LastPass : 4 conseils au PME, Se protÃ©ger des piratages
Internet
PostÃ© par : JulieM
PubliÃ©e le : 26/1/2018 13:00:00

Face Ã l'interminable succession de piratages notoires, la sÃ©curitÃ© des entreprises revÃªt dÃ©sormais une importance sans prÃ©cÃ©dent. Cependant, selon la toute derniÃ¨re enquÃªte Global State of Information Security Survey, les dÃ©penses consenties sur ce plan ont diminuÃ© d'un tiers au cours des 12 derniers mois, en particulier dans les TPE et PME.

MalgrÃ© la menace, les PME commettent encore l'erreur d'estimer que leurs donnÃ©es n'intÃ©ressent pas les hackers parce qu'elles ne sont que de petites ou moyennes structures. Cette absence d'investissement est souvent Ã l'origine de stratÃ©gies de sÃ©curitÃ© laxistes, les utilisateurs en profitant pour recourir Ã des pratiques manuelles, comme le fait de regrouper leurs mots de passe dans des tableurs.

Â

Â

La culture du BYOD et du travail Ã distance complique encore la tÃ¢che pour les entreprises ne disposant pas des technologies adÃ©quates pour obtenir une visibilitÃ© globale de leur sÃ©curitÃ©.Â

Dans de nombreux cas, les salariÃ©s deviennent alors la premiÃ¨re ligne de dÃ©fense contre les menaces externes ciblant les donnÃ©es professionnelles.

Ainsi, selon une enquÃªte publiÃ©e rÃ©cemment par LastPass et Ovum, plus de la moitiÃ© des responsables informatiques s'attendent Ã ce que les employÃ©s adoptent d'eux-mÃªmes les bons comportements vis-Ã -vis de leurs mots de passe, ce qui constitue en soi un risque pour leur entreprise.Â

Bien qu'il soit important que ces derniers soient sensibilisÃ©s et maÃ®trisent les meilleures pratiques en la matiÃ¨re, il n'en est pas moins essentiel pour les Ã©quipes informatiques d'investir suffisamment de temps et de ressources pour contrÃ´ler la sÃ©curitÃ© de leur organisation.

Voici donc 4 mesures qui permettront aux entreprises de revoir leurs stratÃ©gies de sÃ©curitÃ© pour 2018 :

Reprendre la main sur la gestion des mots de passe

Cela peut paraÃ®tre Ã©vident comme point de dÃ©part, mais beaucoup d'entreprises peinent Ã faire face aux lacunes de sÃ©curitÃ© de leur entreprise bien qu'elles en soient conscientes.

Ainsi, en matiÃ¨re de gestion de mots de passe, beaucoup de services informatiques auront tendance Ã nier leur responsabilitÃ©, considÃ©rant que les employÃ©s les choisissent eux-mÃªmes, et que c'est donc Ã eux qu'il revient de les gÃ©rer et d'en assurer le contrÃ´le.

Cependant, selon le rapport d'investigation de Verizon sur les fuites de donnÃ©es, plus de 80 % des failles sont la consÃ©quence de mots de passe faibles, compromis, ou rÃ©utilisÃ©s. Cette approche n'a donc rien d'infaillible.Â

En outre, une enquÃªte publiÃ©e rÃ©cemment a rÃ©vÃ©lÃ© que plus de trois quarts des employÃ©s auraient des problÃ¨mes relatifs Ã l'utilisation ou Ã la gestion de leurs mots de passe au moins une fois par mois, bon nombre d'entre eux estimant ne pas avoir l'assistance nÃ©cessaire.Â

Il est clairement temps pour les Ã©quipes informatiques de se rendre Ã l'Ã©vidence et de reprendre le contrÃ´le de la gestion des mots de passe des utilisateurs.

Adopter une vision Ã 360Â°

Les entreprises doivent comprendre que les frontiÃ¨res entre le monde professionnel et personnel sont de plus en plus floues, et que ce phÃ©nomÃ¨ne s'Ã©tend Ã©galement Ã la sÃ©curitÃ©.Â

Avec la popularitÃ© croissante du BYOD et du travail Ã distance, les Ã©quipes informatiques se doivent de reconnaÃ®tre l'Ã©mergence de mÃ©thodes de travail modernes, et d'adapter leurs stratÃ©gies et approches en fonction de ces pratiques.

Il faudra notamment Ã©tendre leur supervision au-delÃ des identifiants et mots de passe professionnels des employÃ©s. Il suffit de prendre l'exemple de la faille de Yahoo (3 millions de mots de passe dÃ©robÃ©s) pour comprendre que les pirates disposent d'une multitude de points d'entrÃ©e afin d'accÃ©der Ã des donnÃ©es professionnelles.

Par exemple, si un employÃ© vÃ©rifie ses e-mails personnels et professionnels et clique sur un lien contenant un malware, l'ensemble du rÃ©seau d'entreprise devient potentiellement vulnÃ©rable.Â

Plus vite les Ã©quipes informatiques comprendront qu'elles ont besoin d'une vision Ã 360 degrÃ©s de la sÃ©curitÃ© des utilisateurs, mieux ce sera pour la capacitÃ© de leurs systÃ¨mes de dÃ©fense Ã rÃ©sister aux agressions.

Sensibiliser les employÃ©s

La sÃ©curitÃ© d'une entreprise passe Ã©galement par le fait de sensibiliser les employÃ©s aux meilleures pratiques. Surtout, il est essentiel de leur faire comprendre l'importance d'utiliser des mots de passe complexes et uniques sur l'ensemble de leurs comptes, les risques des rÃ©seaux publics, et les ressources auxquelles ils devraient ou ne devraient pas accÃ©der sur de tels rÃ©seaux.

Les entreprises doivent donc dÃ©finir des stratÃ©gies de sÃ©curitÃ© et s'assurer de sensibiliser rÃ©guliÃ¨rement aussi bien les utilisateurs existants que les nouvelles recrues. Pour cela, elles peuvent recourir Ã la ludification afin d'aider les employÃ©s Ã prendre de bonnes habitudes.

Faire de la sÃ©curitÃ© un jeu permet Ã©galement de mieux comprendre la place du facteur humain. Les salariÃ©s pourraient ainsi Ãªtre Ã©valuÃ©s sur le niveau de sÃ»retÃ© de leurs mots

de passe, et celui qui obtiendrait le meilleur score recevrait un prix.

Investir dans les nouvelles technologies et s'assurer qu'elles soient Ã jour

Enfin, Ã l'approche de la nouvelle annÃ©e, il n'est plus acceptable de gÃ©rer manuellement la sÃ©curitÃ© de son entreprise. Noter les mots de passe des employÃ©s dans une feuille de calcul sur Excel, ou Ã©crire des numÃ©ros de cartes de crÃ©dit sur des feuilles de papier ne sont pas des mÃ©thodes acceptables.

IndÃ©pendamment de leur taille, les entreprises doivent investir dans des technologies leur permettant de gÃ©rer leurs donnÃ©es confidentielles en toute sÃ©curitÃ©, et activer l'authentification multifacteur sur l'ensemble de leurs comptes (donnÃ©es biomÃ©triques, mots de passe Ã usage unique etc.).

Thierry Behaghel, SpÃ©cialiste produit EMEA chez LastPass