[Fiche 06] Les mots de passe

L'usage de l'informatique implique souvent d'identifier les internautes. La technique la plus courante est basée sur le couple "identifiant/mot de passe". Selon les situations, l'identifiant peut être privé ou public, mais est souvent mal protégé. Le mot de passe est l'outil qui assure donc l'essentiel de la sécurisation. Si un individu mal intentionné obtient un mot de passe d'une personne, il pourra usurper son identité avec des conséquences potentiellement très graves (récupération des données, opérations commerciales, détournement de listes de contacts, etc.).

Les opérateurs qui demandent une identification doivent donc mettre en place de nombreuses mesures de sécurité pour gérer les mots de passe : dans les règles de création, dans la méthode de conservation, etc. C'est un enjeu très important, mais sur lequel on a peu de prise (si ce n'est d'éviter les opérateurs qui conservent et/ou transmettent les mots de passe en "clair" ou dont il est établi qu'ils sécurisent mal leurs données).

Côté utilisat·rice, il faut toutefois prendre des précautions.

La première précaution est d'utiliser un mot de passe qui ne soit pas facilement devinable par un attaquant (mot de passe basiques type 123456 ou azerty, date de naissance, identique à l'identifiant…), mais il faut également se prémunir des techniques de "force brute" consistant à tester automatiquement de très nombreux mots de passe. Pour réduire ce risque, il faut que le mot de passe soit suffisamment long (minimum 14 caractères) et comporte de la diversité : des minuscules, des majuscules, mais aussi des chiffres et des caractères spéciaux. Un opérateur sérieux mettra en place des mesures protectrices : nombre limité de tentatives, utilisation de "captcha"… Cela ne dispense pas pour autant de se protéger car dans ces certains cas ces mesures ne seront plus opérationnelles (failles, récupération de la base de données chiffrée...).

Le problème reste que même une pratique numérique limitée implique d'avoir de nombreux comptes. Comme il est très important de diversifier ses mots de passe et de ne pas réutiliser le même pour tous les services, leur mémorisation devient vite complexe. Une conservation en clair sur post-it, dans un tableur ou un courriel est à l'évidence risquée.

Pour limiter ce problème de mémorisation, trois méthodes complémentaires sont disponibles :

- utiliser des "phrases de passe" facile à mémoriser, mais complexes à deviner,
- utiliser des méthodes d'identification mixtes,
- utiliser un gestionnaire de mot de passe.

Les "phrases de passe"

Plutôt que de devoir retenir des mots de passe complexes tels que "M9çT#411kl", on conseille d'adopter des "phrases de passe", plus simples à mémoriser tout en étant plus complexes à casser. Il s'agit de retenir un assemblage de termes inspiré d'éléments connus de la seule personne concernée. Au lieu de la date et lieu de naissance on pourrait mettre "NéàdouzeH13 unmardi". Cette phrase peut être liée ou non au service utilisé (de façon non évidente) pour que l'on s'en souvienne. Pour une boîte courriel par exemple : "HereJereçois~10mails/jour".
La phrase de passe permet de concilier les avantages d'un mot de passe complexe tout en le mémorisant plus facilement.

Même sur des services non critiques où une compromission du compte ne serait pas vraiment problématique (sans élément relatif à la vie privée, données bancaires, base de contact, etc.), il faut éviter d'utiliser le même mot de passe. Au minimum, on peut adopter une phrase de passe unique modulée pour chaque site avec quelques variations non prédictibles. Il s'agit là d'un compromis avec le risque que la découverte d'un mot de passe entraîne celle d'autres comptes (ex. si on est la cible particulière d'une attaque).

Les méthodes d'identification mixtes

Des opérateurs mettent à disposition des méthodes d'identification mixtes où un élément supplémentaire au mot de passe va être demandé à l'utilisat·rice. Pour les opérations importantes, l'identification se fait souvent avec un contrôle supplémentaire. Il s'agit fréquemment d'indiquer un code éphémère transmis par SMS.

La contrepartie de cette amélioration de la protection des comptes est la transmission de données supplémentaires (numéro de téléphone dans le cas précédent, validation par courriel, utilisation d'une carte à puce, mais des données biométriques peuvent aussi être utilisées dans des approches similaires). Attention toutefois cette méthode n'est pas infaillible et le vol du téléphone peut parfois paradoxalement permettre d'accéder au compte plus facilement.

Les méthodes mixtes sont très intéressantes en termes de sécurité pure. Il faudrait pouvoir s'assurer qu'elles soient bien mises en œuvre et que l'autre élément demandé n'implique pas d'autres risques. Ainsi accepter de communiquer son numéro de téléphone portable à une banque peut être justifié, fournir des données biométriques pour un achat en ligne est clairement disproportionné.

Les gestionnaires de mots de passe

Quelle que soit la manière dont on fabrique ses mots de passe, leur mémorisation est toujours un défi. Une solution est d'utiliser des gestionnaires de mots de passe qui offrent une protection sans effort de mémorisation.

Attention, toutes les solutions disponibles ne sont pas équivalentes. Ainsi, la quasi-totalité des navigateurs offre la possibilité d'enregistrer les mots de passe. Cette possibilité, si elle simplifie la vie, peut s'avérer dangereuse. Ce point est critique sur Firefox, mais aussi sur d'autres navigateurs où, par défaut, les mots de passe sont conservés en clair sans protection. Un mécanisme similaire existe au niveau du système sur Mac où, par défaut et sur simple validation de l'utilisat·rice, tous les mots de passe sont enregistrés dans un "trousseau".

Quiconque ayant accès au navigateur peut prendre connaissance de tous les mots de passe enregistrés. Pour pallier ce risque, il est préférable de ne pas y recourir. Si l'on ne peut s'en passer, il est absolument nécessaire de créer un "mot de passe principal" protégeant l'accès aux mots de passe enregistrés. Il faudra l'indiquer à chaque session ou accès, mais c'est une protection indispensable. La procédure est détaillée dans l'aide de Firefox.

> En bref, il s'agit d'aller dans "Préférences", onglet "Sécurité", "Utiliser un mot de passe principal", puis d'indiquer une phrase de passe.

Une meilleure solution est d'utiliser un gestionnaire extérieur. Ce logiciel, à installer sur son ordinateur, gérera la mémorisation des mots de passe à notre place. Si les pratiques varient d'un logiciel à l'autre, les plus sérieux chiffrent les mots de passe qui ne deviennent accessibles qu'en fournissant le mot de passe maitre, le seul à devoir être mémorisé par l'utilisat·rice. Il doit être

complexe et respecter les règles précédemment évoquées. Il sera ensuite possible de stocker tous les mots de passe, même les plus complexes, dans le gestionnaire sans devoir les mémoriser.
Le logiciel peut aussi proposer des mots de passe complexes (qu'il est tout de même conseillé de les modifier après génération, par précaution).

De nombreux gestionnaires sont disponibles ; Lastpass, onepassword… En raison de sa gratuité, de sa relative praticité d'utilisation, du fait qu'il ait été audité et certifié par l'ANSSI comme sûr, et qu'il s'agisse d'un logiciel libre, le CECIL recommande le logiciel "Keepass" ou son "Fork"KeepassXC. Il s'agit de références en la matière.

Une pratique plus basique peut être de conserver ses passes peu utilisés dans une archive chiffrée en AES avec une phrase de passe solide.

Pour aller plus loin :

- l'ANSSI est l'Agence nationale de la sécurité des systèmes d'information, rattachée au Secrétaire général de la défense et la sécurité nationale. Elle "assure la mission d'autorité nationale en matière de sécurité des systèmes d'information". À ce titre elle préconise des règles de sécurisation des systèmes d'information pour le grand public,
- les recommandations de l'ANSSI sur les mots de passe qui ont toutefois certains défauts,
- une fiche pratique de la CNIL, *Sécurité : Comment construire un mot de passe sûr et gérer la liste de ses codes d'accès ?*,
- un tutoriel de la CNIL sur Dailymotion pour installer et utiliser Keepass,
- une fiche de la CNIL concernant le piratage de ses comptes sociaux *via* mot de passe ("prévenir, repérer et réagir"),
- quelques règles de base sur la création de mots de passe sur Ecrans.fr, *Choisir un bon mot de passe*,
- Zythom.blogspot.fr, *Cracker les mots de passe*, une présentation sur les méthodes "de base" permettant de casser des mots de passe pour comprendre ce dont il faut se prémunir,
- Quartz, Qz.com (en anglais), *A password like "adgjmptw" is nearly as bad as "123456"*, sur les séquences de mots de passe à éviter,
- NextInpact.com, *Ashley Madison : les mots de passe navrants de banalité*,
- NextInpact.com, **Mots de passe : on vous aide à choisir le gestionnaire qu'il vous faut**,
- Numerama.com, *Vos réponses aux questions secrètes ne sont pas si sûres, prévient Google*, sur les limites des questions secrètes pour la récupération des mots de passe,
- LeMonde.fr, *Le mot de passe, espèce en voie de disparition*, sur les velléités des constructeurs de remplacer les mots de passe par d'autres méthodes, notamment par des méthodes biométriques,
- Pour sortir des seules considérations de sécurité et de protection, voir les deux articles suivants du New York Times (en anglais), *The secret life of passwords*, et de Rue 89, *Dans mon mot de passe, il y a…*, qui révèlent tout l'intime et l'aspect émotionnel et poétique de certains mots de passe.

Fiche 6 [publiée le 2 avril 2015, dernière mise à jour avril 2018]