L'insécurité du « Login / Mot de passe » face aux enjeux d'Internet
Internet
Posté par : JPilo
Publiée le : 7/3/2011 15:00:00

Je suis un inconditionnel de l'usage d'Internet ! Chaque jour, pour mon travail ou à titre personnel, je suis connecté sur la toile. Comme chacun d'entre nous, ma vie est régulée par l'utilisation du fameux couple « Login / Mot de passe » !

J'accède à ma messagerie Gmail, mon réseau d'entreprise, mes comptes Facebook, Twitter, Linkedin, Viadeo... avec un **« Login / Mot de passe »**. Et puis comme nous tous, je me pose des questions sur notre avenir en ligne quand je réalise que le monde change à une vitesse vertigineuse.

Mon PC d'hier est devenu un iPad, mon iPad d'aujourd'hui sera demain ma télévision connectée à mon fournisseur d'accès et plus besoin d'aucun logiciel puisque tout est disponible sur le web....mais avec ce fameux « Login / Mot de passe », étant donnés sa fragilité et les cas de piratage sur Internet, je me dis que finalement, même mes données personnelles sont disponibles pour tous sur Internet !

Alors avec juste un peu de bon sens, je réalise que si quelqu'un accède à mon nom, mon prénom, ma date de naissance, mon adresse personnelle, etc... Il peut devenir moi ! Et les conséquences deviennent effrayantes puisque si quelqu'un d'autre est moi, il peut me voler de l'argent, faire des

actes délictueux en mon nom, et ce sera à moi de me justifier et d'en subir les conséquences, il peut donc transformer ma vie en cauchemar en quelques clics de souris...

Les scandales se multiplient dans les médias, chaque jour partout dans le monde, de nouvelles victimes apparaissent. En France, l'usurpation d'identité représenterait plus de 210 000 victimes par an selon le CREDOC en 2009, et ces chiffres ne cessent de progresser.

Je lis pourtant dans la presse que tout le monde est bien conscient de cette fragilité en matière de sécurité mais je ne vois pas beaucoup d'actions et de réponses aux problèmes. Comme tout le monde, mon Mot de passe est presque le même pour tous les sites auxquels je suis connecté. Je sais bien que j'augmente mon risque d'usurpation d'identité mais j'ai du mal à gérer de nombreux mots de passe différents.

Alors, je découvre quand même qu'il existe des solutions alternatives pour sécuriser mon Mot de passe. L'une, appelée le SSO (Single Sign On) est un gestionnaire de mots de passe. On enregistre tous ses mots de passe puis c'est le logiciel qui les gère, les renouvelle, etc, intéressant comme concept mais je reste sur la base d'un mot de passe et en tant que néophyte, l'utilisation n'est pas toujours adaptée à ma connaissance.

L'autre solution largement utilisée au sein des entreprises s'appelle des solutions d'authentification forte à base de Tokens, des petits boîtiers que l'on vous donne et qui affichent une suite de numéros qu'il faut taper dans une fenêtre sur sa page de connexion du site web concerné. Une autre alternative repose sur le même principe de saisie de numéros mais c'est une petite application installée sur votre smartphone qui vous le délivre.

Toutes ces solutions sont certes efficaces mais ne remportent pas une large adoption par le public car bien souvent pas adaptées aux besoins. Le public sur Internet n'est pas constitué que d'ingénieurs, et posséder un Token par site web reviens à transformer ses internautes en porte-clés ! Je préfère m'abstenir de parler également du coût de fabrication et de gestion de ces Tokens car nous constatons que ces solutions pourtant viables technologiquement ne peuvent pas l'être sur un marché aussi vaste que celui du web.

Dans ce contexte, d'autres approches orientées sur les usages semblent mieux adaptées au marché. En effet, il s'agit d'ajouter l'authentification d'un équipement que l'internaute possède déjà. Dans ce cas, on ajoute à ce que vous savez (votre mot de passe ou code PIN par exemple), ce que vous possédez (un équipement matériel). Cette méthode appelée authentification à deux facteurs permet de garantir que vous êtes bien celui que vous prétendez être.

Comment fonctionne cette technologie : l'internaute qui accède à un site web équipé de ce système (appelé l'ADN du Numérique) choisit d'ajouter l'ADN numérique d'un équipement de son choix (son ordinateur ou son smartphone ou sa clé USB, etc.. voir même plusieurs équipements.) à son compte existant.

La technologie va alors créer et enregistrer l'ADN de cet équipement qui sera utilisé pour toutes ses connexions comme une clé de démarrage pour une voiture. L'équipement est connecté, l'internaute accède à son compte en ligne, il est déconnecté, l'internaute ne peut plus y accéder. Facile à expliquer, présenter et utiliser, cette technologie est mieux adaptée au public qui peut d'ailleurs utiliser le même équipement sur plusieurs sites web.

Le choix de cette approche permet de garantir un accès sécurisé à un service en ligne. Il n'est plus possible de partager son « Login / Mot de passe » avec différentes personnes. Il permet notamment aux entreprises qui proposent des services et des abonnements en ligne, de s'assurer qu'un seul abonné accède à son contenu. Ce point est particulièrement sensible pour différents secteurs tels que les médias (musiques, vidéos, jeux en ligne, etc.), les offres de partage de documents et de coffre-fort électronique en ligne, les jeux d'argent en ligne, les services financiers, les services de

dématérialisation qui génèrent leurs revenus par de la vente d'abonnement pour accéder au service en ligne.

De plus, la démocratisation de ces nouvelles solutions sur Internet permettra rapidement de protéger les données personnelles ou sensibles des internautes sur de multiples sites tels que les réseaux sociaux, les boîtes emails sur Internet, etc.

Le challenge du web d'aujourd'hui repose sur la création de nouvelles solutions d'authentification pour les internautes respectant les usages pour ne pas entrer en conflit frontal avec les « mauvaises » habitudes. L'homme par essence est réfractaire aux changements. Cependant, face à l'insécurité de notre environnement numérique, il est devenu indispensable de proposer des solutions à la portée de tous. C'est à cette unique condition que la confiance numérique pourra être restaurée d'une part et que, d'autre part, les fondations d'un écosystème respectueux de l'identité de chacun et sécurisé pour tous permettront à notre monde de grandir vers de nouveaux horizons.

François-Pierre Le Page

Président Directeur Général Login People

Conseiller du Commerce Extérieur de la France