SÃ©curitÃ© : 125 millions d'heures perdues en PME pour mauvais MDP
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 30/3/2011 11:00:00

Selon une nouvelle Ã©tude rÃ©alisÃ©e par **YouGov pour Symantec**, les entreprises franÃ§aises perdent chaque annÃ©e plus de**125** millions d'heures de productivitÃ© en raison des problÃ¨mes de gestion des mots de passe et d'accÃ¨s Ã leurs systÃ¨mes informatiques auxquels sont confrontÃ©s leurs salariÃ©s.

Un certain nombre de facteurs contribuent Ã cette perte de temps significative, notamment la nÃ©cessitÃ© pour les salariÃ©s de crÃ©er et mÃ©moriser des mots de passe, de gÃ©rer des problÃ¨mes dâaccÃ¨s et de redÃ©finir des mots de passe. En raison de ces problÃ¨mes de mots de passe, les entreprises franÃ§aises perdent du temps et de l'argent inutilement, puisque des technologies permettent de donner accÃ¨s aux comptes et applications en ligne de maniÃ¨re fiable, pratique et rapide.

L'Ã©tude a Ã©galement abouti aux conclusions suivantes :

â¢ Les internautes franÃ§ais doivent collectivement mÃ©moriser plus de 185,2 millions de mots de passe pour accÃ©der Ã leurs comptes en ligne chaque jour et il est demandÃ© Ã chacun de saisir en moyenne cinq mots de passe (4,94) par jour.

â¢ Plus de la moitiÃ© (52 %) des internautes franÃ§ais dÃ©clare utiliser le mÃªme mot de passe pour au moins la moitiÃ© de leurs comptes en ligne. Cette pratique courante, mais dangereuse, expose les salariÃ©s et leurs employeurs aux cybercriminels qui, capables de dÃ©chiffrer ne serait-ce qu'un mot de passe, peuvent dÃ©verrouiller plusieurs services en ligne et accÃ©der Ã une multitude de donnÃ©es personnelles et professionnelles.

â¢ 45 % des internautes franÃ§ais sÃ©curisent leurs comptes avec des mots de passe faciles Ã deviner ou identifiables avec des informations disponibles sur des rÃ©seaux sociaux.

â¢ Ces mots de passe faciles Ã deviner contiennent, par exemple, le nom de l'animal (13 %), le

nom du partenaire (7 %), la date de naissance (6 %) ou le nom de jeune fille de la mÃ¨re des utilisateurs (5 %).

â□¢ Seulement un cinquiÃ¨me (21 %) font l'effort de crÃ©er des mots de passe forts, comprenant des sÃ©quences alÃ©atoires de lettres et de chiffres.

â□¢ Les autres mots de passe courants, faciles Ã deviner, contiennent :

â□¢ Le mot Â« motdepasse Â» suivi d'un chiffre, par exemple Motdepasse1, Motdepasse1234 (17 %),

â□¢ Une sÃ©quence numÃ©rique, par exemple 12345, 56789 (9 %),

â□¢ Le nom de la ville ou de la rue de l'utilisateur (4 %),

â□¢ Des chiffres rÃ©pÃ©tÃ©s, par exemple 0000, 5555 (3 %).

Recommandations :

Aux entreprises qui souhaitent amÃ©liorer lâ□□utilisation et la gestion des mots de passe permettant lâ□□accÃ¨s Ã leurs systÃ¨mes dâ□□informations, Symantec recommande de :

1. Mettre en place un systÃ¨me d'authentification forte, Ã l'Ã©chelle de lâ□□ensemble de l'entreprise, et non pour certaines applications uniquement. Ce systÃ¨me devra intÃ©grer des applications pour les terminaux mobiles et sâ□□inscrire dans leur politique de sÃ©curitÃ© et leurs contraintes budgÃ©taires. SÃ©curiser les accÃ¨s aux systÃ¨mes externes, tels que les plates-formes SaaS et de partenaires, en assurant un niveau de sÃ©curitÃ© Ã©quivalent Ã celui des accÃ¨s aux systÃ¨mes internes.

2. Appliquer l'authentification forte aux environnements d'entreprise ouverts pour Ã©tendre la sÃ©curitÃ© au cloud computing, aux outils de collaboration et Ã l'accÃ¨s mobile.

3. Communiquer au personnel les rÃ¨gles et les pratiques associÃ©es, puis renforcer cette communication avec des programmes de formation.

4. Imposer au personnel l'utilisation de mots de passe forts : les mots de passe doivent contenir au moins huit caractÃ¨res et combiner des caractÃ¨res alphanumÃ©riques et spÃ©ciaux. Plusieurs mots de passe sont nÃ©cessaires et il est important que les salariÃ©s les modifient

rÃ©guliÃ¨rement.

Citation :

Danilo Labovic, Directeur EMEA de la division Verisign de Symantec confirme: Â« *Il est aujourd'hui plus important que jamais de protÃ©ger les informations rÃ©sidant sur les rÃ©seaux d'entreprise. Les mots de passe faibles exposent les entreprises Ã de nombreux risques, tels que la fuite de donnÃ©es, le vol de secrets professionnels, la fraude financiÃ¨re et l'usurpation d'identitÃ©, tandis que les problÃ¨mes de gestion des mots de passe leur coÃ»tent de l'argent qui pourrait Ãªtre naturellement mieux utilisÃ©. Dans le mÃªme temps, l'utilisation croissante d'appareils personnels pour accÃ©der aux applications professionnelles (et vice versa) augmente les risques des entreprises. Le fait que plus de la moitiÃ© des internautes franÃ§ais utilisent le mÃªme mot de passe pour plusieurs comptes signifie que des salariÃ©s simplifient la tÃ¢che des cybercriminels. Il est en effet de plus en plus facile pour les cybercriminels avertis de dÃ©chiffrer des combinaisons et informations d'accÃ¨s simples.* Â»