RSA : comment lutter contre le 'phishing' et le 'pharming'?

« *Nous sommes la référence en matière de gestion des accès, de preuve d'identité et d'intermédiaire de confiance. Notre offre est d'abord basée sur la méthode OTP*(one time password)*qui représente 70 % du nmarché. Ensuite sur l'identification de confiance, l'authentification*. » Alexandre Depret-Bixio, '*major account manager*' de RSA Security, résume ainsi la stratégie de la société jusqu'à l'acquisition de Cyota, à l'origine de la nouvelle offre **RSA Adaptive Authentication**, outil de lutte anti-fraude. « *Avec l'acquisition de Cyota, nous proposons une approche différente, par l'analyse des risques pour mettre en place une méthode d'authentification*. » **RSA Adaptive Authentication** reprend donc intégralement l'offre de Cyota. « *Elle permet de gérer le profil de l'utilisateur. Mais aussi de gérer le cycle de vie des applications afin d'enregistrer les données et de gérer les droits*. » Cette offre s'adresse en priorité aux services en ligne et aux services bancaires, deux secteurs très touchés par la **fraude par usurpation d'identité** (dont le *phishing*). « *La législation incite à la mise en place de systèmes d'authentification. Les banques doivent installer des solutions pour se protéger*. » Des pays comme la Suisse se ont déjà engagés dans des systèmes d'authentification forte et des technologies physiques distribuées à leurs clients. A ce titre, « *RSA Adaptive Authentication vise les clients de nos clients*« , à savoir l'authentification du consommateur, client du service financier. « *Notre premier service porte sur la **détection proactive des fraudes**, comme les attaques de '**phishing**' [1] ou de '**pharming**' [2]. Nous disposons de solutions de scan en partenariat avec les opérateurs et nous communiquons des alertes. Nous disposons de systèmes de riposte ou de « contre-mesures »; nous détectons l'origine de la menace afin de la stopper ou de la diluer en envoyant en masse de fausses vraies réponses, par exemple*. » « *Le deuxième service est la '**watermark**' [3] -la reconnaissance d'images, qui rassure l'utilisateur et lui donne plus de confiance. Ce mode de protection reste limité*. » « *Nos deux derniers services proposent une infrastructure technique adaptive d'authentification, soit de l'utilisateur soit de la transaction. Ce sont deux approches différentes mais basées sur la même technologie. Dans le temps, un moteur analyse le profil de l'utilisateur et son comportement durant les transactions. Par exemple, ses habitudes d'utilisation et de connexion, l'origine et la localisation de l'utilisateur*. » « *L'utilisateur laisse une empreinte que nous analysons. En revanche, notre système n'est pas intrusif. Nous définissons à partir de critères choisis par la banque un profil et nous lui associons un niveau de risque. Un moteur «* baïsien *» associe à l'utilisateur au moment de la transaction un scoring de 0 à 1000 qui détermine la méthode d'authentification*. » « *L'avantage de cette méthode est que l'on ne change pas les habitudes d'utilisation du consommateur. En revanche, du côté des banques le problème vient du coût du déploiement de masse. C'est pourquoi notre offre est 'adaptive', que la démarche peut évoluer dans le temps*. » **Lexique…**

[1] **Phishing** : e-mail à l'identité usurpée incitant l'internaute à déposer ses coordonnées bancaires sur un site mafieux. [2] **Pharming** : attaques multiples par *DNS Cache Poisoning* usurpant l'adresse Web d'un site légal. [3] **Watermark** : image à décrypter par l'utilisateur.