Cybersécurité, en route pour la biométrie

(Article 1/3) - Par Philippe Le Pape, expert sécurité et identité, Vice-Président du développement international et des partenariats au sein de la division Digital Security & Authentication de Safran Identity & Security (ex Morpho).

PAIEMENT CONNECTIVITÉ

POSTÉ LE 06.30.16

En février dernier, à l'occasion de la Journée pour un Internet plus sûr, le président des États-Unis, Barack Obama, annonçait un Plan d'action national sur la **cybersécurité** (Cybersecurity National Action Plan, CNAP). Cette nouvelle initiative a pour objectif de renforcer la cybersécurité dans les secteurs privés et gouvernementaux américains. L'annonce est tombée après une vague de fuites de données et de cyberattaques dont ont été victimes les réseaux privés et gouvernementaux.

La fraude en ligne au moyen de logiciels malveillants et de phishing submerge Internet. En 2015, la société de solutions de sécurité informatique **Kaspersky Labs** a détecté plus de 100 000 objets malveillants – entre autres, des fichiers scripts, des exploits et des fichiers exécutables. L'une des caractéristiques préoccupantes de la fraude en ligne est la facilité avec laquelle les identités usurpées et les comptes piratés peuvent être monnayés. En outre, la nature de plus en plus sophistiquée des formes d'attaques privilégiées par les fraudeurs, comme le souligne **Symantec dans son rapport annuel sur les menaces en matière de sécurité (en anglais)**, n'est plus à démontrer.

L'usurpation d'identité est le fait de dérober les données personnelles d'un tiers afin de voler de l'argent ou d'obtenir d'autres avantages comme des remboursements fiscaux. Utiliser de **faux documents**, ou des documents obtenus de manière frauduleuse en vue d'usurper une identité n'est pas un nouveau délit, et les spécialistes se penchent depuis longtemps sur les enjeux d'**authentification** et de protection de ce type de documents. Avec le développement des services en ligne, les échanges numériques et les paiements sur Internet ont accru le type d'identificateurs pouvant être utilisés pour frauder ou voler une identité. Les besoins des particuliers, des entreprises et des banques ont donc évolué et leur mutation se poursuit : les particuliers comptent sur les facteurs sécurité et simplicité d'utilisation pour effectuer des **transactions financières**.

Ces dernières années, ce constat s'est renforcé avec l'essor incroyable des outils informatiques mobiles : aujourd'hui, la grande majorité des opérations en ligne est réalisée à partir d'un smartphone ou d'une tablette. Une **étude (en anglais) réalisée l'année dernière par la Réserve fédérale américaine** a montré que 71 % des téléphones mobiles aux États-Unis sont des smartphones et que plus de la moitié des utilisateurs de smartphones utilisent leurs appareils pour effectuer une opération bancaire. Au sein de l'Union européenne, **KPMG (doc. en anglais)** a constaté que 38 % environ des détenteurs d'un compte bancaire utilisent des **services en ligne mobiles** afin d'effectuer diverses opérations. En outre, des initiatives de services publics électroniques mises en place dans différents pays du monde – **sous l'impulsion du programme d'e-gouvernement des Nations unies (en anglais)** – incitent les citoyens à effectuer différentes opérations en ligne, comme voter ou remplir ses déclarations fiscales. De plus en plus, ces actions sont réalisées depuis

un appareil mobile, avec tout ce que cela implique : déplacement perpétuel, écran limité, connexion sans fil. Bref, une multitude de caractéristiques bien loin des conditions idéales de sécurité. Symantec déclare que les fuites de données dans le secteur financier à lui seul représentent 23 % de l'ensemble des identités exposées aux risques de piratage. Pour les experts de la sécurité, le risque d'**usurpation d'identité** est encore plus élevé dans l'univers mobile, car les contraintes liées au format de ces appareils et à la connectivité permanente à portée de main accentuent leur vulnérabilité aux **cyberattaques**.

Mais alors, comment garantir la sécurité dans un monde mobile, connecté et numérique ?

Développer la confiance dans l'économie numérique.

Dans le monde numérique, la confiance est enracinée dans la capacité à bien connaitre les personnes ou les objets avec lesquels on interagit : de **solides fonctions d'authentification** facilitent cette capacité, car elles permettent de prouver que l'utilisateur – qu'il s'agisse d'une personne, d'une entité ou d'un objet – est bien celui qu'il prétend être. Pour favoriser le développement de l'économie et des **échanges numériques**, il est nécessaire d'instaurer un climat de confiance entre les différents protagonistes, particuliers et organisations, et les équipements et logiciels qui les relient.

En d'autres termes, la question est de savoir à quel moment l'on a suffisamment de preuves sur l'identité d'un utilisateur pour affirmer son authenticité et autoriser une transaction. Tandis que la synthèse du Plan d'action national sur la cybersécurité mentionne de manière claire une « **authentification multifacteurs** », le directeur des systèmes d'information du gouvernement américain a parlé précisément d'authentification à deux facteurs. Cette technique a pour objectif de vérifier l'identité d'un utilisateur par l'association de deux éléments différents pouvant être quelque chose que l'utilisateur connait, quelque chose qu'il possède ou dont il est inséparable. Le distributeur automatique de billets est un exemple de solutions dans la vie de tous les jours qui s'appuie sur l'authentification à deux facteurs : pour pouvoir retirer du liquide, il faut combiner une carte bancaire (quelque chose que l'utilisateur possède) et un code PIN (numéro d'identification personnel, quelque chose que l'utilisateur connait).

L'**authentification à deux facteurs** s'est étendue à la vérification au moyen du téléphone portable. Plusieurs grands fournisseurs d'e-mails et d'espace de stockage de données sur le Cloud utilisent désormais communément ce type de vérification. Pourtant, cette approche présente quelques faiblesses, la première étant humaine et liée au fait que nous ne sommes pas très doués, tout simplement, pour créer des mots de passe et nous en souvenir, même lorsque nous nous aidons d'un logiciel de gestion des mots de passe. Il n'y a pas si longtemps, au moment du battage médiatique autour de la sortie du dernier Star Wars, une étude a révélé que « starwars » était devenu un mot de passe très populaire dans le monde entier. Plus préoccupant encore, « 123456 » et « password » restent les plus utilisés. Cela illustre le dilemme permanent pour nous entre sécurité et simplicité.

Ce qu'il faut retenir, c'est que le mot de passe n'est plus la meilleure façon d'authentifier un utilisateur.

Cela soulève deux questions : pourquoi continue-t-on de s'appuyer sur des outils archaïques – les mots de passe alphanumériques ? Quelles approches pourraient les rendre définitivement obsolètes ? … Cette série de publications examine ces questions dans les deux prochains articles, **Vous avez vu ? Le PIN a disparu ! (2/3)** et **La Planète du tout mobile (3/3)**.