* permet cette répartition du calcul sur plusieurs ordinateurs en réseau afin d'augmenter l'efficacité du cassage.

[60] Dans son livre *The art of intrusion* (Wiley publishing, 2006), Kevin Mitnick relate le cas d'étudiants américains qui avaient deviné le mot de passe utilisé par les salariés de la firme Coca-Cola qui protégeaient les distributeurs de boissons : Pepsi !

casse de certaines lettres ou en les remplaçant par leurs équivalents en *leet speak*[61]. Les mots peuvent être aussi répétés. Il existe aussi des dictionnaires correspondant à l'ensemble des numéros de plaque d'immatriculation, des numéros de sécurité sociale, des dates de naissance, etc. Ainsi le logiciel *John the Ripper*[62] est fourni avec une liste de règles qui permettent d'étendre l'espace de recherche et d'explorer les failles classiques dans l'élaboration des mots de passe par les utilisateurs.

Qu'est-ce qu'une fonction de hash ?

L'attaque la plus redoutable est tout de même le vol de la base de mots de passe. C'est la raison pour laquelle il convient de les « hasher ». Contrairement à l'idée reçue, la ressource (le site Web, par exemple) ne conserve jamais (ne doit jamais conserver) les mots de passe en clair. À la première saisie du mot de passe, une fonction de hash est appliquée et seule l'empreinte obtenue est conservée. Lors des saisies suivantes le même procédé est appliqué. Si les deux empreintes sont identiques, l'identification est réussie. Cette procédure permet aussi d'éviter que les administrateurs techniques ne puissent être en mesure de connaître (et d'usurper) les mots de passe des utilisateurs. Si c'était le cas, un utilisateur indélicat pourrait toujours prétendre que l'intrusion dont il est l'auteur a été réalisée par un administrateur, dont on sait qu'il a souvent accès à tous les fichiers et toutes les ressources du système d'information.

Le Correspondant Informatique et Libertés doit vérifier que les mots de passe sont bel et bien stockés sous une forme inintelligible (cette vérification aboutit quelques fois à quelques surprises). Suite à plusieurs contrôles, la CNIL a adressé en 2012 un avertissement public à la société FNAC Direct[63]. Parmi les manquements sanctionnés, la commission pointait une violation de l'article 34 de la loi relatif à la sécurisation des données, les informations relatives à plusieurs millions de cartes bancaires ayant été stockées sans protection suffisante : « établi que dans la même base de données apparaît le nom du porteur de la carte, son numéro de carte bancaire, la date d'expiration de celle-ci, et parfois son cryptogramme visuel, l'ensemble de ces éléments étant conservé dans la même base, en clair, sans hachage ni chiffrage ». En juillet 2014, la société éditrice du site www.regimeducan.com a reçu un avertissement public de la part de la CNIL[64], suite à trois contrôles sur place. Parmi les griefs reprochés au responsable de traitement, on relève que « les mots de passe des comptes clients étaient conservés en clair ».

Mais que recouvre la technique de hash ? Il s'agit d'une fonction mathématique très particulière qui présente deux caractéristiques spécifiques qui en font tout son intérêt : il est tout d'abord impossible, à partir du résultat de cette fonction, de deviner la valeur de départ : à titre d'analogie, on retiendra l'image de la vitre cassée qu'il est impossible de ramener à son état d'origine en recollant les morceaux, de la feuille de papier froissée qu'on ne peut rendre à l'état initial ou des peintures mélangées que l'on souhaiterait dissocier pour retrouver les couleurs de départ. La deuxième qualité d'une fonction de hash est de donner un résultat univoque (jamais deux valeurs de départ ne donneront le même résultat). C'est une fonction très souvent utilisée, par exemple pour vérifier qu'un document placé en archives probantes n'a pas été modifié depuis son dépôt, ou bien pour vérifier que deux personnes partagent bien le même secret, sans que jamais ce secret soit exposé.

---

[61] De l'anglais *elite speak* (« langage de l'élite »), le *Leet speak*, est un système d'écriture utilisant les caractères alphanumériques d'une manière peu compréhensible pour le néophyte. Le principe est d'utiliser des caractères graphiquement voisins des caractères usuels, par exemple 5 au lieu de S, 4 au lieu de A, etc.

[62] *John the Ripper* est un logiciel libre de cassage de mot de passe. Ces logiciels ne sont pas toujours utilisés dans un but malicieux. Certains RSSI les utilisent pour tester la résistance des mots de passe choisis par les utilisateurs et les alerter sur les risques encourus. Dès qu'un mot de passe est craqué par l'administrateur sécurité, celui-ci doit immédiatement demander à l'utilisateur de le changer pour un mot de passe plus robuste.

[63] Délibération n° 2012-214 du 19 juillet 2012

[64] http://www.cnil.fr/fileadmin/documents/La_CNIL/decisions/20140711_deliberation_regimecoache.pdf

La fonction en elle-même est appelée fonction de hash ou prise d'empreinte. Son résultat est appelé hash, empreinte[65], condensat, condensé, résumé de message ou encore signature. Cette empreinte est de longueur fixe, quelle que soit la valeur d'entrée (le résultat d'un mot ou d'une longue phrase ou d'un document donnera une chaîne de caractères de même longueur, qui dépend de l'algorithme sélectionné). Quand une fonction de hash est employée à des fins de sécurité, ses concepteurs font en sorte que le moindre changement de la donnée initiale (modification d'un seul caractère, par exemple) entraine une perturbation importante de l'empreinte, afin de rendre difficile une recherche inverse par approximations successives. Ce phénomène est appelé « effet avalanche ».

Le calcul de l'empreinte consomme peu de ressources informatiques, mais le stockage des résultats peut quelquefois poser problème (l'empreinte d'un mot de passe de huit caractères peut atteindre une longueur de plus de cent caractères). Les concepteurs de ces fonctions cherchent donc à trouver le compromis idéal[66].

Très rapidement il a été découvert des imperfections dans les fonctions sélectionnées. Elles concernent la « robustesse » de l'algorithme (il s'avère possible, à partir d'une empreinte, de découvrir la valeur de départ) ou l'unicité du résultat produit (on parle dans ce cas de « collision » quand deux données de départ donnent un même résultat). Le Correspondant Informatique et Libertés devrait donc également s'assurer – si besoin en s'appuyant sur le RSSI – que l'algorithme de hash utilisé respecte l'état de l'art. Ainsi les procédés MD5 et SHA-1 sont aujourd'hui déconseillés[67], alors que la famille SHA-2 (principalement SHA-256) répond aux attentes. Prévoyant une possible faiblesse de cette dernière famille, le NIST (*National Institute of Standards and Technology*) avait lancé en 2007 une compétition pour trouver un remplacement au SHA-1. Fin 2012, c'est l'algorithme KECCAK qui a remporté la coupe. Baptisé SHA-3, cette nouvelle fonction va sans doute mettre du temps avant de se répandre, car SHA-2 n'a pas été encore compromis par une attaque significative.

« Pouvez-vous me passer le sel ? »

Dans le cas où un cybercriminel parviendrait à exfiltrer la liste des empreintes de mots de passe conservée par la ressource, le fait de « hasher » les mots de passe ne suffit-il pas à assurer une sécurité qui respecte « l'état de l'art » ? Les cybercriminels disposent de techniques qui leur permettent de découvrir les mots de passe les plus faibles, notamment en utilisant des tables arc-en-ciel (*rainbow table*). Hacher les mots de passe n'est donc pas suffisant[68]. Il vaut mieux y ajouter une pincée de sel.

C'est ici qu'intervient le « petit plus de nos grands-mères ».

Si on compare l'algorithme de hash à une recette de cuisine (qui est publiée, que tout le monde connaît…y compris le cybercriminel), le sel correspond à ce « petit truc de cuisine » que vous a légué votre grand-mère, ce qui rendait son plat si particulier. Le principe est simple : avant de procéder à la prise d'empreinte du mot de passe, on le « concatène » avec une valeur qui est ce fameux sel[69]

---

[65] L'auteur recommande cette sémantique et déconseille l'expression « somme de contrôle » dans ce contexte.

[66] Signalons une solution élégante tirée des travaux de Gilles Trouessin, membre de l'AFCDP et l'un des rares experts français dans l'art de l'anonymisation : il « suffit » d'exprimer l'empreinte non pas en codage hexadécimal, mais dans un codage d'ordre supérieur (comme la Base 36, par exemple). Gilles Trouessin est l'un des co-auteurs de la méthode FOIN (Fonction d'occultation d'identifiant nominatif), procédure élaborée à la fin des années 90 par le Centre d'études des sécurités des systèmes d'information (CESSI) de la CNAMTS.

[67] Pour aller plus loin, se reporter à l'excellent article de Kévin Drapel, *Les fonctions de hachage cryptographiques*, initialement paru dans le défunt magazine Login. Disponible sur http://fr.wikibooks.org/wiki/Les_fonctions_de_hachage_cryptographiques

[68] Un expert a réussi, avec le logiciel ocl-Hashcat-plus, à « cracker » une empreinte (sans sel) et à retrouver le mot de passe suivant : « Ph'nglui mglw'nafh Cthulhu R'lyeh wgah'nagl fhtagn1 ».
Disponible sur http://arstechnica.com/security/2013/08/thereisnofatebutwhatwemake-turbo-charged-cracking-comes-to-long-passwords/

[69] Le sel (également appelé « germe » dans certains documents de l'ANSSI, ou « seed ») devient donc l'élément hautement confidentiel qu'il convient de protéger très précieusement.

Rappelez-vous l'effet « avalanche » : ceci va se traduire par un condensat totalement différent, mais toujours de même longueur. Même grâce à ses dictionnaires, l'attaquant ne peut plus remonter jusqu'à la valeur d'origine (le mot de passe), tant qu'il n'a pas connaissance du fameux sel. Ainsi, si le mot de passe « AFCDP » donne l'empreinte f42edc3ec7cc4b9647a12abee3a5d8ad en utilisant la fonction MD570, il donne avec la même fonction un résultat complétement différent si j'y ajoute le sel[71] « 38 » (le condensat de « AFCDP38 » est alors 560d7e6704e555c1ccfb1cc2f582f2a4). On en déduit donc que toute précaution utile doit désormais être prise pour choisir ce nouveau « petit secret » avec soin[72] et en assurer la confidentialité… Les Correspondants Informatique et Libertés ont lu avec profit le document que le G29 a publié en mars 2014 et intitulée *Opinion 03/2014 on Personal Data Breach Notification* (693/14/EN - WP13). Il y est bien spécifié que le fait de hacher les mots de passe n'est pas considéré comme suffisant par le groupe qui représente les autorités de contrôle pour arguer de l'inintelligibilité des données dans le cas d'une violation à un traitement de données.

Les « CNIL » intégreront-elles ce principe dans leur doctrine locale ? Dans ce cas, seul un procédé de hash conforme à l'état de l'art et mettant en œuvre un sel a une chance de vous éviter la notification aux personnes concernées[73].

Le lion et la girafe

Une approche, de plus en plus répandue, permet de compliquer la tâche des pirates : celle du mot de passe « jetable »[74]. Après la saisie fructueuse de l'identifiant et du mot de passe statique, la ressource l'adresse – le plus souvent via un SMS – pour qu'il soit fourni dans un laps de temps donné. Cela suppose de disposer du numéro de téléphone portable de la personne, et que le téléphone mobile soit desservi par le réseau au moment de l'identification. Le fait qu'il soit transmis par un canal différent de celui emprunté par l'utilisateur renforce la sécurité : il est difficile pour un cybercriminel d'espionner à la fois la connexion Internet et la communication téléphonique. Cette approche permet de qualifier de « forte » l'identification car elle requiert en l'occurrence la conjonction de deux facteurs : la connaissance d'un secret (le mot de passe statique personnel) et la possession d'un élément matériel (le téléphone portable avec son n° d'appel associé). Souvent appelé par son appellation anglaise OTP (*One-time password*), le mot de passe jetable pallie plusieurs des faiblesses du mot de passe statique traditionnel : il compense une durée de vie du mot de passe personnel souvent trop longue et offre une excellente résistance aux attaques en ligne par dictionnaire et en force brute. L'OTP n'a pas besoin d'être complexe, puisqu'il est conçu à la volée par la ressource et ne peut être utilisé qu'une fois : un pirate ne sera pas en mesure de l'utiliser par la suite car il ne sera plus valide. En revanche, il nécessite la mise en œuvre de technologies complémentaires. Les banques s'en servent notamment pour augmenter le niveau de sécurité sur des transactions de transferts de fonds vers d'autres comptes extérieurs, opérations jugées plus sensibles qu'une simple consultation.

Il existe d'autres implémentations du principe d'OTP : avec la « liste à biffer », l'utilisateur saisit, en plus de son mot de passe personnel statique, un code figurant sur une liste qui lui a été fournie par la ressource. Les codes sont « consommés » dans l'ordre, les uns après les autres. La liste peut prendre la

[70] Le site Web http://www.sinfocol.org/herramientas/hashes.php vous permet d'obtenir l'empreinte obtenue à partir de plus de 130 procédés.

[71] Dans la réalité, le sel est d'une longueur bien plus grande. De plus l'emplacement du sel par rapport au mot de passe est également gardé secret (avant, après, la moitié avant et l'autre moitié après, etc.).

[72] La bonne pratique est de ne pas utiliser une clé de salage unique (la même pour toutes les tables comprenant des mots de passe) mais de la générer aléatoirement pour chaque enregistrement. A titre d'exemple, un système comme Joomla est capable de gérer, pour chaque utilisateur, un sel dynamique (un par utilisateur) et un sel statique (unique pour tous).

[73] Pour le moment ne sont concernés que les opérateurs, dans le cadre de l'ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques, mais il est probable que la mesure se généralise dans le cadre du futur règlement européen.

[74] Sans surprise, cette technique présente tout de même quelques faiblesses, surtout si elle a mal été implémentée au niveau du serveur, et des cybercriminels ont réussi – sous certaines conditions – à la contourner, par exemple dans un scenario de type man-in-the-middle.

forme d'une carte comportant une matrice, également fournie par la ressource[75]. Le défi est exprimé sous forme de coordonnées (« Qu'elle est la valeur qui figure dans la matrice qui vous a été remise, dans la troisième case de la deuxième ligne ? »). Une solution commerciale a élégamment supprimé la possession de la carte (élimant ainsi les risques de pertes et les frais liés à sa fabrication et à son envoi) : à sa connexion initiale, l'utilisateur est invité à configurer lui-même un « secret » supplémentaire exprimé sous forme d'un déplacement simple dans un échiquier (par exemple deux cases en diagonale vers le haut à droite). Suite à la saisie de l'identifiant et du mot de passe statique personnel, la ressource affiche à l'utilisateur une matrice comportant, par exemple, des photographies d'animaux. Le défi est traduit par l'affichage sur l'écran de l'une des photos (par exemple celle du lion). On attend que l'utilisateur clique sur la case illustrée d'une girafe, située à l'arrivée du déplacement dans la matrice. Les « token[76] » qui figurent aux porte-clés de certains informaticiens appartiennent aussi à la famille OTP : les deux parties (le *token* et la ressource) sont synchronisées sur le temps universel[77] et utilisent le même algorithme de génération du mot de passe unique (affiché sur un écran à cristaux liquides minuscule dont est équipé le *token*) : l'utilisateur dispose alors de quelques instants pour le saisir sur la ressource.

Le brahmane Sissa face au roi Belkib

Ne nous leurrons pas. C'est bien le cybercriminel qui a la partie la plus facile. La mission du CIL et de son partenaire RSSI est de lui rendre la vie difficile. Techniquement, cela se traduit souvent par une bonne gestion du temps, qui est essentielle, car la question est moins de savoir si un cybercriminel va réussir à prendre connaissance des mots de passe, que de savoir combien de temps il lui faudra pour atteindre cet objectif.

Lorsqu'un algorithme d'empreinte est présenté par son concepteur comme « impossible à casser », il faut traduire par « très difficile à circonvenir en un temps raisonnable…mais à la longue tout est possible ». Le Correspondant Informatique et Libertés doit donc obtenir une estimation fiable de la part de son RSSI – au besoin en se faisant assister par un expert – du temps qu'il faudrait à un assaillant pour prendre connaissance des mots de passe. L'intérêt de l'organisme est de prendre toute mesure permettant d'allonger ce temps, par exemple en ajoutant un « gel » entre deux tentatives d'identification en ligne. Cette temporisation peut être d'une valeur peu perceptible par un humain (c'est le cas de la technique dite du *Blowfish*[78], dans laquelle le procédé de hash utilisé pour comparer le mot de passe qui vient d'être saisi et l'empreinte stockée est de plus en plus lent) ou se concrétiser par une période de blocage plus longue suite à plusieurs tentatives consécutives infructueuses[79]. Cette temporisation peut être constante (dix minutes, par exemple, entre chaque série de tentatives) ou bien croissante : à titre d'exemple, un doublement du temps d'attente entre deux séries de tentatives[80] rend le délai rédhibitoire aussi bien pour l'utilisateur légitime (qui utilise dans ce cas la fonction « Mot de passe oublié ») que pour le cyberpirate. Il convient bien sûr de mettre en œuvre une alerte sur les log[81] d'identification afin de détecter ce type d'évènements. On peut aussi opter pour une approche plus

[75] Exemple de la banque Crédit Mutuel.

[76] Petit dispositif électronique de la taille d'une clé USB, générant des nombres synchronisés destiné à l'authentification.

[77] Cette approche présente l'avantage d'être utilisable même dans des zones non desservies par le réseau de téléphonie mobile, par exemple dans une salle informatique. C'est l'une des raisons pour lesquelles elle est très répandue au sein des équipes d'exploitation informatique.

[78] Du nom que les anglo-saxons ont donné aux poissons qui se gonflent en cas de danger et dont la plupart des espèces sont toxiques. Les procédés techniques PBKDF2, bcrypt et scrypt mettent en œuvre cette fonction « retardatrice ».

[79] Plusieurs des paramètres propres aux systèmes UNIX permettent de déterminer ces critères, comme PASSWORD_LIFE_TIME (durée de vie du mot de passe), FAILED_LOGIN_ATTEMPTS (nombre de tentatives consécutives autorisées), ou PASSWORD_LOCK_TIME (durée du gel – période de blocage).

[80] Sur le modèle de l'histoire de l'échiquier et des grains de blé, qui met en scène le brahmane Sissa et le roi Belkib : Sissa demande pour récompense le riz que le roi placera sur un échiquier, à raison dans chaque case du double de grains de riz par rapport à la case précédente.

[81] Dans le jargon informatique, le log est un « événement », enregistré dans un « log file ».

radicale : le compte est désactivé et le mot de passe invalidé au bout d'un certain nombre d'échecs (ce qui se fait au niveau des guichets automatiques de banque et des cartes bancaires, au bout de trois tentatives erronées). Ces précautions sont très efficaces contre les attaques en force brute et par dictionnaire, mais là aussi, des tests ergonomiques préalables sont recommandés si vous ne voulez pas voir votre service relations clients pris d'assaut.

Il faut également être capable d'estimer le temps qu'il faudrait à un pirate qui a réussi à exfiltrer une base d'empreintes de mots de passe pour « casser » le hash : si le temps nécessaire est estimé à quatre mois (par exemple), les mots de passe devraient avoir une durée de vie inférieure. En cas de preuve ou de forte suspicion de vol de la liste des empreintes de mots de passe, la rotation de ceux-ci devrait être enclenchée[82] : le pirate se retrouve alors en possession d'informations sans aucune utilité. C'est sans doute ce qui explique la demande qu'eBay a adressée à ses utilisateurs en mai 2014[83]- incitant au changement du mot de passe[84] - alors que l'entreprise précisait dans sa communication que les mots de passe qui figuraient dans la base accédée par les pirates étaient « chiffrés[85] ». En janvier 2014 et dans une situation apparemment proche, Orange a précisé à 800.000 de ses clients concernés par une exposition de leurs données personnelles que les mots de passe n'avaient pas été impactés[86].

Pas de recette miracle

En 2007, la CNIL avait pointé les failles de sécurité du Dossier Médical Personnel (DMP), dont les mots de passe étaient trop facilement réductibles[87]. Mais de quoi dépend la robustesse d'un mot de passe ? Une erreur commune est de se focaliser uniquement sur leur longueur et leur composition. En fait la robustesse d'un contrôle d'accès logique dépend en pratique d'un ensemble de critères, au premier rang desquels, bien sûr, figure la force intrinsèque du mot de passe, c'est à dire sa complexité. Mais il faut également prendre en compte les mécanismes mis en œuvre pour transmettre l'élément secret et pour vérifier le mot de passe et ses caractéristiques ; le nombre d'échecs d'identification autorisés avant blocage d'un compte protégé par le mot de passe ; les mécanismes d'alerte éventuels. Compte tenu de ce qui précède, il n'existe pas de recette miracle pour déterminer à coup sûr ce qu'est un bon mot de passe. À titre d'exemple, le choix paraît naturel entre un mot de passe de huit caractères complexes et un mot de passe composé uniquement de quatre chiffres. Si nous précisons maintenant que, dans le premier cas, le mot de passe est transmis en clair à l'utilisateur lors de sa conception et qu'il est possible à un cybercriminel de tester toutes les combinaisons sans aucune limite ni déclenchement d'une alarme d'aucune sorte, et que, au contraire, dans le cas du mot de passe composé de quatre chiffres, seuls trois tentatives sont autorisées avant suspension du compte, et que toutes les précautions ont été prises en respect de l'état de l'art pour sécuriser les empreintes de ces mots de passe… laquelle de ces deux approches vous apparaît à présent la plus sûre ?

---

[82] Les solutions d'IAM (*Identity and Access Management*) les plus avancées prévoient la possibilité de suspendre temporairement un compte si l'on pense que celui-ci a été compromis, dans l'attente des résultats de l'enquête.

[83] Se référer aux nombreux articles parus à l'occasion, comme « *Piraté, eBay conseille de changer de mot de passe* », Le Point, 21 mai 2014 (source AFP).

[84] Il est indispensable d'enjoindre les utilisateurs à concevoir un nouveau mot de passe qui n'ait aucun lien avec l'ancien : des études ont montré que plus de 40 % des utilisateurs se contentaient de créer une nouvelle variante, ce qui permet au pirate de trouver facilement le nouveau mot de passe en partant de l'ancien.

[85] Il convient de veiller à utiliser la bonne sémantique. L'une des caractéristique d'une fonction de hash, c'est d'être irréversible, alors qu'un chiffrement est réversible (ce qui a été chiffré peut être déchiffré). Pour les puristes, le terme « chiffré » est ici impropre.

[86] Voir *Orange victime d'une intrusion informatique*, E.Erconali, L'Informaticien, 30 janvier 2014, disponible sur www.linformaticien.com/actualites/id/31886/orange-victime-d-une-intrusion-informatique.aspx

[87] Conclusions des missions de contrôles relatives à l'expérimentation du DMP, avril 2007

Comme les mots de passe, les procédures doivent être robustes

Il est essentiel de mettre en place des mesures organisationnelles et des procédures robustes, mises en œuvre lors de plusieurs phases critiques : lors de la création de compte (initialisation et première fourniture du mot de passe), lors de la rotation du mot de passe, lors de la fourniture d'un mot de passe transitoire (en cas d'oubli du mot de passe personnel). Il est encore fréquent de voir des cas qui font dresser les cheveux sur la tête : certains sites Web obligent à se créer un compte et un mot de passe… et vous adressent un courriel (en clair) comportant l'intégralité des informations dont rêve tout cybercriminel : prénom, nom, adresse email, identifiant, mot de passe ! Cette pratique sera sans doute assimilée dans le futur à une violation à un traitement de données personnelles[88]. Ce scénario présente un risque accru si le mot de passe saisi est celui qui contrôle l'accès à des comptes bancaires en ligne. C'est pourquoi la CNIL recommande d'utiliser des mots de passe différents pour tous ses comptes. Ainsi, en cas de compromission du mot de passe, les autres comptes ne seront pas exposés[89].

Le mot de passe initial doit être de préférence fourni sur un canal sûr. Lorsque ce mot de passe initial est fourni par l'administrateur du système ou lorsqu'il est communiqué sur un canal non confidentiel, il doit absolument être changé dès la première connexion de l'utilisateur. L'ANSSI indique que l'administrateur qui a fourni un mot de passe sur un canal non sûr « doit avoir une vigilance plus soutenue afin de s'assurer que le mot de passe n'est pas utilisé par un tiers ». Il est recommandé également, dans ce cas de figure, de ne laisser que peu de temps à l'utilisateur pour créer son propre mot de passe.

Le renouvellement (rotation) des mots de passe est également une phase critique : les mots de passe doivent avoir une date de validité maximale, à partir de laquelle l'utilisateur ne doit plus pouvoir s'identifier sur le système si le mot de passe n'a pas été changé. Ceci permet de s'assurer qu'un mot de passe découvert par un utilisateur mal intentionné ne sera pas utilisable indéfiniment dans le temps. Cela constitue également une protection naturelle contre le phénomène des « droits fantômes », liés aux utilisateurs qui n'ont plus aucune légitimité à accéder au service. Dans sa délibération n° 2014-294 du 22 juillet 2014 (sanction de 5.000 € avec publicité, à l'encontre de la société Loc Car Dream), la formation restreinte de la CNIL a critiqué le non renouvellement des mots de passe : bien que l'entreprise ait pris le soin d'opter pour des mots de passe de douze caractères alphanumériques pour accéder à un traitement de géolocalisation, la Commission a remarqué « que le mot de passe est resté inchangé depuis l'installation de ce dispositif, soit environ plus de deux ans ».

La procédure de réinitialisation en cas d'oubli ou perte du mot de passe par un utilisateur devra être pensée de telle façon qu'elle ne soit pas mise à profit par les cybercriminels. Certains services demandent à l'utilisateur de répondre à une question secrète qu'il a lui-même configurée lors de la création de son compte (par exemple le nom de jeune fille de sa grand-mère). Il est également recommandé de protéger la procédure par un test de Turing[90] (ou Captcha[91]) afin d'éviter que des robots n'invalident les comptes pour perturber le fonctionnement du service.

---

[88] C'est la raison pour laquelle le CIL doit s'intéresser au libellé des courriels adressés aux utilisateurs dans le cadre de la gestion des mots de passe, et notamment lors de l'envoi d'un mot de passe provisoire, quand la personne a oublié son mot de passe. Ce courriel ne doit contenir que le strict nécessaire et l'utilisateur doit formuler le plus vite possible un nouveau mot de passe personnel (il ne devrait pas pouvoir continuer à utiliser longtemps le mot de passe provisoire qui lui a été transmis par un canal non sécurisé).

[89] Les utilisateurs du navigateur Google Chrome savent-ils que, par défaut, les mots de passe qu'ils utilisent pour visiter des sites tiers et mémorisés dans Chrome sont transmis à Google, et que cette récupération se fait d'une façon telle que la société américaine est en mesure de les déchiffrer ? La NSA pourrait-elle y avoir accès ? (voir « *Comment Chrome envoie tous vos mots de passe à Google* », par Guillaume Champeau, Numerama, 18 août 2014).

[90] Alan Turing (1912-1954), mathématicien et informaticien anglais, est considéré comme l'« inventeur » de l'ordinateur. Durant la Seconde Guerre mondiale, il joue un rôle majeur dans les recherches pour casser les codes générés par la machine Enigma, utilisée par les nazis. En 1952, un fait divers lié à son homosexualité lui vaut des poursuites judiciaires. On lui donne le choix entre la prison et la castration chimique

Plusieurs autres points méritent réflexion. Faut-il par exemple rendre techniquement impossible la connexion simultanée sous le même code utilisateur et le même mot de passe ? De quelle façon afficher les dates et heures de la dernière connexion pour donner une chance réelle à l'utilisateur de détecter une usurpation de ses droits. La CNIL le préconise pour faciliter le repérage d'éventuelles intrusions frauduleuses sur le système, mais sur de nombreux sites cette indication est quasi invisible, et aucune information n'est délivrée aux utilisateurs : que doivent-ils faire très concrètement ?

Le Correspondant Informatique et Libertés, en synergie avec le RSSI, a tout intérêt à s'assurer que soit formalisée une politique relative aux mots de passe[92], en tant qu'élément crucial pour une prise de conscience de l'importance de la sécurité. Mais cette démarche ne doit pas se limiter aux seuls utilisateurs. En application du principe de *Privacy by Design*, une version spécifique doit être conçue spécifiquement pour les chefs de projets, les maîtres d'ouvrage et les développeurs. En annexe de son registre, le CIL peut ainsi conserver trace des analyses menées et du relevé de décision (Pourquoi l'adresse email a-t-elle été retenue comme identifiant ? Quel raisonnement a mené à imposer la rotation du mot de passe tous les trois mois ?), ce qui permettra de s'y reporter en cas d'audit, de contrôle ou de changement du niveau de risques qui obligerait à revoir les choix faits. Une fois cette politique formalisée, le plus dur reste à faire : veiller à sa stricte application. Le Maréchal Foch l'exprimait ainsi : « Si le commandement devait se borner à donner des ordres, ce ne serait pas difficile. Il faut les faire exécuter ».

Une obligation de moyen, pas de résultat

La Directive 95/46/CE – dont est issue notre loi Informatique et Libertés – indique dans son considérant 46 que « la protection des droits et libertés des personnes concernées à l'égard du traitement de données à caractère personnel exige que des mesures techniques et d'organisation appropriées soient prises tant au moment de la conception qu'à celui de la mise en œuvre du traitement, en vue d'assurer en particulier la sécurité et d'empêcher ainsi tout traitement non autorisé ; qu'il incombe aux États membres de veiller au respect de ces mesures par les responsables du traitement ; que ces mesures doivent assurer un niveau de sécurité approprié tenant compte de l'état de l'art et du coût de leur mise en œuvre au regard des risques présentés par les traitements et de la nature des données à protéger ». Plusieurs points spécifiques ne se retrouvent pas dans l'article 34 de la loi Informatique et Libertés qui dispose simplement que « Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ». Ainsi, l'article 34 de la loi Informatique et Libertés pouvant être interprété par une obligation de moyen – et non de résultat –, des discussions intenses peuvent opposer RSSI et CIL sur les notions « d'état de l'art » et de « coût de mise en

---

par prise d'œstrogènes. Il se suicide par empoisonnement au cyanure le 7 juin 1954. Le test de Turing est une proposition de test d'intelligence artificielle fondée sur la faculté d'imiter la conversation humaine. Décrit par Alan Turing en 1950 dans sa publication *Computing machinery and intelligence*, ce test consiste à mettre en confrontation verbale un humain avec un ordinateur et un autre humain, à l'aveugle. Si l'homme qui écoute les conversations n'est pas capable de dire lequel de ses interlocuteurs est un ordinateur, on peut considérer que le logiciel de l'ordinateur a passé avec succès le test.

[91] Marque commerciale de l'université Carnegie-Mellon et acronyme de *Completely Automated Public Turing test to tell Computers and Humans Apart*, le CAPTCHA est un test permettant de différencier de manière automatisée un utilisateur humain d'un ordinateur. Le site affiche une série de chiffres et de lettres, dans des polices de caractères étranges, sur un fond brouillé. À l'utilisateur de saisir ce qu'il arrive à lire et de prouver qu'il est un être humain et non pas un programme informatique...

[92] À titre d'exemple : « Toute opération effectuée à partir de ses mots de passe ou codes confidentiels personnels sera réputée, a priori, être de son fait. Dans le même temps il est interdit d'utiliser le compte (ou matricule) d'un autre utilisateur sans son autorisation. Chaque utilisateur doit respecter les règles de création et de gestion des mots de passe définies par la Direction de la Sécurité des SI, et notamment : choisir des mots de passe ou codes secrets sûrs; lorsqu'elle est proposée par l'application, ne pas répondre à la sollicitation de mémorisation du mot de passe ; ne pas communiquer ses mots de passe ou codes secrets à un tiers, sous réserve des nécessités liées à la continuité du service, telles que définies par chaque responsable de service ; Ne pas enregistrer les mots de passe pour les accès distants sur le PC portable ou sous quelque forme que ce soit (étiquette, post-IT, etc.) ; respecter la limite de ses droits. »

œuvre » des mesures de sécurité envisagée. Ces débats[93] ne peuvent se tenir de façon constructive sans qu'une étude de valeurs et de risques (pour les personnes concernées en priorité) ait préalablement été menée.

Voici un exemple dans lequel l'état de l'art n'était pas respecté : en juin 2012, la base des mots de passe de LinkedIn était attaquée. Un hacker a publié sur la Toile un fichier comprenant 6.458.020 mots de passe… uniquement protégés par un hash sans sel. Il a suffi au chercheur en sécurité Jeremi Gosney trente secondes pour déchiffrer 20 % des mots de passe les moins sécurisés (comme *linkedin*, *love* ou … *password*), deux heures pour cracker le tiers suivant, une journée pour en déchiffrer 64 %. Après six jours de travail, le chercheur a reconstitué 90 % des millions de mots de passe dérobés car c'est l'algorithme SHA-1 qui était utilisé par le réseau social, dont les faiblesses étaient pourtant connues. Certains membres de l'AFCDP, concernés, ont reçu le courriel suivant : « Nous avons découvert que certains mots de passe ont été compromis et mis en ligne sur un site de hackers. Nous avons immédiatement mené une enquête et avons des raisons de croire que l'un des mots de passe publiés correspond à votre compte. Bien qu'une minorité de mots de passe ait été décodée et publiée, nous ne pensons pas que le vôtre en fasse partie. Par mesure de précaution, nous avons désactivé votre mot de passe et nous vous conseillons de suivre les étapes ci-dessous pour le réinitialiser. Si vous avez réinitialisé votre mot de passe au cours des deux derniers jours, aucune action supplémentaire n'est nécessaire. Si vous utilisiez le même mot de passe sur d'autres sites, nous vous recommandons de les changer également. ». Un mois plus tard, en juillet 2012, c'était au tour du Figaro de s'excuser auprès de 162 de ses lecteurs : « *Une faille informatique*[94] *a permis de consulter en clair les mots de passe d'un petit nombre (moins de 200 sur plusieurs centaines de milliers) des internautes inscrits au Figaro.fr et ayant déposé récemment des commentaires. Le Figaro.fr présente ses excuses aux internautes concernés pour ce désagrément. Alertés le 10 juillet 2012 au soir, les équipes techniques du Figaro.fr ont pu identifier et corriger ce problème dans la journée. Par mesure de sécurité, les mots de passe des internautes concernés ont été réinitialisés d'office par nos équipes. Un lien de génération d'un nouveau mot de passe sécurisé leur a été adressé ».* Un an après, c'est au tour d'OVH, piraté, de contacter ses clients[95]*,* qui ont reçu le message suivant : « Récemment, nous avons relevé un incident de sécurité sur notre réseau interne au siège social d'OVH. Nous avons immédiatement sécurisé et enquêté sur l'incident. Nous avons relevé que la base de données des clients Europe aurait pu être illégalement copiée. Cette base comporte les données suivantes : le nom, le prénom, l'adresse, la ville, le pays, le téléphone, le fax et le mot de passe chiffré. Les informations sur les cartes bancaires ne sont pas concernées puisqu'elles ne sont pas stockées par OVH. Même si le chiffrement[96] du mot de passe de votre identifiant est très fort, nous vous conseillons de changer le mot de passe dans les plus brefs délais. »

En janvier 2013, l'ICO (*Information Commissioner's Office*, équivalent de la CNIL et de la CADA pour la Grande-Bretagne), a infligé une pénalité financière de 250.000 £ (soit environ 300.000 €) à *Sony Computer Entertainment Europe Limited* suite à l'incident de sécurité qui avait affecté, en avril 2011, des millions d'informations personnelles - dont les mots de passe et les détails des cartes

[93] C'est à cette occasion que CIL et RSSI peuvent s'entendre sur une sémantique commune, par exemple pour établir une claire différence entre mot de passe provisoire initial, mot de passe personnel et mot de passe transitoire (envoyé par le système en cas d'oubli). Les règles pouvant être différentes pour chacune de ces catégories.

[94] Dans ce cas, la vulnérabilité consistait en un bug de Drupal.

[95] *OVH piraté, la base de données des clients Europe exposée*, Journal du Net, par Virgile Juhan, 22 juillet 2013, disponible sur http://www.journaldunet.com/solutions/dsi/ovh-hacke-0713.shtml

[96] A nouveau, il s'agit ici d'une sémantique erronée mais compréhensible pour le public visé. Est-ce la raison pour laquelle même la CNIL l'utilise quelques fois ? A titre d'exemple, on le relève dans sa délibération n° 2013-392 du 5 décembre 2013 autorisant le SYMEV à mettre en œuvre un traitement pour finalité la gestion et la prévention des impayés des Commissaires-priseurs : « L'intégrité des données ainsi que la protection des mots de passe sont assurées par un chiffrement » (dans la version du puriste, il faut traduire par «« L'intégrité des données est assurée par un chiffrement, tandis que la protection des mots de passe l'est par un procédé de hash ») .

bancaires. L'enquête de l'autorité de contrôle a montré que l'attaque aurait pu être contrée si les mises à jour logicielles indispensables avaient été effectuées. Elle a pointé également du doigt une gestion des mots de passe pour le moins « perfectible ». Là encore, l'état de l'art n'avait pas été respecté.

Un utilisateur ne pourrait gérer que cinq mots de passe

Une étude a montré qu'en moyenne un collaborateur du Département du Commerce (USA) utilise neuf mots de passe[97]alors qu'un utilisateur ne pourrait en gérer que cinq au maximum, et encore, s'il les utilise fréquemment[98]. On comprend donc que certains d'entre nous aient pris l'habitude de les noter sur un support papier ou dans notre Smartphone. Lors des contrôles sur place effectués par la CNIL, il n'est pas rare de voir les agents soulever les claviers, à la recherche de petits papiers autocollants portant les précieux codes. Mais pourquoi ne pas conserver sur support papier les mots de passe, dans un endroit bien sécurisé ? L'expert sécurité Bruce Schneider recommande dans ce cas d'utiliser une astuce similaire au code rendu célèbre par George Sand dans une lettre destinée à Alfred de Musset[99], en notant non pas le mot de passe mais une suite de mots dont les premières lettres forment le secret, les chiffres étant remplacés par des mots basés sur leur forme[100] (9 est un ballon d'enfant au bout de sa ficelle, 6 un éléphant qui barrit, 3 une belle poitrine…).

Pour les utilisateurs grand public, il existe des « gestionnaires de mots de passe » qui permettent de constituer une base de données sécurisée et qui vous permettent de ne retenir qu'un mot de passe « maître ». Celui-ci vous ouvre l'accès à tous les autres, qui pourront être très longs, très complexes et tous différents, car c'est l'ordinateur qui les retient à votre place. Il existe de nombreuses solutions sur le marché. Parmi les logiciels libres régulièrement mis à jour, la CNIL cite l'outil Keepass[101]dont la sécurité a été évaluée par l'ANSSI[102] (Agence Nationale de Sécurité des Systèmes d'Information) - mais aussi Passreminder ou Passwordsafe.

Ce même principe se retrouve en environnement professionnel.

Le principe du mécanisme de SSO (*Single Sign On*) est de rassembler tous les mots de passe que l'utilisateur doit mémoriser dans un coffre-fort numérique. C'est ce dispositif qui prend à sa charge la création, la rotation et la protection de chaque mot de passe individuel. Le déploiement de ce type de solution correspond à une augmentation générale du niveau de sécurité : chaque mot de passe géré par le SSO peut être plus long, plus complexe et changé plus fréquemment, de plus les mots de passe ne sont plus notés. Par contre, le point critique devenant la procédure qui permet d'accéder aux mots de passe stockés, il vaut mieux protéger son accès par une authentification forte… et non pas la fourniture d'un « simple » mot de passe[103].

Il existe des solutions SSO spécifiquement adaptées à la gestion des mots de passe partagés (et non pas rattachés à une seule personne). Comme l'indiquent Laurent Bloch et Christophe Wolfhugel dans leur

---

[97] 2014, *United States Federal Employees' Password management behaviors Case study*, NIST

[98] 1999, *Users are not the Enemy*, Anne Adams & Martina Angela Sasse, Department of Computer Science, University College London

[99] L'astuce consiste à lire une ligne sur deux (procédé littéraire appelé acrostiche). La lettre commence ainsi : « Cher ami, Je suis toute émue de vous dire que j'ai/ bien compris l'autre jour que vous aviez/ toujours une envie folle de me faire/ danser. Je garde le souvenir de votre/ baiser et je voudrais bien que ce soit/ une preuve que je puisse être aimée/ par vous. ». En fait la lettre a été attribuée à tort à Amantine Aurore Lucile Dupin. Il s'agit d'un canular qui remonte à la fin du XIXe siècle.

[100] *Remembering Passwords*, disponible sur http://changingminds.org/techniques/memory/remembering_passwords.htm

[101] http://keepass.info

[102] Voir www.ssi.gouv.fr/IMG/cspn/anssi-cspn_2010-07fr.pdf. L'ANSSI avertit bien que « la certification ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information, et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables. »

[103] Sur la critique de l'approche SSO, voir *SSO/RSO/USO/oh no?*, de Michael B.Scher, décembre 2004

ouvrage *Sécurité informatique, Principes et méthodes*[104], « De mauvaises pratiques héritées des premiers temps de l'informatique conduisent encore beaucoup de systèmes à être utilisés par plusieurs personnes qui se connectent sous un compte unique dont tout le monde connaît le mot de passe : une telle habitude doit être combattue sans relâche, parce que sur un tel système, aucune sécurité n'existe ni ne peut exister. »

La chasse aux fantômes

Il est de bonne pratique que de procéder régulièrement à des revues de comptes, afin de prévenir l'existence de comptes malveillants, périmés ou inconnus. Cette démarche s'effectue en lien avec le service des ressources humaines, qui gère le rôle des employés[105]. Lorsqu'un collaborateur quitte la société, les comptes et mots de passe utilisateurs qui lui étaient associés sont-ils immédiatement révoqués[106] ? Les comptes inutilisés pendant une durée prolongée (comptes inactifs) sont-ils automatiquement désactivés sur le système au-delà d'un délai prédéfini ? On peut aller plus loin et imaginer utiliser les plannings d'absence : est-ce normal qu'un collaborateur en congés ou en arrêt maladie se soit connecté à une ressource sensible ? Il est possible d'étudier le relevé des comptes inactifs, le relevé des identifiants qui se connectent simultanément, de ceux qui se connectent à partir d'un grand nombre d'adresses IP.

Naturellement, tous ces contrôles, qui constituent des traitements de données à caractère personnel, doivent être mis en conformité avec la loi Informatique et Libertés. Il est également utile de prévoir, lors de l'étude de chaque nouveau traitement, une éventuelle sous-finalité de vérification du bon usage des moyens d'identification.

Lors de l'Université AFCDP des CIL de 2010, le Commissaire principal Yves Crespin, alors chef de la BEFTI[107], avait relaté quelques expériences vécues. Dans le cas d'une entreprise de transports maritimes, confrontée à une attaque de son système d'informations avec pertes de données, la brigade était facilement remontée jusqu'à un ancien administrateur technique, remercié quelques mois auparavant par la société. Il avait tout bonnement conservé ses droits. L'informaticien avait alerté à plusieurs reprises sa direction de la sécurité insuffisante du système d'information : son attaque n'avait d'autre but que de le prouver. De plus, il avait installé des logiciels espions dans l'espoir de surprendre un échange entre directeurs de service, le regrettant et reconnaissant a posteriori son mérite. Pour Yves Crespin, « il aurait fallu écouter ce collaborateur avec plus d'attention… ».

Dans le même registre, le policier recommandait de penser aux stagiaires, qui peuvent être instrumentalisés dans le cadre d'opération d'espionnage industriel. Les mots de passe inchangés, même suite au départ d'un administrateur clé, sont monnaie courante : « Dans plus de la moitié des dossiers que ma brigade traite, nous mettons en évidence des problèmes de sécurité classiques ».

En 2007, le compte-rendu d'une réunion secrète du comité directeur d'une société cible d'une OPA s'est retrouvé dans la presse. L'enquête a rapidement mis en évidence qu'un ancien administrateur réseau avait quitté l'entreprise sans que ses droits soient invalidés. Dans la même veine, la question « Avez-vous connaissance d'anciens collaborateurs qui ont quitté l'entreprise et qui disposent

---

[104] Eyrolles, 2006

[105] Attention à bien respecter le code du travail. Le fait qu'un collaborateur ne soit pas présent (même pour une longue durée) ne signifie pas forcément qu'il ne fait plus partie de l'entreprise.

[106] Dans la procédure de test du PCI DSS (*Payement Card Industry Data Security Standard*), le point 8.1.3.a recommandé de « Sélectionner un échantillon d'employés qui ont quitté la société au cours des six derniers mois, et passer en revue les listes d'accès pour examiner à la fois l'accès local et l'accès distant, afin de vérifier que leur ID ont été désactivées ou supprimées de la liste d'accès ». http://fr.pcisecuritystandards.org/_onelink_/pcisecurity/en2frfr/minisite/en/docs/PCI_DSS_v3.pdf

[107] Brigade d'enquêtes sur les fraudes aux technologies de l'information.

toujours des droits d'accès à l'infrastructure ? » recueillait 28 % de réponses positives dans une enquête menée en 2008 par la société Cyber-Ark.

La mort du mot de passe ?

En 2004, Bill Gates avait prédit que les mots de passe allaient être de moins en moins utilisés[108] grâce à un nouveau système d'identification basé sur une carte sur laquelle devaient figurer des informations personnelles et un code-barre qui servirait d'identifiant. La même entreprise a repris la même prédiction en dévoilant son « mot de passe image » lors du lancement de Windows 8 (il est demandé de reproduire sur l'écran une séquence de mouvements secrets sur une photographie choisie). Les tenants de la biométrie[109] tiennent naturellement le même discours. Cela peut être une solution[110], mais les mots de passe ne disparaîtront pas aussi vite que cela. Gwendal Le Grand, chef du service d'expertise informatique de la CNIL, interrogé par 20 Minutes en août 2012, estime que « le mot de passe n'est pas obsolète ».

On a vu que certaines approches – comme celle de l'OTP – permettaient de pallier plusieurs de ses faiblesses. En fait, ce qui est à souhaiter, c'est la mort du mauvais mot de passe. Bien utilisé, le mot de passe a encore de beaux jours devant lui. Cormac Herly et Paul C. van Oorschot, dans leur article « *A research agenda acknowleddging the Persistence of Passwords*[111] », recommandent tout d'abord de commencer par se poser la question « La protection par mot de passe est-elle adaptée à notre projet ? », de définir les objectifs et d'identifier les menaces réelles (et non pas supposées).

On peut aussi s'interroger pour savoir si certaines doctrines ne sont pas au final contre productives. Ainsi, exiger de façon uniforme et non adaptée au contexte, des renouvellements à fréquence élevée et une trop grande complexité de mot de passe, peut induire des comportements qui diminuent la sécurité. Certaines règles trop strictes peuvent faire plus de mal que de bien[112] et participer de l'abandon de cette approche, au profit de techniques plus intrusives pour la vie privée. S'agissant de protection de données personnelles, le CIL devra s'assurer que son responsable de traitement remplit sa part des efforts (protection de la base d'empreinte, généralisation du SSL, juste équilibre sécurité/ergonomie, etc.).

Ne reste plus, alors, qu'à responsabiliser les utilisateurs vis-à-vis du choix et de la gestion de leur mot de passe[113], car « Le mot de passe, c'est comme une brosse à dents : on la change régulièrement, on ne la partage pas avec ses amis, et on ne la laisse pas traîner ! ».

Bruno RASLE, Délégué général de l'AFCDP. Chef de projet Informatique et Libertés à la CNAF (Mission de l'Audit, de la Conformité Informatique et Libertés, de la Sécurité du Système d'Information). Auteur du livre *Halte au Spam* (Eyrolles, 2003), Bruno Rasle a été membre du groupe de contact anti-spam mis en place par la DDM (Direction du Développement des Médias, services du Premier ministre), pour lequel il a organisé un cycle de conférences. Il est l'organisateur du premier séminaire français sur le sujet, le *Spam Forum Paris*, qui s'est tenu dans une salle mise à disposition par l'Assemblée nationale. Bruno Rasle forme les CIL depuis 2007.

---

[108] *Bill Gates prédit la fin des mots de passe*, Clubic. La même année, il avait également annoncé la fin des spams…

[109] Certaines banques américaines utilisent déjà des logiciels capables de reconnaître votre voix, en plus du simple PIN classique demandé.

[110] La proposition de loi déposée par Monsieur Gaëtan Gorce et votée à l'unanimité au Sénat le 27 mai 2014 limiterait l'usage de la biométrie qu'à des strictes nécessités de sécurité, et non de confort (voir le chapitre sur la biométrie au sein de cet ouvrage).

[111] http://research.microsoft.com/apps/pubs/?id=154077

[112] Voir sur ce thème l'excellent papier « *Meilleures pratiques pour gérer les mots de passe : les politiques relatives aux utilisateurs finaux doivent trouver l'équilibre entre le risque, la conformité et la convivialité* », Ant Allan, Gartner, in. Perspectives n° 99, juillet-août 2014.

[113] L'un des leviers passe par les CGU (Conditions Générales d'Utilisation), qui doivent comprendre un chapitre dédié à ce sujet.