Internet : MÃ©dias sociaux : 3 menaces pÃ¨sent sur les entreprises
Internet
PostÃ© par : JulieM
PubliÃ©e le : 20/3/2012 13:30:00

Bien que la majoritÃ© des responsables de la sÃ©curitÃ© des entreprises connaissent parfaitement les principaux risques associÃ©s aux mÃ©dias sociaux, dâautres risques moins connus peuvent sâavÃ©rer plus dangereux encore.

Trois moyens permettent aux programmes et aux codes malveillants de se faufiler Ã travers les pare-feux dâune entreprise via les mÃ©dias sociaux.

Il est heureusement possible de prÃ©venir toute utilisation Ã mauvais escient de ces moyens en prenant les prÃ©cautions qui sâimposent. Le principal problÃ¨me est que la plupart des dirigeants dâentreprise ignorent ce qui transite rÃ©ellement sur leurs rÃ©seaux et ne disposent pas dâune visibilitÃ© globale des caractÃ©ristiques du trafic ni des attaques potentielles.

Le protocole HTTPS nâest pas aussi sÃ©curisÃ© quâon pourrait le penser.

Le protocole SSL/TLS est le protocole de chiffrement le plus largement utilisÃ© dans les applications Web modernes - des sites de mÃ©dias sociaux (comme Twitter ou Facebook), aux messageries Web (comme Gmail), en passant par les services de synchronisation vers un cloud (comme Dropbox). La plupart du temps, ce protocole protÃ¨ge efficacement la confidentialitÃ© de lâutilisateur.

Toutefois, si vous utilisez le rÃ©seau dâune entreprise ou que vous vous connectez via un VPN, ces connexions chiffrÃ©es peuvent Ã©galement constituer une menace pour vous (et pour votre entreprise). Cela sâexplique par le fait que le tunnel chiffrÃ© entre vous et le serveur masque le trafic rÃ©seau, mais ne vous protÃ¨ge pas contre les menaces provenant du site auquel vous Ãªtes dÃ©jÃ connectÃ©. Ainsi, mÃªme si les pirates informatiques ne peuvent pas voir le trafic Web que vous envoyez vers les serveurs dâun rÃ©seau social, ils peuvent vous attaquer directement sur le site en utilisant le clickjacking (ou dÃ©tournement de clic) et dâautres attaques couramment utilisÃ©es sur les rÃ©seaux sociaux.

Sur le plan informatique, le problÃ¨me est que si vous ne pouvez pas voir le trafic chiffrÃ©, vous ne pouvez pas totalement protÃ©ger les utilisateurs en ligne. Heureusement, les entreprises spÃ©cialisÃ©es dans la sÃ©curitÃ© des rÃ©seaux connaissent cette faille et prÃ©voient deux cas de figure dans le futur : soit les entreprises de sÃ©curitÃ© sauront dÃ©chiffrer le trafic SSL, soit elles sâÃ©quiperont des fonctionnalitÃ©s indispensables qui le permettent.

Les terminaux mobiles constitueraient la plus grosse faille

Il y a quelques annÃ©es, le moindre soupÃ§on de programme malveillant mobile faisait les gros titres des journaux mondiaux. En 2011, ce type de programme malveillant est passÃ© du statut de Â« preuve de concept Â» Ã celui de Â« menace rÃ©elle Â». En 2012, la situation ne devrait pas sâ□□amÃ©liorer puisque lâ□□on prÃ©voit une augmentation des banniÃ¨res publicitaires malveillantes et des rÃ©seaux de zombies sur les terminaux mobiles.

Toutefois, la plus forte menace provient des applications mobiles elles-mÃªmes, puisquâ□□elles sont peu nombreuses Ã fournir une protection adÃ©quate des informations dâ□□authentification. Sur le plan de la sÃ©curitÃ©, une application mobile compromise nâ□□est pas Â« moins pire Â» quâ□□un ordinateur de bureau compromis ou un rÃ©seau compromis. Si votre nom dâ□□utilisateur et votre mot de passe dâ□□accÃ¨s Ã une application Web sont compromis sur votre terminal mobile, les auteurs de cet acte malveillant peuvent utiliser vos comptes Ã des fins illicites. Y compris les comptes que vous utilisez au travail. Nâ□□oubliez pas non plus que si votre terminal mobile est connectÃ© au rÃ©seau Wi-Fi de lâ□□entreprise, toutes les applications prÃ©sentes sur ce terminal fonctionnent Ã©galement sur le rÃ©seau de lâ□□entreprise. MÃªme en lâ□□absence d'une politique BYOD (Bring Your Own Device) formelle, nâ□□importe qui dans lâ□□entreprise connaissant le mot de passe Wi-Fi dâ□□accÃ¨s au rÃ©seau peut potentiellement connecter son terminal personnel Ã votre rÃ©seau.

Extensions de navigateurs et applications tierces suspectes

Tout ce qui a Ã©tÃ© dit concernant les applications mobiles sâ□□applique doublement aux applications tierces, aux extensions de navigateurs et aux scripts de sites tels que Facebook, Google+ et dâ□□autres plateformes qui sâ□□intÃ¨grent aux applications Web de confiance. Les conseils de protection contre les menaces associÃ©es aux applications Web - avoir une meilleure visibilitÃ© du trafic rÃ©seau, sâ□□assurer que le systÃ¨me de sÃ©curitÃ© peut identifier les activitÃ©s malveillantes mÃªme lorsquâ□□elles sont chiffrÃ©es et dÃ©finir de bonnes pratiques dâ□□utilisation pour les utilisateurs - sâ□□appliquent Ã©galement aux extensions de navigateurs et aux applications tierces.

La meilleure dÃ©fense ?

Les menaces qui pÃ¨sent sur lâ□□entreprise et sur les employÃ©s sont donc diverses et variÃ©es. MÃªme sâ□□il nâ□□existe pas de solution unique pour Ã©liminer toutes ces menaces, lâ□□Ã©ducation des utilisateurs et la mise en Å□uvre de bonnes pratiques informatiques peuvent vÃ©ritablement les diminuer. Aussi, il est important de noter que lâ□□accÃ¨s Ã ces applications Web sociales sur le rÃ©seau reste bÃ©nÃ©fique pour lâ□□entreprise dans son ensemble, puisquâ□□il permet dâ□□amÃ©liorer la productivitÃ© et la collaboration, et contribue globalement au bon moral des employÃ©s. Les sociÃ©tÃ©s informatiques doivent aider les entreprises Ã se tenir informÃ©es des changements et des besoins en matiÃ¨re de sÃ©curitÃ© de leurs employÃ©s qui accÃ¨dent au Web social.

Vient de nous confier **RenÃ© Bonvani**, Chief Marketing Officer de **Palo Alto Networks**