Gildas Avoine
Pascal Junod

Cybersécurité et hygiène numérique au quotidien

129 bonnes pratiques à adopter pour se protéger

DUNOD

Direction artistique : Nicolas WIEL
Graphisme : Florie BAUDUIN
Édition : Matthieu DANIEL et Anne TEMPS

NOUS NOUS ENGAGEONS EN FAVEUR DE L'ENVIRONNEMENT :

Nos livres sont imprimés sur des papiers certifiés pour réduire notre impact sur l'environnement.

Le format de nos ouvrages est pensé afin d'optimiser l'utilisation du papier.

Depuis plus de 30 ans, nous imprimons 70 % de nos livres en France et 25 % en Europe et nous mettons tout en œuvre pour augmenter cet engagement auprès des imprimeurs français.

Nous limitons l'utilisation du plastique sur nos ouvrages (film sur les couvertures et les livres).

11 rue Paul Bert, 92240 Malakoff
www.dunod.com
ISBN 978-2-10-086118-7

Sommaire

6. Choisir une solution sécurisée pour communiquer

7. Conserver ses systèmes informatiques simples et sains

8. Anticiper les menaces et réagir aux attaques

Biographie des auteurs

Gildas Avoine est professeur de cybersécurité à l'INSA Rennes et membre honoraire de l'Institut Universitaire de France. Il mène des recherches scientifiques dans le domaine de la cryptographie au sein du laboratoire IRISA. Il est également le président du Conseil scientifique de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), qui est en France un service à compétence nationale faisant autorité en matière de sécurité et de défense des systèmes d'information. Gildas Avoine a occupé des fonctions au CNRS, comme directeur du Groupement de Recherche (GdR) en sécurité informatique de 2016 à 2021, puis comme codirecteur du Programme et Équipements Prioritaires de Recherche (PEPR) en cybersécurité de 2021 à 2023. Auparavant, il a exercé à l'UCLouvain en Belgique, au MIT aux États-Unis et à l'EPFL en Suisse. Il a également enseigné à l'ENSTA Paris ainsi qu'à la New York University Paris.

Pascal Junod est le fondateur et directeur de modulo p SA, une société basée en Suisse offrant des services d'expertise en matière de cryptographie et de cybersécurité. Il est également chargé de cours externe à la Haute École Spécialisée de Suisse Occidentale (HES-SO). Pascal Junod a travaillé dans l'industrie, au sein de l'opérateur du réseau social Snapchat, Snap Inc., de 2017 à 2021, en tant que cofondateur de la startup strong.codes SA, lancée en 2016 et active dans le domaine de la protection logicielle, ainsi qu'en tant qu'expert en cryptographie de 2005 à 2008 au sein du groupe Kudelski, une société suisse évoluant dans le domaine du contrôle d'accès pour la télévision payante. Il a également travaillé dans le domaine académique de 2008 à 2017, comme professeur à la Haute École d'Ingénierie et de Gestion du Canton de Vaud (HEIG-VD) à Yverdon-les-Bains. Pascal Junod est titulaire d'un master en informatique de l'ETH Zurich ainsi que d'un doctorat en cryptographie de l'EPFL.

Avant-propos

La sécurité informatique est apparue dès les premières heures de l'informatique, vers la fin des années 60. Elle n'était alors qu'embryonnaire, et c'est dans les années 90, avec le déploiement d'Internet et plus particulièrement du web, qu'elle a connu un véritable essor dans la communauté informatique : bien qu'Internet ait été conçu pour résister à une destruction partielle des infrastructures, la présence de personnes malveillantes qui opéreraient sur les systèmes ou les canaux de communication n'avait pas été prise en compte. Il a donc fallu imaginer des solutions pour pallier ces failles de conception. C'est ensuite, à partir des années 2000, avec l'arrivée d'Internet dans tous les foyers, que la sécurité informatique est apparue au grand public. Une décennie plus tard, vers 2010, il devenait clair que les criminels avaient compris que l'informatique, devenue « technologies du numérique », était destinée à devenir leur nouvel Eldorado. C'est alors que la « sécurité informatique » a progressivement cédé la place au terme « cybersécurité » et ses dérivés.

La cybercriminalité, qui s'est structurée en bandes organisées et qui voit la fraude sur Internet comme plus accessible et moins risquée que d'autres formes de criminalité, connaît une évolution sans précédent depuis une dizaine d'années. Alors que la cybersécurité consistait jusqu'à présent à mettre en place des protections pour empêcher les attaques de pénétrer dans les systèmes informatiques, comme on construit des remparts pour protéger une citadelle, la pensée a aujourd'hui fondamentalement évolué : résister à toute offensive étant vain, il faut alors se préparer à affronter l'adversaire au sein même de la citadelle. Avec ce nouveau paradigme, la cybersécurité est devenue l'affaire de tous et non plus l'apanage des responsables de systèmes d'information. L'ampleur de la cybercriminalité nécessite en effet l'implication de chacun, ce qui passe par une sensibilisation à la cybersécurité à large échelle et conduit ainsi au concept « d'hygiène numérique ». Sachant que les cyberattaques exploitent généralement une faiblesse humaine dans leur cycle de vie, acculturer la société à l'hygiène numérique peut contribuer à réduire significativement l'impact de la cybercriminalité.

L'hygiène numérique est constituée de bonnes pratiques à appliquer quotidiennement. Elle est destinée aux particuliers, alors que nombre de guides sur la cybersécurité s'adressent à des professionnels. Cet ouvrage s'envisage alors comme un recueil de bonnes pratiques expliquées simplement pour toute personne déjà initiée aux technologies du numérique.

L'ouvrage est ainsi structuré en huit grandes parties indépendantes, elles-mêmes divisées en plusieurs thèmes. Le lecteur pourra choisir de les parcourir séquentiellement ou de s'orienter directement vers le thème qui l'intéresse. Chacun de ces thèmes est illustré d'exemples, avec des focus sur des points techniques et bien évidemment des bonnes pratiques synthétiques que le lecteur pourra facilement mettre en œuvre. L'ouvrage a été rédigé dans un souci de sensibiliser et former le lecteur à l'hygiène numérique, pas seulement de lui fournir des recettes clefs en main qui deviendraient obsolètes avant même d'avoir eu le temps de les appliquer. L'hygiène est un travail de fond et, de manière similaire à une formation au secourisme, il est important que chaque individu procède à des recyclages réguliers. Sensibiliser les plus jeunes à l'hygiène numérique à travers la formation initiale, par exemple au niveau de l'enseignement secondaire, est à notre sens une priorité absolue à laquelle les pouvoirs publics devraient accorder plus d'importance. Mais ce vecteur ne peut être suffisant à lui seul, le monde de l'entreprise doit également s'emparer de la question en formant ses employés, le milieu associatif en proposant d'accompagner les plus fragiles face aux technologies du numérique, tandis que d'autres vecteurs sont encore à construire, comme l'autoformation.

Forts d'une longue expérience dans le domaine de la cybersécurité, dans l'enseignement supérieur, la recherche publique, mais aussi dans le secteur privé, nous avons souhaité mettre à profit nos connaissances et compétences en proposant un ouvrage accompagné d'un site web (https://hygiene-numerique.guide), pour aller encore plus loin dans ce cheminement vers un monde numérique plus sûr.

Cet ouvrage n'aurait pu voir le jour sans les enrichissantes interactions que nous avons eues tout au long de ces années avec nos collègues et collaborateurs, ainsi qu'avec nos étudiants, jamais avares d'épineuses mais pertinentes questions. Sans les remercier nommément, nous leur en sommes reconnaissants. Nous souhaitons également remercier les relecteurs de la première heure, à savoir Adrien Bouquet, Franck Gaultier, Michel Junod, Stéphane Koch, Diane Leblanc-Albarel et Carine Sandmeier, que nous avons sollicités à plusieurs reprises et dont les retours sur une maquette initiale et le manuscrit nous ont encouragés à poursuivre notre effort. Enfin, et avant tout, ce projet n'aurait jamais pu arriver à sa fin sans la bienveillance sans faille et la patience de nos compagnes et enfants qui subissent régulièrement notre passion pour la cybersécurité.

Gildas Avoine, Pascal Junod

1

S’authentifier correctement

L'authentification est l'un des piliers de notre société, qui permet à chacune et chacun de prouver son identité. Dans le monde physique, elle repose généralement sur la vérification d'une pièce d'identité officielle, car sa délivrance fait l'objet d'une procédure rigoureuse qui permet d'associer l'identité d'une personne à ses données biométriques, comme une photo ou des empreintes digitales. L'authentification ne se limite pas aux individus, elle peut aussi concerner des groupes d'individus (tels que les employés d'une entreprise) ou des organisations (comme l'entreprise elle-même).

Dans le domaine des technologies numériques, l'authentification permet par exemple de vérifier l'identité de la personne avec laquelle on communique, ou celle d'une personne qui se connecte à un ordinateur ou à un site web. Il est important de souligner que ce n'est pas parce qu'une personne est authentifiée qu'elle est nécessairement autorisée à accéder à une ressource : authentification et autorisation sont deux concepts différents, où l'authentification a uniquement pour objectif de vérifier que la personne est bien celle qu'elle prétend être.

Pour cela, l'authentification repose généralement sur l'une des trois catégories de facteurs suivantes : « je sais » (pour un mot de passe par exemple), « je possède » (c'est le cas d'une carte à puce) ou « je suis » (comme une empreinte digitale). Elle peut aussi utiliser une combinaison de ces facteurs – on parle alors communément d'authentification « multifacteur » – et c'est exactement ce qui est recommandé pour renforcer la sécurité.

GÉNÉRER ET GÉRER SES MOTS DE PASSE

Un sondage de Google réalisé par Harris Poll en décembre 2018 auprès de 3 000 Américains montre que 52 % d'entre eux utilisent le même mot de passe pour plusieurs comptes. Une autre enquête, réalisée de décembre 2018 à janvier 2019 auprès de 1 305 utilisateurs d'Avast en France, montre que 51 % des répondants utilisent le même mot de passe professionnel et personnel. Même s'il est difficile d'obtenir des chiffres fiables plus récents, nul doute que la situation est inquiétante. Le site web *Have I been pwned?*, qui permet à chacun de vérifier si un mot de passe apparaît dans des bases de données qui ont fuité, en témoigne : il recense actuellement 12 milliards de comptes dont les identifiants ont été volés et publiés. Ce seul chiffre devrait suffire à convaincre tout un chacun qu'il est important d'utiliser des mots de passe différents pour des services différents.

Importance de protéger ses mots de passe

Exposer un mot de passe, c'est s'exposer soi-même aux personnes malveillantes : à partir d'un mot de passe, les cybercriminels peuvent récupérer des informations privées en se connectant aux comptes en ligne de son détenteur (messageries, réseaux sociaux, etc.), éventuellement frauder en se connectant sur ses comptes bancaires ou de e-commerce, voire pénétrer sur son ordinateur pour exfiltrer des informations ou en chiffrer le contenu en vue d'obtenir une rançon. Le vol d'un mot de passe peut donc entraîner des conséquences financières mais aussi psychologiques, en nuisant, par exemple, à la réputation de la victime à travers des pratiques comme le doxxing, une activité répréhensible qui consiste à diffuser des données personnelles sur une personne dans le but de lui nuire, ou le revenge porn, qui consiste à diffuser des contenus sexuellement explicites sur une personne (via des photos ou des vidéos) dans le but de se venger. Si les conséquences du vol d'un mot de passe personnel sont problématiques, il en est de même dans le cadre professionnel. Laisser fuiter son mot de passe, c'est en effet exposer son entreprise à des attaques ayant par exemple pour objectif de faire du chantage, de réaliser un déni de service – c'est-à-dire une attaque qui consiste à empêcher un système informatique

de fonctionner correctement – ou d'exfiltrer des informations techniques ou commerciales à des fins d'espionnage économique. Un collègue qui attache peu d'importance à la sécurité de son mot de passe est un collègue qui met en péril toute l'entreprise car son comportement crée une brèche dans le système informatique.

Protéger tous ses comptes

Il est important de choisir des mots de passe robustes, y compris pour des comptes qui vous semblent peu importants. En effet, si la valeur de vos données sur un compte vous semble faible, le vol de votre mot de passe ouvre la porte à un cybercriminel qui l'utilisera peut-être pour pénétrer dans le système et attaquer d'autres comptes.

Vol de mots de passe

Le vol, c'est notamment le mot de passe observé par un collègue qui regardait par-dessus votre épaule, ou le mot de passe griffonné sur un bout de papier mis à la corbeille ou épinglé sur un tableau, le logiciel malveillant qui espionne votre clavier, ou encore un fraudeur qui arrive à vous convaincre par des moyens d'ingénierie sociale (voir focus p. 105) de lui donner votre mot de passe. Mais le vol, c'est aussi et surtout une base de données d'un site web marchand qui a fuité, révélant ainsi des milliers, voire des millions de mots de passe. Le cybercriminel pourra alors les utiliser directement sur le site marchand ou sur d'autres sites, voire les vendre sur le *dark web* (voir focus p. 167).

Mots de passe identiques pour plusieurs services

Hubert possède un compte sur le site marchand boulatique.com. La base de données du site a été piratée. Les données concernant Hubert qui ont fuité sont : son identité, à savoir Hubert Dupont, son adresse mail et son mot de passe. Le fraudeur qui exploitera ces données tentera par exemple le mot de passe sur Gmail avec l'adresse hubert.dupont@gmail.com, mais il pourra aussi essayer des identifiants construits à partir de « Hubert » et « Dupont » sur X (Twitter), Instagram, etc.

Il est important de prendre conscience que la grande majorité des attaques ne ciblent pas une victime prédéfinie. Nous faisons généralement face à des attaques de masse qui ont pour but d'hameçonner des victimes quelconques. C'est seulement dans un second temps que le cybercriminel concentrera ses forces sur la personne hameçonnée.

FOCUS **Bits et octets**

Dans le domaine du numérique, un bit est l'unité d'information élémentaire, qui ne peut prendre que deux valeurs, notées « 0 » et « 1 ». Toute information intelligible par un humain est *in fine* transformée en bits regroupés par blocs de 8, formant ainsi un « octet ». Par exemple, avec l'encodage appelé « ASCII », la lettre « A » sera représentée par « 01000001 » et la lettre B « 01000010 ». À partir des préfixes du Système international d'unités, un « kilooctet » (ko) représente mille octets, un « mégaoctet » (Mo) un million d'octets et un « gigaoctet » (Go) un milliard d'octets.

Cassage de mots de passe

Les bases de données, par exemple sur des sites marchands, ne contiennent généralement pas les mots de passe à proprement parler, mais des « empreintes » de mots de passe. Une empreinte est le résultat d'une fonction dite « à sens unique » appliquée au mot de passe. L'empreinte d'un mot de passe est similaire à une empreinte digitale :

- Qu'il s'agisse de deux individus ou de deux mots de passe différents, leurs empreintes respectives seront différentes l'une de l'autre.
- Une empreinte seule ne permet pas d'identifier l'individu ou de retrouver le mot de passe correspondant.
- Étant donné une empreinte et un mot de passe, il est possible de déterminer si cette empreinte provient de celui-ci.

En pratique, on ne peut donc pas retrouver directement un mot de passe à partir de son empreinte, mais on peut en revanche tester tous les mots de passe pour trouver lequel permet de générer l'empreinte considérée : on dit alors que le mot de passe est cassé.

FOCUS

Empreinte de mot de passe et fonction de hachage cryptographique

Techniquement, l'empreinte est le résultat d'une fonction dite « à sens unique » qui est appliquée sur le mot de passe.

Il s'agit en pratique d'une fonction de hachage cryptographique telle que les fonctions de dérivation de clef PBKDF2 ou Argon2 qui ont été spécifiquement conçues pour ralentir les cybercriminels. En guise d'illustration, le (très mauvais) mot de passe « maison » pourrait avoir pour empreinte « 1b0fd375f084fb14a6dbb f71ba832201498034ed75925008f2b5ee639e05187764a9ec662eefc6f755be6 eda93c31d256bb4038fdb9a69b089957a99f19eb0c6 ». Ainsi, PBKDF2(*maison*) ou Argon2(*maison*) seraient très faciles à calculer pour un ordinateur (cela ne prendrait qu'une fraction de seconde), mais l'opération inverse serait impossible en pratique.

Une fonction de hachage cryptographique h est une fonction qui prend en entrée une valeur de taille arbitraire, qui génère en sortie une valeur de petite taille (par exemple 512 bits) et vérifie plusieurs propriétés fondamentales, en particulier :

- Étant donné une valeur x, il est facile de calculer $h(x)$.
- Étant donné une valeur y, il est impossible en pratique de trouver x tel que $h(x) = y$. On dit que h est « à sens unique ».
- Il est impossible en pratique de trouver x_1 et x_2 tel que $h(x_1) = h(x_2)$. On dit que h est « résistante aux collisions ».

Les fonctions de hachage les plus connues sont SHA-2 (il s'agit d'une famille qui se décline en plusieurs fonctions dont SHA-256 et SHA-512) et SHA-3.

Dans le domaine des mots de passe, les fonctions PBKDF2 et Argon2 sont préférées car elles sont conçues pour volontairement ralentir les éventuelles attaques. Quant aux fonctions MD5 et SHA-1 qui ont été utilisées pendant de très longues années, elles sont aujourd'hui obsolètes.

Les logiciels permettant de casser des mots de passe, ou « casseurs », tels que John the Ripper et hashcat, testent en premier lieu les mots de passe courts ainsi que les mots du dictionnaire et leurs variantes (par exemple « voiture », « turevoi »,

« erutiov », « voiture2024 », « voiture! », etc.). Aussi, la multitude de bases de mots de passe qui fuitent permet de déduire des statistiques sur les techniques les plus communes pour définir des mots de passe, techniques qui sont ensuite exploitées pour tester les mots de passe les plus probables. Lorsqu'aucune des approches précédentes ne fonctionne, tous les mots de passe possibles sont testés de manière exhaustive : c'est un peu la technique du dernier espoir qui n'aboutit que rarement sans une grande puissance de calcul.

Il convient d'ailleurs de souligner que les attaques qui consistent à tester des mots de passe directement sur un site web jusqu'à trouver le bon sont peu praticables : elles sont en effet très lentes à cause du temps de réponse du serveur web et facilement détectables par ces derniers, ce qui permet de bloquer le compte attaqué.

FOCUS **Casseurs évolués**

Les casseurs évolués exploitent la connaissance issue des bases de mots de passe qui ont fuité pour déterminer les mots de passe les plus probables. Par exemple, un mot de passe qui commence par une majuscule, suivie de lettres minuscules, d'un ou plusieurs chiffres et d'un caractère spécial est un schéma récurrent. On appelle cela un « masque » permettant de casser facilement les mots de passe fortement structurés. Les casseurs évolués utilisent également des techniques reposant sur l'intelligence artificielle pour générer les mots de passe les plus probables. Enfin, d'autres techniques reposent sur l'algorithmique : les techniques dites de « compromis temps-mémoire cryptanalytiques » permettent de réduire le temps de cassage d'un mot de passe, sous certaines conditions, en réalisant en amont des pré-calculs qui sont stockés et réutilisés pour casser n'importe quel mot de passe.

Protéger ses mots de passe

Il est tout à fait possible de se protéger efficacement. Pour cela, il faut avant tout :

- Utiliser des mots de passe robustes.
- Ne pas utiliser un mot de passe identique pour plusieurs usages.
- Changer de mots de passe régulièrement.

Les deux dernières recommandations sont importantes même si un mot de passe est robuste car un cybercriminel pourrait obtenir les mots de passe non pas en les cassant mais par ingénierie sociale (voir focus p. 105) ou grâce à une fuite d'une base de données d'identifiants. Notons toutefois qu'obliger les utilisateurs à changer leur mot de passe trop souvent n'est pas recommandé : cela les incite à en choisir des faciles à mémoriser (et donc faciles à casser) ou à les écrire quelque part.

Mot de passe dédié à un seul usage

Julia utilise un mot de passe robuste pour l'accès à sa messagerie. Elle est à l'abri d'un cybercriminel qui tenterait de le casser. Mais Julia a commis une erreur : elle utilise le même mot de passe sur un site marchand qui les stocke en clair – au lieu de stocker leur empreinte – dans sa base de données et qui… s'est fait pirater la semaine dernière.

Un mot de passe robuste, c'est un mot de passe choisi aléatoirement, c'est-à-dire « au hasard » dans un ensemble de mots de passe suffisamment grand. Choisir un mot de passe dans un dictionnaire est bien sûr inadapté car un dictionnaire ne contient pas plus de 60 000 mots en général. Si l'on prend en compte la conjugaison, les accords grammaticaux et les variations usuelles (comme ajouter une majuscule au début du mot ou un chiffre à la fin), l'ensemble des mots de passe reste toujours trop petit.

Pour mesurer la robustesse d'un mot de passe choisi aléatoirement, on compte le nombre de tests que devra faire un cybercriminel dans le pire des cas pour le casser. Cela correspond à la taille de l'ensemble dans lequel est choisi le mot de passe.

FOCUS **Taille de l'ensemble des mots de passe**

Si les mots de passe considérés sont de longueur équivalente à 8 caractères ($c = 8$) et que chaque caractère est choisi dans un alphabet comportant 26 valeurs possibles ($n = 26$), par exemple les lettres de « a » à « z », alors la taille de l'ensemble des mots de passe possibles est $n^c = 26^8$. Ainsi, le cybercriminel devra tester 26^8 mots de passe dans le pire des cas, soit un peu moins de 209 milliards, ce qui représente un nombre de possibilités facile à explorer pour un ordinateur standard.

Robustesse des mots de passe

La robustesse d'un mot de passe est, intuitivement, la difficulté à laquelle une personne devra faire face pour le casser. Paradoxalement, il n'est pas possible de suggérer dans un livre de bons mots de passe car le simple fait de les écrire en fait des mots de passe de piètre qualité puisqu'ils deviennent connus de tous. Comme déjà mentionné, un bon mot de passe doit être choisi aléatoirement dans un grand ensemble de mots de passe possibles. En France, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), définit quatre niveaux de robustesse, présentés dans le tableau suivant.

Taille de l'ensemble dans lequel est choisi le mot de passe	Robustesse du mot de passe
2^{64}	Très faible
2^{64} à 2^{80}	Faible
2^{80} à 2^{100}	Moyen
$> 2^{100}$	Fort

FOCUS **Mot de passe très faible ou fort**

L'ensemble des mots de passe alphabétiques en minuscule de longueur exactement 8 caractères contient 26^8 mots de passe, soit environ 2^{37} (dans le domaine du numérique, on préfère compter en puissance de 2 plutôt qu'en puissance de 10 – voir focus p. 13) Tout mot de passe choisi dans cet ensemble de près de 140 milliards de combinaisons serait pourtant extrêmement faible et pourrait être cassé en quelques heures sur un ordinateur standard. En utilisant quelques processeurs de cartes graphiques, ce mot de passe ne résisterait pas plus de quelques secondes à un cybercriminel disposant de son empreinte.

Le mot de passe « b!sDzf5w,5 » de longueur 10 caractères, construit à partir d'un alphabet constitué de lettres, de chiffres et de 8 caractères spéciaux, sera toujours considéré comme très faible, bien que difficile à mémoriser. En effet, la

…

…

taille de l'ensemble est 70^{10}, soit environ 2^{61}. Ce genre de mot de passe résistera aux cybercriminels amateurs, mais il ne sera pas assez robuste si vous êtes la cible d'un cybercriminel déterminé, ce qui peut par exemple être le cas dans le milieu professionnel.

Pour être considéré comme fort selon les critères de l'ANSSI, le mot de passe devrait contenir au moins 17 caractères. Vous comprenez ainsi la difficulté, pour ne pas dire l'impossibilité, de générer des mots de passe forts sans l'aide de l'informatique : un mot de passe qui sort uniquement de l'imagination d'un humain aura beaucoup de mal à résister aux casseurs.

Il existe des outils pour vous aider à générer des mots de passe, par exemple KeePass, outil gratuit et certifié par l'ANSSI. En revanche, les outils en ligne qui mesurent la robustesse des mots de passe (avec des codes couleurs allant du vert au rouge) sont peu efficaces, voire parfois trompeurs. En effet, la majorité de ces outils ne considèrent que la longueur du mot de passe et les types de caractères utilisés (lettres, chiffres, caractères spéciaux). C'est-à-dire qu'ils s'interrogent sur le temps que mettrait une recherche exhaustive sans se soucier des chances de succès d'un casseur évolué. Ainsi, un même mot de passe peut être qualifié de « faible » sur un site web et de « fort » sur un autre. L'utilisation d'un tel outil n'est généralement pas un choix de l'utilisateur mais un passage obligé pour créer un compte sur un site web. Lorsqu'il s'agit d'un choix, il faut s'assurer que le mot de passe est bien conservé localement et qu'il n'est pas transmis au site web.

Mesure de la robustesse d'un mot de passe

Brigitte a choisi un nouveau mot de passe en suivant les consignes qu'elle a lues sur un forum : il contient des lettres (majuscules et minuscules), au moins un chiffre et au moins un caractère spécial : « Anticonstitutionnellement1234! ». Elle l'a testé sur plusieurs sites web qui mesurent la robustesse de mots de passe. Elle a de la chance, tous ces sites faisaient la vérification localement dans le navigateur et ne pouvaient donc pas voler le mot de passe de Brigitte. Là où elle a moins de chance, c'est que parmi les 5 sites testés, y compris un éditeur de logiciels antivirus et un site ministériel français, tous lui ont dit que son

mot de passe était fort, l'un d'entre eux spécifiant même qu'il faudrait plusieurs siècles pour le casser. Malheureusement, son mot de passe ne résistera pas plus d'une seconde face à un casseur évolué car il correspond au masque le plus classique qui existe : mot du dictionnaire avec une lettre capitale au début, suivi de chiffres et d'un caractère spécial parmi les plus utilisés.

FOCUS **Agences en cybersécurité**

De nombreux pays possèdent une ou des agences pour la cybersécurité dont les missions sont essentiellement d'assurer l'expertise étatique dans ce domaine en vue de sécuriser les administrations publiques, le secteur privé, voire les particuliers et, *in fine*, la société civile. Pour cela, ces agences peuvent être amenées à accompagner la conception ou le développement de produits de sécurité, par exemple en les certifiant, contrôler les mesures de sécurité mises en place par une administration ou une entreprise du secteur privé, intervenir directement en cas d'attaque, etc. Les prérogatives de ces agences diffèrent d'un pays à l'autre mais elles ont généralement la caractéristique de jouir de fortes compétences en cybersécurité et de publier des recommandations à l'état de l'art. On peut notamment mentionner l'Agence nationale de la Sécurité des Systèmes d'Information (ANSSI) en France, l'Office fédéral de la Cybersécurité (OFCS) en Suisse, le Centre pour la Cybersécurité Belgique (CCB), le Centre canadien pour la Cybersécurité (CCC), l'Office fédéral de la Sécurité des Technologies de l'Information (BSI – *Bundesamt für Sicherheit in der Informationstechnik*) en Allemagne, l'Institut national des Normes et de la Technologie (NIST – *National Institute of Standards and Technology*) aux États-Unis, ou encore l'Agence de l'Union européenne pour la Cybersécurité (ENISA – *European Union Agency for Cybersecurity*). Ces agences ne doivent pas être confondues avec des agences de renseignement.

Les phrases de passe

Pour générer des mots de passe robustes mais faciles à mémoriser, une approche consiste à utiliser des « phrases de passe », c'est-à-dire des suites

de mots (plutôt que simplement des caractères) choisis aléatoirement. Ainsi, une phrase de passe de sept mots choisis dans un dictionnaire de 60 000 mots peut être tout aussi robuste qu'un mot de passe aléatoire de 17 lettres, chiffres et/ou caractères spéciaux. Utiliser des mots plutôt que des caractères permet d'augmenter la taille de l'alphabet : cette approche est recommandée par l'ANSSI dans son guide sur les mots de passe. Bien évidemment, il faut que les mots soient choisis aléatoirement dans le dictionnaire. Si les mots sont choisis par l'utilisateur lui-même, la phrase de passe risque d'être bien faible car l'humain n'utilise généralement que quelques centaines de mots dans son langage quotidien.

Les gestionnaires de mots de passe

L'utilisation d'un gestionnaire de mots de passe est aujourd'hui recommandée par tous les grands acteurs étatiques de la cybersécurité (ANSSI, Cybermalveillance, NIST, BSI, etc.). Le gestionnaire permet de satisfaire les trois contraintes mentionnées plus haut : mot de passe aléatoire, usage unique et possibilité de changement fréquent.

Un gestionnaire de mots de passe est par exemple une application installée sur un équipement informatique (ordinateur, téléphone portable, etc.) ou une extension d'un navigateur (Chrome, Firefox, etc.). Le gestionnaire stocke dans un coffre-fort numérique chiffré tous les mots de passe de l'utilisateur pour qu'il n'ait pas besoin de les mémoriser. L'utilisateur n'a alors qu'à se souvenir d'un seul mot de passe qui lui donnera accès à tous les autres : c'est le mot de passe maître. Les gestionnaires de mots de passe permettent également de générer des mots de passe robustes à la place de l'utilisateur.

Pas de doute, la sécurité du gestionnaire repose sur la qualité du mot de passe maître : celui-ci devra donc être le plus fort possible tout en restant mémorisable. Les gestionnaires possèdent également des contraintes qu'il est important de mentionner.

Mémoriser son mot de passe maître

Le mot de passe maître doit être robuste et mémorisable. Ne pas se souvenir de son mot de passe maître peut conduire à une situation critique

…

car il n'y a aucun moyen de le retrouver. L'écrire et le conserver dans un endroit sûr peut prévenir une telle situation. Typiquement, si le cybercriminel dont on souhaite se protéger n'est pas un proche parent, conserver son mot de passe maître dans une enveloppe cachetée à la maison est une approche acceptable : le vol ou l'ouverture non légitime de l'enveloppe doit immédiatement conduire à changer tous ses mots de passe.

Gestionnaires dans le cloud

Avec les gestionnaires les plus renommés dans le cloud, comme 1Password (payant) ou Bitwarden (gratuit), votre coffre-fort de mots de passe est chiffré sur votre ordinateur avant d'être envoyé dans le cloud.

FOCUS **Cloud**

Un cloud est un ensemble d'infrastructures informatiques et de réseaux fournissant des ressources (temps de calcul, stockage, réseau, etc.), voire des services (bases de données, noms de domaines, gestion du courrier électronique, intelligence artificielle, etc.) qui sont accessibles depuis n'importe où dans le monde, et souvent, à la demande. Les plus grands fournisseurs de services cloud dans le monde sont Amazon Web Services, Google Cloud, Azure (Microsoft) et Alibaba Cloud, mais il en existe une quantité d'autres, plus petits et parfois concentrés sur certaines zones géographiques. Plutôt que de gérer elles-mêmes leurs infrastructures et services informatiques, de nombreuses entreprises ont choisi de migrer leurs activités vers l'un de ces clouds. Par extension, on dit de données qu'elles « sont dans le cloud » lorsqu'elles sont stockées et traitées par un prestataire de cloud, voire simplement par une entreprise tierce.

Vous êtes le seul à pouvoir le déchiffrer. Pour autant que l'on utilise un gestionnaire renommé, le fait qu'il y ait une faille dans le logiciel (faille éventuellement volontaire, ce que l'on appelle une « trappe ») n'est pas un risque spécifique aux gestionnaires de mots de passe et ne doit pas