LIVRE BLANC

ACCÈS À DISTANCE ET BYOD, RENFORCER LA SÉCURITÉ DES NOMADES SANS CONTRAINTES

ATHENA Global Services

Expert en Sécurité Informatique
www.athena-gs.com

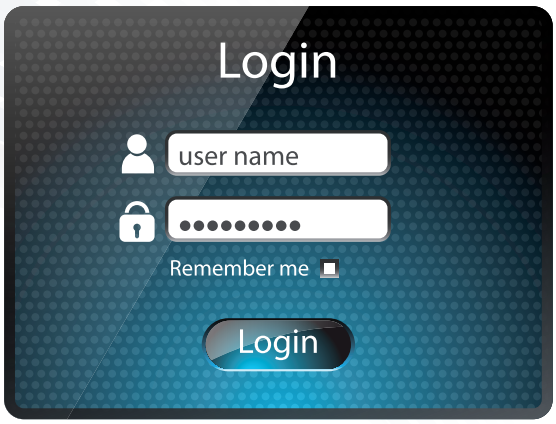
Imaginer un monde virtuel sans règles ni devoirs relève de l'inconscience. Sans pour autant tomber dans la cyber-paranoïa, l'ampleur du vol d'identités sur la toile devient inquiétante. Le dernier en date concerne Evernote®, un service de partage de documents dans le cloud, qui a été obligé de forcer la réinitialisation de 50 millions de mots de passe et de demander à ses utilisateurs de le changer. Or, même si l'usurpation d'identité constitue en France un délit[1] assorti d'une peine d'un an d'emprisonnement et de 15 000 € d'amende (à condition de porter plainte), le vol d'identité sur les réseaux sociaux dépasse le cadre des frontières.

>> Par Benjamin Malizia

En effet, d'un pays à l'autre le droit diffère parfois considérablement, que ce soit sur les aspects de la vie privée, de l'exploitation des données ou même dans la définition des infractions. Par conséquent, les organisations cybercriminelles profitent de ce manque d'homogénéité pour envoyer les attaques les plus importantes depuis les localisations où elles sont « légalement » protégées. Cette situation résulte notamment du fait que pendant de nombreuses années, les politiques menées par les états ont été pensées avec une vision territoriale limitée. Pourtant, dès son origine, que ce soit à des fins commerciales ou informatives, Internet s'imposait à l'échelle mondiale.

LES MOTS OU LES MAUX DE PASSE ?

A priori, les mots de passe pourraient constituer une protection contre le vol d'informations confidentielles, mais à la condition de choisir des chaînes de caractères complexes et de les renouveler souvent. Comme l'indique Pierre-Marc Bureau, chercheur chez ESET, « Les mots de passe c'est comme les brosses à dent… : ils sont personnels et il faut les changer régulièrement… ». Certes, mais encore faut-il les mémoriser en évitant les Postits accolés à l'écran, par exemple.



Le plus inquiétant, c'est que la confidentialité apportée par les mots de passe est considérée par les internautes comme efficace à presque 100 %[2]. Pourtant d'autres mécanismes d'authentification s'avèrent souvent indispensables pour des transactions sensibles, notamment pour permettre aux salariés d'une entreprise de pouvoir se connecter en tous lieux aux sites de sa maison mère.

A noter également l'importance de la gestion et du stockage des mots de passe coté serveur. Dans l'environnement Windows par exemple, les mécanismes d'authentification passent par l'annuaire Active Directory et l'on considère que le niveau de protection est correct, notamment avec Windows Server 2008. De plus, ces serveurs savent exploiter les systèmes d'authentifications dites fortes. Cette appellation signifie qu'au moins deux facteurs d'authentification sont employés pour contrôler l'accès au serveur : l'identifiant (login ou Pin code) et le mot passe à usage unique délivré à chaque tentative de connexion.

Si beaucoup de grandes entreprises ont optés pour des connexions privées (VPN SSL[3] assorties à des mécanismes d'authentification plus élaborés que les mots de passe, il n'en reste pas moins que la grande majorité des PME n'est pas protégée par ce type de solutions, pour des raisons de coût et de complexité.

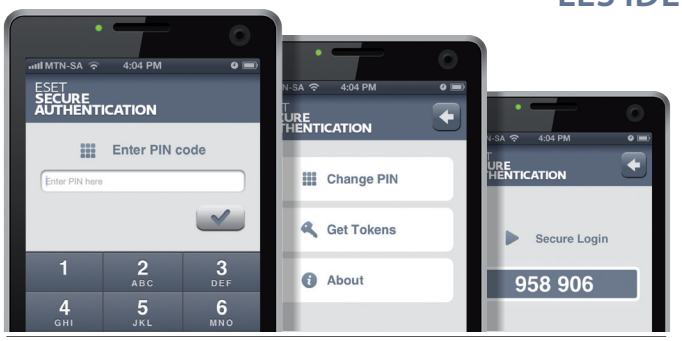
LES SYSTÈMES D'AUTHENTIFICATION

Pour sortir du piège de l'authentification limitée au seul mot de passe (authentification faible), de nombreuses solutions ont été élaborées par des éditeurs et fabricants de matériels en apportant un autre facteur d'identification (authentification forte) s'apparentant à une clé capable de générer des mots de passe aléatoires à chaque tentative de connexion.

Cette solution appelée multi-facteurs permet à l'utilisateur, qui dispose de ce dispositif, à travers un Token (gage d'authentification), une clé OTP (one-time password) ou un téléphone mobile, de s'affranchir de mémoriser un mot de passe. Dans le cas du téléphone mobile, deux possibilités existent : soit l'appareil est un smartphone capable de stocker une application générant des mots de passe, soit l'appareil reçoit un SMS comme identifiant.

Il existe également des solutions fondées sur la biométrie (authentification forte à trois facteurs via une empreinte digitale ou rétinienne) qui sont, certes, très efficaces, mais qui restent très coûteuses et peu adaptées à la mobilité. de ne pas le perdre, même si cela n'est pas exclu. Les solutions décrites plus loin, entrent dans cette catégorie.

COMMENT APPORTER UNE SOLUTION ACCESSIBLE AUX PME POUR CONTRÔLER EFFICACEMENT LES IDENTITÉS ?

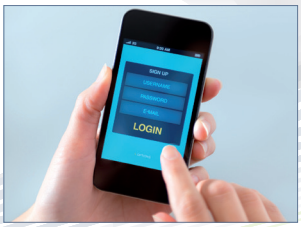


Source : ESET

Pour mettre en place une solution d'authentification multi-facteurs à un coût raisonnable pour les PME, il est préférable de passer par le téléphone mobile dans la mesure où chaque employé d'une entreprise en dispose tout naturellement.

L'usage des Token implique en effet que l'utilisateur conserve en permanence avec lui, une clé USB spécifique ou un dispositif à pile de la taille d'un porte-clés, qui peut plus facilement être égaré ou volé. Dans le cas du téléphone mobile en revanche, l'utilisateur prend généralement soin de ne pas le perdre, même si cela n'est pas exclu. Les solutions décrites plus loin, entrent dans cette catégorie.

L'AUTHENTIFICATION SÉCURISÉE À DEUX FACTEURS



ESET via les smartphones

ESET Secure Authentication est une solution permettant l'authentification à deux facteurs avec mot de passe à usage unique (2FA-OTP) lors de la connexion aux réseaux d'entreprise à travers le téléphone mobile des utilisateurs. Simple à mettre en œuvre, la solution ajoute une seconde couche de contrôle au processus d'authentification traditionnel composé de l'identifiant et du mot de passe.

ESET Secure Authentication fonctionne dans les environnements mobiles iPhone, Android, BlackBerry, Windows Phone 7 et 8, Windows Mobile et J2ME. La solution prend également en charge l'authentification via SMS et supporte ainsi les anciens téléphones mobiles qui ne pourraient exécuter l'application.

ESET Secure Authentication (ESA) est une offre originale destinée plus particulièrement aux PME(4) qui n'ont pas forcement les moyens d'investir dans du matériel coûteux et dans le déploiement d'une solution complexe en matière de contrôle d'identité.

La solution ESA prend acte du développement du télétravail et du BYOD (équipement personnel employé pour se raccorder au site de l'entreprise). Ainsi, en conjonction avec les solutions de sécurité d'ESET pour les smartphones, ESA apporte la couche indispensable de protection des accès aux réseaux d'entreprise.

La solution est bâtie sur un modèle client / serveur où l'application mobile génère les mots de passe à usage unique de façon aléatoire, tandis que le serveur d'authentification valide l'accès au réseau. L'utilisateur peut alors employer ce mot de passe unique pour s'authentifier sur le site de l'entreprise sur lequel il souhaite accéder. A travers cette authentification forte, l'utilisateur peut se connecter aux VPN d'entreprises via un serveur Radius ou à sa messagerie Outlook Web Access (OWA).

Cette solution est un complément essentiel à la protection de l'infrastructure et des données sensibles de chaque entreprise. Outre l'avantage de la facilité de déploiement et d'utilisation d'ESA, sa gestion et le support d'un grand nombre de plates-formes mobiles constituent un atout considérable pour les PME. Cette nouvelle solution d'authentification à deux facteurs s'accorde parfaitement avec les applications existantes telles que, Outlook Web Access/App et l'infrastructure VPN.

Conçue pour être très simple à installer, facile à configurer et à gérer, la solution proposée par défaut supporte les services et protocoles les plus largement utilisés. ESA offre une protection pour Outlook Web Access/App et RADIUS (serveur d'authentification) et supporte les environnements Windows Server (2003, 2003 R2, 2008, 2008 R2 et 2012) à travers l'Active Directory.

SMS PASSCODE

SMS PASSCODE® propose également un système d'authentification à deux facteurs, grâce au téléphone mobile personnel. Il permet de protéger les employés des entreprises lors de leur procédure d'identification et d'accès à des sites Intranet. À travers l'envoi d'un code envoyé par SMS sur le mobile de l'utilisateur, SMS PASSCODE® complète la procédure d'authentification initiée par l'identifiant et le mot de passe. Elle offre une solution complémentaire d'identification externe aux boîtiers spécialisés de sécurité tels que Citrix, Cisco, Microsoft, Juniper et autres protocoles IPsec et SSL VPN.

Cette seconde solution sera privilégiée lorsque les utilisateurs accèdent aux réseaux d'entreprise employant des passerelles Citrix et Cisco (serveur TACACS) notamment.

(1) https://www.internet-signalement.gouv.fr/
(2) http://blog.eset.com/2012/08/17/lists-of-bad-passwords-dont-miss-the-point
(3) VPN SSL : réseau privé virtuel avec connexion cryptée
(4) Entreprises de moins de 1000 personnes