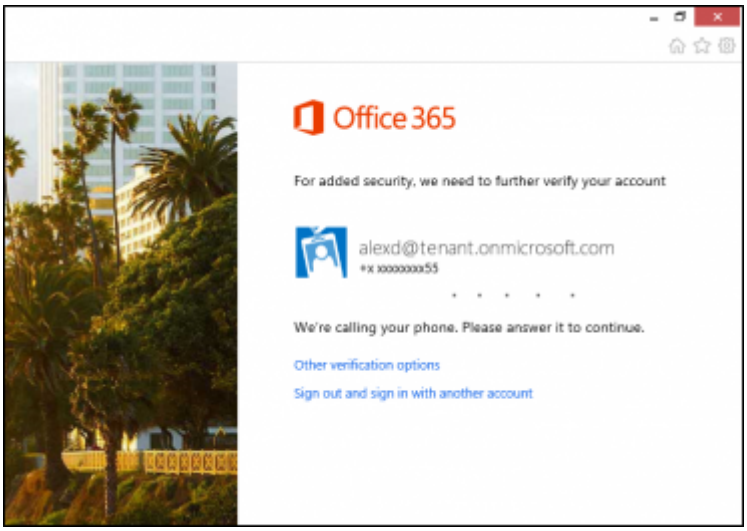
Cloud : Microsoft adopte l'authentification forte pour Office 365

Face à la montée des menaces de sécurité et aux interrogations des DSI quant à la sécurité des services du Cloud, Microsoft adopte **l'authentification à double facteur** pour sa solution de bureautique en mode Saas, Office 365. Cette annonce couvre toutes les applications bureautiques ainsi que Exchange Online et SharePoint Online.



L'éditeur exploite en réalité les technologies héritées du rachat de PhoneFactor pour adjoindre au couple identifiant / mot de passe une couche de protection supplémentaire, sans passer par l'emploi de jeton. Un téléphone suffit en l'occurrence à l'utilisateur (employé, client ou prospect), qui dispose de **trois possibilités pour finaliser le processus d'identification**.

Premier choix, recevoir un **code secret communiqué par SMS**. Autre méthode, **déclencher automatiquement un appel** (sur un fixe ou un portable) et presser la touche dièse (#) en réponse. Ou encore valider la connexion directement **via une application mobile** et bénéficier ainsi d'un accès sécurisé – y compris en environnement Active Directory – aux diverses briques d'Office 365. Chacun de ces processus de connexion présente l'avantage d'impliquer un facteur physique – en l'occurrence un téléphone – plus difficile à pirater qu'un vérificateur logiciel comme un clavier virtuel.

Pallier la faiblesse des mots de passe

Accessible sans surcoût au contraire de la fonction Active Authentication liée à la plate-forme Azure, l'authentification forte était déjà disponible dans Office 365, mais uniquement pour les administrateurs. Elle n'est **pas encore active dans les applications desktop** de la suite bureautique : en 2014, Microsoft permettra aux clients Office 365 d'utiliser l'authentification à double facteur directement depuis ces applications clientes. En attendant cette implémentation, Microsoft recommande d'utiliser le service App Passwords, qui génère des mots de passe aléatoires de 16 caractères. Les prochaines mises à jour introduiront aussi le support des certificats électroniques et des cartes magnétiques (SmartCards).

Alors que la fragilité des mots de passe devient un écueil majeur dans l'univers de la sécurité informatique – comme l'a récemment montré « l'affaire Adobe », l'adoption de l'authentification forte s'accélère. En ligne de mire, des systèmes évolués exploitant des tatouages, des puces RFID,

de la reconnaissance faciale ou encore de l'identification rétinienne.

Certaines entreprises IT comme Twitter ont **développé leur propre solution**, souvent basée sur des clés d'identification cryptées stockées à même le terminal de l'utilisateur. Google pense plutôt à introduire une dimension essentiellement physique avec la clé USB YubiKey. En toile de fond, le comportement des cybercriminels évolue : les techniques d'interception de type « Man-in-the-Middle » conçues pour déjouer l'authentification forte se multiplient.

En complément :

– Avec Power BI, Microsoft Office 365 s'essaie au Big Data

– La toute jeune DSI groupe de Limagrain choisit Office 365 pour se roder

– Un contrat géant pour Microsoft Office 365… et pour les Google Apps