La biométrie vient au renfort de la sécurisation des mobiles

En 2016, **30% des entreprises** utiliseront **l'authentification biométrique** pour sécuriser l'usage professionnel des terminaux mobiles, estime le Gartner. **Contre 5% aujourd'hui**. Une tendance qui viserait à simplifier l'expérience utilisateur sans sacrifier la politique de sécurité de l'entreprise.

Face à la consumérisation et au phénomène du BYOD, *« les utilisateurs résistent farouchement aux méthodes d'authentification qui étaient tolérables sur PC et restent nécessaires pour renforcer l'accès sécurisé depuis les appareils mobiles*, souligne l'analyste et vice-président du cabinet d'études **Ant Allan**. *Les responsables sécurité doivent gérer les attentes des utilisateurs et tenir compte de l'expérience utilisateur sans compromettre la sécurité. »* Et le Gartner de rappeler les différentes méthodes et recommandations de sécurisation des terminaux mobiles.

Le mot de passe, première barrière

Si les mots de passe complexes, ou même à 4 chiffres, s'avèrent mal adaptés aux usages mobiles, ils n'en constituent pas moins le premier obstacle pour empêcher un utilisateur malveillant d'accéder aux données professionnelles que contient le smartphone ou la tablette (ou ses accès au système d'information de l'entreprise).

« Un code numérique à huit chiffres demande des heures à déchiffrer, et découragera les hackers occasionnels, assure **John Girard** du Gartner. Qui ajoute que *les pirates n'ont pas le temps de tester toutes les combinaisons, même avec un code à 6 chiffres, en regard des vitesses relativement lentes de traitement que nécessitent les attaques par force brute des smartphones et tablettes. »* En conséquence, le cabinet d'analyse préconise **l'usage de mots de passe à six caractères** (au moins) alphanumériques, en évitant les mots du dictionnaire.

Chiffrement et token pour les données sensibles

Autre niveau de protection : **le chiffrement des données.** Si celui-ci ne protègera pas l'accès illicite au contenu du terminal, il permet de le rendre inexploitable. A condition *« que le chiffrement ne soit pas lié à l'authentification de mise sous tension, empêchant ainsi toute récupération de la clé à partir de l'appareil »*, précise John Girard.

Pour les données ultra-sensibles, le Gartner préconise une méthode d'authentification supplémentaire : un autre mot de passe (à minima) ou, mieux, l'usage d'un identificateur via les générateurs, hardware ou software, de jetons (token) uniques. Mais, outre la lourdeur d'implémentation de ces solutions pour les terminaux mobiles et leur gestion, leur usage est tout sauf pratique en mode mobile. *« Demander aux utilisateurs de jongler avec le jeton dans une main, le téléphone dans l'autre et une mallette dans la troisième, c'est être assuré de se heurter à résistance justifiée de leur part »*, schématise l'analyste.

La biométrie en surcouche

D'où l'usage de la biométrie qui devrait simplifier l'accès aux terminaux sensibles sans pour autant supprimer les indispensables barrières de sécurité. Interface interactive (type lecteur d'empreintes), reconnaissance vocale, topographie du visage, analyse de la structure de l'iris, analyse contextuelle… Les méthodes d'identification passive ne manquent pas. Au besoin, l'usage de la biométrie peut parfaitement **se combiner, avec la saisie de mot de passe**, renforçant ainsi la sécurisation de l'accès.

Il n'en faudra pas moins vérifier **le poids de l'implémentation** et **l'accueil par les utilisateurs** d'une nouvelle politique d'authentification. *« Adopter des méthodes d'authentification sensiblement différentes pour de multiples terminaux serait potentiellement insoutenable*, commente John Girard pour qui *une combinaison de certificats X.509 (norme de chiffrement pour les infrastructures de clés publiques, NDLR) sur le terminal, de biométrie passive et d'authentification contextuelle fera probablement l'affaire. »*

Comme toujours, tout dépend du niveau de sécurité que souhaite atteindre l'entreprise. Autant de questions que le Gartner abordera au cours de son séminaire Identity & Access Management Summit 2014 en mars prochain à Londres.

crédit photo © Bloomua- shutterstock

Voir aussi
Silicon.fr étend son site dédié à l'emploi IT
Silicon.fr en direct sur les smartphones et tablettes