Bientôt la fin du mot de passe ?

Aujourd'hui encore, le mot de passe reste le moyen d'authentification le plus courant et le plus utilisé. Pourtant, il est l'une des solutions d'authentification les plus vulnérables.

Le mot de passe ne présente pas une preuve suffisamment robuste pour prouver son identité. En effet, quiconque s'empare du mot de passe d'un compte peut alors y accéder et récupérer des informations. La sécurité des comptes protégés par mots de passe repose uniquement sur la robustesse de ces derniers qui est, la plupart du temps, insuffisante. Ainsi, deux développeurs d'outils en sécurité ont créé le projet Richelieu, regroupant une liste des 20 000 mots de passe français les plus communément utilisés.

Nous constatons que les utilisateurs ne sont pas réceptifs à l'idée de mémoriser des chaînes de caractères mêlant majuscules, minuscules, chiffres et caractères spéciaux tel que préconisé par l'ANSSI ou encore la CNIL. Ils veulent quelque chose de simple et facile à retenir, mais qui se trouve, par la même occasion, fortement vulnérable. Or comme si cela ne suffisait pas, les préconisations en matière de complexité des mots de passe s'accompagnent bien souvent d'une politique de renouvellement des mots de passe. Microsoft a reconnu que ces politiques d'expiration de mot de passe adoptées jusqu'à présent constituaient une mesure de sécurité inutile, le SANS et le NIST appuyant cette approche.

Les logiciels gestionnaires de mots de passe

Pour pallier les difficultés de mémorisation de mots de passe robustes, des solutions de coffres-forts de mots de passe ont fait leur apparition.

De nombreux produits existent aujourd'hui sur le marché **(Keepass, Lastpass, Dashlane, 1Password…)** permettant de stocker les mots de passe en toute sécurité dans un coffre-fort numérique. L'avantage de ces outils est de n'avoir plus à retenir qu'un seul mot de passe permettant de déverrouiller le coffre-fort et ainsi accéder à tous ses mots de passe. Ainsi, le mot de passe à retenir, appelé « mot de passe maître », est d'une criticité très importante : il doit être extrêmement robuste et pour autant facilement mémorisable. Il est également important de souligner la démocratisation de coffres forts numériques à vocation bien plus large que le simple stockage de mot de passe, telle que la solution Vault de chez Hashicorp.

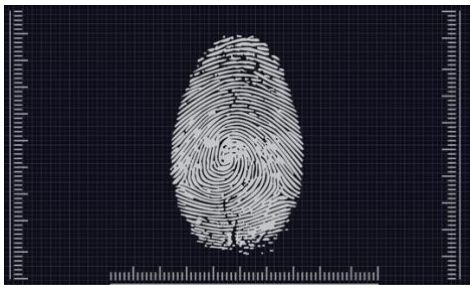
Le « Social Provider »

Une autre solution largement démocratisée consiste en l'utilisation d'un « Social Provider » tel que Google ou Facebook pour accéder à un site plutôt que de créer un compte spécifique à chaque fois. Toutefois, ces solutions ne sont pas adaptées au monde de l'entreprise ; de

plus, les social providers sont presque intégralement américains, ce qui restreint certains cas d'usage.

Les facteurs d'authentification

C'est dans ce contexte que se sont démocratisés d'autres facteurs d'authentification.



Pour rappel, les facteurs d'authentification sont les suivants :

- *Ce que je sais* : Mot de passe, code PIN, etc.
- *Ce que je possède* : un téléphone, un token physique, une pièce d'identité, etc.
- *Ce que je suis* : L'ensemble des solutions biométriques telles que l'empreinte digitale, la reconnaissance faciale, vocale, etc.

Contrairement aux mots de passe et codes secrets (ce que je sais) qui s'implémentent aisément avec un simple champ de saisie, l'intégration des solutions biométriques (ce que je suis) a nécessité une démocratisation technologique. Or depuis quelques années maintenant, le marché des solutions permettant d'effectuer une authentification par capteur biométrique est de plus en plus mature : la majorité des téléphones et ordinateurs intègre désormais nativement un capteur. Et au niveau réglementaire, des directives telles que le RGPD ont normé ce nouvel usage de données personnelles.

De même pour le dernier facteur (ce que je possède), les solutions se sont démocratisées dans un format réduit facilitant leur adoption et réduisant leur coût (yubikey, application MOTP, etc.). Cependant, l'intégration de ce type de solutions nécessite avant tout un standard d'échange éprouvé. C'est dorénavant chose faite avec WebAuthN ou encore FIDO2 qui normalisent l'intégration de ces solutions (ce que je suis et ce que je possède) dans les applications web.

« L'authentification multi-facteurs repose sur l'idée qu'aucun facteur n'est parfait. »

Ainsi, la mise en œuvre d'une authentification forte ou multi-facteurs devient de plus en plus aisée, permettant ainsi d'assurer un contrôle d'accès renforcé aux ressources sensibles en garantissant un meilleur niveau de sécurité. L'authentification multi-facteurs repose sur l'idée qu'aucun facteur n'est parfait. Chaque facteur implémenté présente des points forts et des points faibles. Ainsi un deuxième, voir un troisième facteur viendra compenser les limites des autres, et inversement.

« L'authentification multi-facteurs s'est aujourd'hui généralisée dans les usages qui le nécessitent dans un contexte de plus en plus risqué et dangereux »

Le passage vers une authentification forte se généralise via des directives et préconisations institutionnelles :

- Dans le domaine bancaire par exemple, la Direction sur la Sécurité des Paiements rend obligatoire l'authentification forte pour les paiements en ligne.
- Au niveau national, la Loi de Programmation Militaire (LPM), ainsi

que l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) préconisent l'utilisation d'une authentification forte dès que cela est possible.

- Plus largement, au niveau européen l'Agence Européenne de CyberSécurité (ENISA) a publié une étude avec des recommandations précises quant à la mise en œuvre du RGPD préconisant le recours à une authentification double facteurs.
- De même de l'autre côté de l'océan atlantique, le « National Institute of Standards and Technology » (NIST) a mis à jour ses recommandations pour l'utilisation de l'authentification multi-facteurs.

L'authentification multi-facteurs s'est aujourd'hui généralisée dans les usages qui le nécessitent dans un contexte de plus en plus risqué et dangereux (télétravail, travail en mobilité, tentative de fraude et vol d'identité…).

Les éditeurs de logiciels intègrent de plus en plus ces standards afin de répondre aux besoins de sécurité de leurs clients.

Le mot de passe n'est pas encore mort, car très facile à implémenter et à mettre en œuvre, il reste très largement utilisé pour l'accès aux applications, systèmes.

Comme exposé précédemment, de nouvelles solutions existent et permettent de renforcer le niveau de sécurité par l'utilisation de plusieurs facteurs. Auparavant réservée à des contextes très sensibles, l'intégration de ce type de solutions au sein des applications et systèmes d'information est aujourd'hui facilitée par l'utilisation de standards comme SAML ou OpenIDConnect par exemple et grâce à une montée en maturité des solutions.
Un projet d'authentification forte ? Formind est en capacité de vous accompagner depuis la phase de design jusqu'à la phase de mise en œuvre et de maintien en conditions opérationnelles.

Rédacteurs : L'équipe Intégration

formind CONSULTING