Tous plongés dans l'enfer du mot de passe (et quelques trucs pour s'en sortir)

Nos mots de passe sont souvent tellement nombreux qu'il est pratiquement impossible de tous les mémoriser, sans compter qu'à cet inconvénient s'ajoutent des risques de piratage.

Avec Benjamin Bayart

Atlantico : Le créateur du mot de passe, Fernando Corbato, a déclaré que le mot de passe était devenu un calvaire. Quelles sont les difficultés que rencontrent aujourd'hui les utilisateurs ?

Benjamin Bayart : Il existe deux grandes lignes. D'une part, les problèmes que les utilisateurs ne voient pas mais ressentent. Normalement en matière de sécurité, il ne faudrait pas utiliser le même mot de passe sur différentes plateformes. Or, vu le nombre de mot de passe que l'utilisateur doit générer et surtout retenir, nous arrivons à un nombre de 300 mots de passe à mémoriser, c'est impossible. Ce mécanisme pose problème. Il y de nombreux sites où la structure du mot de passe est imposée, il doit par exemple contenir une majuscule, un chiffre ou autre. De ce fait, le mot de passe habituel utilisé ne peut pas être exploité sur ces plateformes, ce qui rend la mémorisation encore plus complexe.

Nous sommes face à une erreur structurelle, à l'origine le mot de passe devait valoir pour un seul point d'entrée. Partant de cette logique, pour trois plateformes différentes, il faudrait trois mots de passe différents. Ce système fonctionnait parfaitement dans les systèmes informatiques des années 60 car un mot de passe était utilisé pour déverrouiller un ordinateur, il n'y avait pas tous les services et sites que nous avons aujourd'hui.

D'autre part, les mots de passe sont pour la majorité à sécurité très faible. Idéalement, il faudrait ne jamais utiliser le même mot de passe, ne pas le noter sur un carnet et le mémoriser, mais ces mesures paraissent impossibles vu le nombre de mots passe que les utilisateurs détiennent. De ce fait, les personnes utilisent des mots de passe très simples, composés par exemple du nom de leur mère, enfants, femme, mari, date naissance et autres. Ils facilitent ainsi leur décodage car il est bien souvent simple à retenir donc facile à trouver.

Qu'en est-il du côté des acteurs, notamment lorsque des mastodontes comme eBay en viennent à demander à leurs utilisateurs de changer leur mot de passe ?

Le problème de fond est le manque d'efforts de ces plateformes. Les outils de standardisation qui sont mis en place sont peu utilisés. Le problème majeur est la centralisation des données, le fait qu'E-bay détiennent des millions de mots de passe est problématique. **Le monde serait plus sûr si les mots de passe n'étaient pas la propriété de plateformes comme eBay, Facebook et autres.**

Il existe des plateformes d'OpenID qui permettent une autre voie d'identification. Si l'utilisateur souhaite se connecter sur un site A, il s'identifie sur le site B. C'est utilisé lorsque vous pouvez vous connecter par exemple avec votre compte Facebook ou Twitter. Ce

mécanisme n'est pas réellement optimal aujourd'hui mais il a l'avantage d'être plus sécurisant. Le point noir réside dans le fait que ces plateformes ne sont pas spécialisées dans la sécurisation des données.

Une plateforme qui détient autant d'identités comme Facebook, cela est extrêmement dangereux. Lorsqu'elles sont piratées, c'est un drame mondial, alors que ces incidents devraient être anodins.

Quels sont les conseils pour avoir une gestion optimisée de ses différents mots de passe ?

La bonne méthode consiste à utiliser un portefeuille de mots de passe, qui est un logiciel de stockage. Il va mémoriser les mots de passe complexes des utilisateurs, et son accès est sécurisé par un seul mot de passe que l'utilisateur a choisi et mémorisé. C'est un système très sécurisant, car dans le cas où Ebay se fait pirater, il suffit à l'utilisateur de changer uniquement son mot de passe pour cette plateforme.

Quelles sont les limites du mot de passe aujourd'hui ? Sommes-nous arrivés à l'essoufflement de sa mécanique ?

Il était au départ prévu qu'un utilisateur ait un mot de passe pour définir son identité.**Aujourd'hui, ces mots de passe sont stockés dans des centaines d'endroits alors qu'ils ne devraient pas l'être.** Le problème vient de la multiplication des lieux de stockage.**Le portefeuille de mot de passe ou les plateformes d'OpenID sont des systèmes qui permettent de revenir à un seul mot de passe.**

Les utilisateurs commencent à comprendre les limites du mot de passe. Nous sommes arrivés à l'essoufflement de la mécanique telle qu'on la pratique : le mot de passe répliqué à plusieurs endroits. Le mot de passe en tant que tel n'est pas essoufflé, c'est son utilisation actuelle qui représente un danger.

Quelles sont les autres alternatives existantes ?

Il faudrait ouvrir un compte au sein d'un fournisseur d'authentification qu'on appelle un fournisseur d'identité OpenID, l'utilisateur peut ouvrir autant de comptes que d'identités souhaitées pour les différentes plateformes (une identité pour les impôts, la banque, les sites politiques, les jeux en ligne). Ces plateformes sont spécialisées dans la sécurisation des identités, de ce fait, elles sont plus aptes à gérer les mots de passe. Seulement, les plateformes d'OpenID sérieuses et fiables, il n'en existe pas réellement. Toutes les plateformes qui fournissent de l'authentification fournissent d'autres services, et pour y accéder, il faut s'identifier. Or ce n'est pas leur métier et ils ne savent pas sécuriser, et c'est exactement le cas d'Ebay. **Les plateformes d'OpenID ne peuvent bien fonctionner que si elles sont payantes car leur rémunération par la publicité ou autre suggère la revente des données personnelles, ce qui représente un danger.** Ce service ne peut pas être gratuit, il devrait être à 4 euros ou 5 euros par an.

Dans un monde idéal, il faudrait que l'outil soit le système d'authentification, par exemple un ordinateur ou un téléphone. Les systèmes vont dans cette voie, pour réaliser un virement sur votre banque en ligne, le banquier vous envoie un code sur votre téléphone. Imaginons que le téléphone puisse faire serveur OpenID et qu'il gère vos différentes identités. Lorsque l'utilisateur se rend sur un site comme Ebay, il souhaite se connecter et son téléphone lui demande s'il souhaite s'identifier et avec quelle identité. De ce fait, il ne suffit pas qu'une personne vous vole votre mot de passe pour rentrer dans votre compte.