Mot de passe : quelles alternatives ?

Il existe des règles basiques pour bien utiliser les mots de passe. Pour que ce système soit efficace, il faut impérativement utiliser un mot de passe différent par compte, et que chaque mot de passe ne soit pas trop facile à trouver.

Malheureusement chaque année les classements nous montrent que les mots de passe les plus souvent utilisés restent trop simple comme « 123456 », « password » etc. et ce sont donc aussi, assez logiquement, les plus piratés.

Les études sur le sujet confirment également que la majorité des internautes utilisent un même mot de passe pour plusieurs (si ce n'est tous leurs) comptes, ce qui permet au pirate d'accéder à plusieurs comptes dès qu'il en a trouvé un. Il est faux de croire que le moyen d'attaque le plus courant pour les hackers est de deviner les mots de passes. Dans un monde ou des milliards de mots de passe sont en vente sur le Dark Web, il n'est plus nécessaire de deviner, juste de dérober ou d'acheter pour quelques centimes.

Sachant qu'un internaute possède en moyenne 100 comptes en ligne, il apparaît alors logique de devoir s'appuyer sur la technologie pour gérer sans peine cette multitude de mots de passe complexes. Les outils existent déjà, encore faut-il les utiliser.

Un standard de fait

Si le mot de passe s'est imposé depuis des décennies comme un « standard de fait », ce n'est pas l'œuvre du hasard. Pour réussir à substituer un standard par un autre, il faut offrir plus que ce que le premier proposait. Or le système des mots de passe en propose déjà beaucoup : c'est en effet une technologie peu coûteuse, non brevetée, facilement modifiable et qui peut être utilisée de manière anonyme.
Pour remplacer cette technologie devenue un standard de fait, les autres technologies doivent apporter une meilleure solution, plus sûre et plus pratique, pour compenser largement les coûts liés au changement.

Quelles alternatives ?

On peut identifier trois grands types de solutions souvent présentées comme les alternatives crédibles aux mots de passe. Revue des troupes.

Le SSO, limité par la concurrence, et impossible à sécuriser

La première solution est la technologie de l'authentification unique (Single Sign On ou SSO). Avec une solution de SSO, il suffit de se connecter une seule fois à un service, généralement proposé par un des grands acteurs de l'internet (Apple, Google, Facebook…) pour pouvoir accéder ensuite, et sans nouvelles étapes d'identification, à une multitude d'autres sites qui font confiance à la première authentification. Très pratique sur le papier, ce système est confronté à un problème

important qui bloque son expansion : aucun de ces géants ne donnera accès aux données de ses clients à l'un de ses concurrents. Apple n'est pas près d'autoriser Facebook à venir collecter les emails et mots de passe de ses clients pour leur permettre de s'authentifier.

Mais plus grave encore, un SSO repose sur l'idée d'une clef d'accès unique pour des dizaines ou des centaines de comptes. Si un SSO est compromis, tous les comptes accessibles par l'intermédiaire de ce SSO le sont d'un seul coup. Pendant longtemps on a pu croire que les moyens et la technologie des grand acteurs de l'Internet les protégeaient de ce risque. Mais dans les 6 derniers mois de 2018, les SSO de Facebook et Google ont été compromis et les clefs de millions d'utilisateurs révélées à des hackers sophistiqués et déterminés.

L'authentification forte, une solution pour les pro

Également présentée comme le futur fossoyeur des mots de passe, l'authentification à deux facteurs (2FA) est basée sur l'association d'un facteur que vous connaissez, votre code de carte bleue par exemple (un mot de passe en réalité), et d'un second facteur que vous possédez, comme votre carte de crédit. Vous devez avoir accès aux deux en même temps pour pouvoir vous authentifier, ce qui complique la tâche des pirates. Si cette solution apporte un niveau de sécurité plus élevé, le plus grand frein à son développement est qu'elle implique une complexité que le grand public n'est pas prêt à assumer.

Pourquoi devoir acheter un lecteur de carte à puces ou d'une clé USB dédiée si cela ne fait que ralentir le processus de connexion aux sites web ? Autre inconvénient par rapport aux mots de passe : il n'est pas possible de l'utiliser de manière anonyme. Enfin, l'authentification forte ne remplace pas le mot de passe, elle vient s'y ajouter.

Biométrie : rêves et réalité

Sous différentes formes, la coqueluche des médias est incontestablement la biométrie. Empreinte digitale, reconnaissance faciale, rétinienne ou vocale jusqu'aux pilules, pour les innovations les plus fantaisistes, la biométrie nous est présentée comme la solution parfaite. Malheureusement, derrière ce vernis prometteur, la biométrie a en réalité très peu de chances de remplacer les mots de passe. D'une part, les coups de déploiement sont encore bien trop importants, même s'ils baissent au fur et à mesure que la technologie se démocratise, par exemple sur nos téléphones. Ni les sites ni les particuliers ne sont prêts à s'équiper. Et s'équiper de quoi ? Un lecteur d'empreinte, d'iris, du visage ?

D'autre part, la biométrie ne propose pas tous les services que propose le système actuel : impossible de l'utiliser de façon anonyme, mais aussi et surtout impossible de changer son empreinte digitale comme on peut changer un simple mot de passe. Ce n'est pas une hypothèse, on sait que les pirates sont déjà capables de reproduire des empreintes digitales, des voix pour tromper les systèmes d'authentification. La biométrie s'est déjà fait rattraper par les cybercriminels, excepté à un haut niveau de sophistication, encore réservé à des usages restreints.

C'est pourquoi le mot de passe est aujourd'hui la norme… et qu'il n'est pas près d'être remplacé quoiqu'en disent les marchands. On peut faire un parallèle avec le clavier AZERTY mis au point en 1847 en fonction de la place des touches sur les premières machines à écrire et qui est toujours utilisé jusque sur nos smartphones, qui n'ont pourtant pas de clavier physique.

Sachant cela, il n’est pas inutile que les internautes apprennent à mieux gérer leurs mots de passe afin de protéger leurs précieuses données personnelles plus que jamais disséminées sur chacun de leur compte sur Internet.