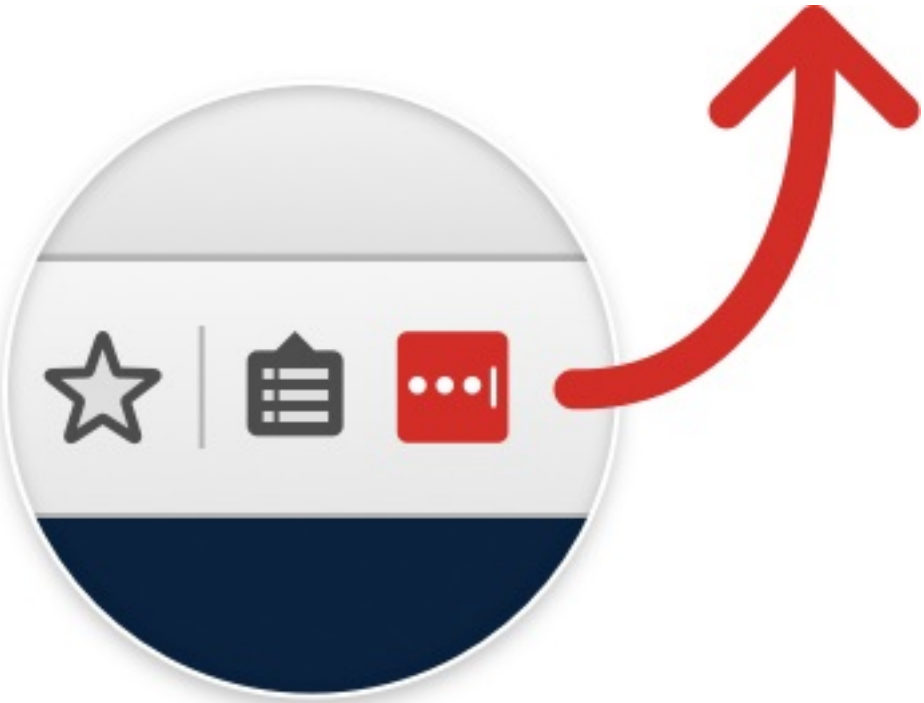
3 rÃ¨gles pour renforcer la sÃ©curitÃ© des entreprises
Internet
PostÃ© par : JulieM
PubliÃ©e le : 11/1/2018 14:30:00

Cette annÃ©e a Ã©tÃ© marquÃ©e par un grand nombre d'incidents majeurs de sÃ©curitÃ©, du piratage d'Uber (qui a affectÃ© 57 millions de personnes dans le monde entier) Ã l'affaire des ministres britanniques partageant leurs mots de passe et l'accÃ¨s Ã leurs ordinateurs avec n'importe quel collaborateur travaillant dans leur bureau.

Bien que la sÃ©curitÃ© des entreprises n'ait jamais Ã©tÃ© un paramÃ¨tre aussi important qu'aujourd'hui, nombre d'entre elles continuent de laisser leurs donnÃ©es Ã la merci d'individus malintentionnÃ©s.



Une enquÃªte publique portant sur les failles de cybersÃ©curitÃ© a rÃ©vÃ©lÃ© que la plupart des sociÃ©tÃ©s britanniques Ã©taient vulnÃ©rables, quelle que soit leur taille.

Les dirigeants choisissant de se cacher dans la masse en croyant ne pas reprÃ©senter une cible convoitÃ©e des pirates sont dans l'erreur et courent un risque rÃ©el.

Beaucoup d'entreprises s'appuient encore sur des processus manuels et sur la bonne volontÃ© de leurs employÃ©s pour assurer leur premier niveau de sÃ©curitÃ©.

Ainsi, bien que les failles soient trÃ¨s souvent la consÃ©quence de mots de passe faibles, compromis ou rÃ©utilisÃ©s, une enquÃªte rÃ©cemment publiÃ©e a montrÃ© que plus de la moitiÃ© des responsables informatiques interrogÃ©s faisaient encore confiance Ã leurs salariÃ©s pour appliquer les meilleures pratiques en la matiÃ¨re.

La mÃªme enquÃªte a Ã©galement rÃ©vÃ©lÃ© que plus de 75 % des employÃ©s rencontraient des problÃ¨mes pour utiliser leurs mots de passe au moins une fois par mois.

Pire, nombre d'entre eux ne bÃ©nÃ©ficient pas de l'aide dont ils ont besoin pour rÃ©gler ces problÃ¨mes.

Les mots de passe Ã©tant souvent le principal point d'accÃ¨s aux comptes professionnels, il est donc Ã©vident qu'une grande quantitÃ© d'entreprises s'exposent Ã des menaces importantes et ne forment pas leur personnel comme il se doit.

En rÃ©sumÃ©, afin d'assurer leur sÃ©curitÃ©, les organisations doivent trouver le bon Ã©quilibre entre commoditÃ© et bouleversement des processus. En effet, lorsqu'une solution n'est pas pratique, les employÃ©s ont davantage tendance Ã essayer de contourner le processus, ce qui peut avoir de lourdes consÃ©quences.

De mÃªme, les Ã©quipes informatiques peuvent Ãªtre rÃ©ticentes Ã l'idÃ©e d'adopter des technologies ajoutant un processus supplÃ©mentaire jugÃ© superflu par de nombreux collaborateurs.

La bonne nouvelle, c'est qu'il existe un certain nombre de solutions permettant aux entreprises et services informatiques de reprendre le contrÃ´le de leur sÃ©curitÃ©. En voici 3 :

Adopter une vue Ã 360 degrÃ©s

En cas de faille de sÃ©curitÃ©, on a souvent tendance Ã considÃ©rer que les employÃ©s sont seuls responsables. Pourtant, bien que l'Homme soit une composante importante de tout systÃ¨me de sÃ©curitÃ©, adopter une vision Ã 360 degrÃ©s nÃ©cessite de reconnaÃ®tre Ã©galement le rÃ´le des technologies.

Les Ã©quipes informatiques doivent prendre conscience de la nature changeante des mÃ©thodes de travail modernes. En effet, la frontiÃ¨re entre professionnel et personnel est de plus en plus floue, ce qui a un impact sur la sÃ©curitÃ©. Il est donc important de mettre en Å□uvre les stratÃ©gies et outils nÃ©cessaires pour s'adapter Ã ce type de comportements.

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

Il suffit de prendre l'exemple du piratage de Yahoo pour comprendre Ã quel point la menace est rÃ©elle : les 3 milliards de mots de passe dÃ©robÃ©s ont ouvert de nombreuses portes aux pirates, leur permettant ainsi d'accÃ©der Ã des donnÃ©es professionnelles.

Plus vite les entreprises parviendront Ã dÃ©velopper une vision globale de leur sÃ©curitÃ©, plus leurs systÃ¨mes de dÃ©fense seront Ã mÃªme de rÃ©sister.

Investir dans les technologies adaptÃ©es Ã son entreprise

Les technologies ont progressÃ© Ã un rythme fulgurant ces derniÃ¨res annÃ©es. Pourtant, en matiÃ¨re de sÃ©curitÃ©, beaucoup d'entreprises n'ont toujours pas mis en place les outils leur permettant de se tenir Ã l'abri de faÃ§on simple et pratique.

Conserver des numÃ©ros de cartes de crÃ©dit professionnelles et des mots de passe dans un document Excel auquel n'importe quel employÃ© peut accÃ©der augmentera Ã coup sÃ»r le niveau de risque de l'organisation. Les Ã©quipes informatiques doivent Ã©valuer les pratiques et outils en place, et comprendre comment elles peuvent renforcer leurs systÃ¨mes de dÃ©fense.

Les besoins varieront en fonction des organisations -nul besoin d'une sÃ©curitÃ© de niveau gouvernemental pour une simple affaire familiale. Cependant, certaines bases valent pour tous. Par exemple, l'utilisation d'un gestionnaire tel que LastPass, qui permet de crÃ©er et de stocker des

mots de passe forts pour chaque identifiant.

Les employÃ©s peuvent Ã©galement partager ces Ã©lÃ©ments en toute sÃ©curitÃ© sans compromettre des donnÃ©es confidentielles, ce qui peut Ãªtre utile au sein d'un mÃªme dÃ©partement, ou pour les individus ayant besoin d'accÃ©der Ã une variÃ©tÃ© d'outils professionnels.

En outre, il est nÃ©cessaire de mettre en Å□uvre une solution d'authentification multifactorielle pour l'ensemble des comptes, et des prÃ©cautions doivent Ã©galement Ãªtre prises au cas oÃ¹ un salariÃ© ayant accÃ¨s Ã des donnÃ©es sensibles venait Ã quitter l'entreprise.

Enfin, il est recommandÃ© d'Ã©valuer rÃ©guliÃ¨rement les technologies en place afin de s'assurer qu'elles soient Ã jour et encore adaptÃ©es.

Sensibiliser encore et toujours

Le contrÃ´le de la sÃ©curitÃ© d'une entreprise ne s'effectue pas que sur le plan technologique. Les Ã©quipes informatiques doivent prendre le temps de sensibiliser les employÃ©s aux meilleures pratiques, et s'assurer de les leur rappeler rÃ©guliÃ¨rement.

Toutes les bases doivent Ãªtre couvertes, y compris l'importance d'utiliser des mots de passe complexes et uniques, ainsi que les risques liÃ©s au BYOD et au fait d'accÃ©der Ã des comptes professionnels sur des rÃ©seaux publics. IdÃ©alement, mieux vaut Ã©tablir une stratÃ©gie claire et concise.

En effet, plus les conseils et recommandations en matiÃ¨re de sÃ©curitÃ© sont longs et techniques, plus les employÃ©s peinent Ã les comprendre et les suivre. Faire de tout cela un jeu ou une compÃ©tition est une excellente mÃ©thode pour stimuler leur engagement, par exemple en rÃ©compensant ceux qui utilisent des mots de passe forts.

Mieux ils comprendront la nÃ©cessitÃ© de rester en sÃ©curitÃ©, plus ils auront tendance Ã adopter de nouvelles pratiques et technologies afin de protÃ©ger autant que possible leurs comptes et donnÃ©es professionnels.

Steve Schult, directeur sÃ©nior, gestion des produits, ***LastPass***