Quest Software : Les pertes de donnÃ©es coÃ»tent chÃ¨res aux PME.
Internet
PostÃ© par : JerryG
PubliÃ©e le : 13/12/2012 14:00:00

L'utilisation d'appareils grand public sur le lieu de travail, les Ã©quipesÂ gÃ©ographiquement dispersÃ©es et la frÃ©quence des rÃ©seaux sociaux ont un impactÂ considÃ©rable sur les modalitÃ©s de partage des informations des entreprises, ceÂ qui pose de **graves problÃ¨mes en ce qui concerne la sÃ©curitÃ© des donnÃ©es.**

Selon une enquÃªte rÃ©alisÃ©e par Vanson Bourne auprÃ¨s de DSI en Allemagne, en France et au Royaume-Uni pour Quest Software, filiale de Dell, les politiques actuelles de sÃ©curitÃ© de l'information ne protÃ¨gent pas les informations critiques. Cette dÃ©faillance est due au fait que les processus de gestion des identitÃ©s et des accÃ¨s n'ont pas Ã©tÃ© mis Ã jour pour reflÃ©ter l'Ã©volution des besoins des employÃ©s, ce qui met en danger les entreprises.

En outre, selon les rÃ©sultats de l'enquÃªte, 65 % des DSI europÃ©ens pensent que les employÃ©s partagent les donnÃ©es de l'entreprise de la maniÃ¨re la plus simple et la plus rapide qui soit : ils contournent rÃ©guliÃ¨rement la politique de l'entreprise et ne se sentent pas vraiment concernÃ©s par la protection de ses informations critiques. 69 % pensent Ã©galement que les entreprises et les employÃ©s doivent engager davantage leur responsabilitÃ© en ce qui concerne les mÃ©thodes de partage, de stockage et de gestion des informations.

Compte tenu de l'impact potentiel important de la perte de donnÃ©es sur la sÃ©curitÃ©, la situation financiÃ¨re et la rÃ©putation des entreprises, la gestion des identitÃ©s et des accÃ¨s sera une prioritÃ© pour plus de trois quarts (76 %) des entreprises europÃ©ennes en 2013.

Â **Quest recommande des mesures fondÃ©es sur les meilleures pratiques pour traiter les problÃ©matiques de sÃ©curitÃ© suivantes :**

â¢ Augmentation des problÃ¨mes de sÃ©curitÃ©

Les DSI europÃ©ens dÃ©clarent que les informations sur le personnel (42 %), les clients (33 %) et RH (31 %) figurent parmi les donnÃ©es les plus partagÃ©es sur les rÃ©seaux sociaux et les sites Web tiers. Au cours des 18 derniers mois, les informations RH (30 %), clients (25 %) et financiÃ¨res

(23 %) ont Ã©tÃ© exposÃ©es Ã des problÃ¨mes de sÃ©curitÃ© Ã l'extÃ©rieur de l'entreprise, en raison d'une mauvaise gestion des identitÃ©s et des accÃ¨s. Parmi les entreprises qui en ont Ã©tÃ© victimes, 33 % dÃ©clarent avoir perdu la confiance des clients et 32 % estiment que leur rÃ©putation a Ã©tÃ© entachÃ©e.

â¢ Baisse de la productivitÃ©

98 % des DSI pensent Ã©galement qu'une mauvaise gestion des identitÃ©s et des accÃ¨s conduit les employÃ©s Ã utiliser des sites tiers comme solution de contournement pour le stockage et le partage d'informations, ce qui nuit Ã la collaboration et Ã la productivitÃ©. 31 % des DSI ont dÃ©clarÃ© qu'au cours des 18 derniers mois, des employÃ©s ont Ã©tÃ© bloquÃ©s pendant de longues pÃ©riodes faute de pouvoir accÃ©der aux informations nÃ©cessaires pour travailler.

â¢ SÃ©curisation des systÃ¨mes

Au cours des 12 derniers mois, 62 % des DSI ont subi des pressions visant la protection des donnÃ©es de leur entreprise en raison du nombre croissant de pertes de donnÃ©es d'entreprise relayÃ©es par les mÃ©dias. Ces pressions proviennent principalement des Ã©quipes juridiques internes (41 %), des directions gÃ©nÃ©rales (40 %) et des organismes de rÃ©glementation (33 %).

Recommandations

Des solutions telles que les solutions de gestion des identitÃ©s Quest One offrent un ensemble complet de fonctionnalitÃ©s, fournissant des mÃ©canismes de contrÃ´le exhaustifs dans une architecture flexible et modulaire. Celle-ci permet de traiter toutes les problÃ©matiques de sÃ©curitÃ© et d'Ã©liminer les risques inhÃ©rents aux mauvaises mÃ©thodes de gestion des identitÃ©s et des accÃ¨s. En appliquant les bonnes pratiques suivantes, les DSI seront plus sereins :

â¢ Mettre l'accent sur la formation : la prÃ©vention et la neutralisation de la majoritÃ© des menaces actuelles pesant sur la sÃ©curitÃ© de l'information passent par la formation, la diligence et des processus reposant sur des technologies appropriÃ©es, le cas Ã©chÃ©ant, qui appliquent des mots de passes Ã©laborÃ©s (modifiÃ©s rÃ©guliÃ¨rement).

â¢ Adopter le principe du privilÃ¨ge minimal : accorder Ã chaque employÃ© le privilÃ¨ge minimal nÃ©cessaire pour accomplir les tÃ¢ches requises et veiller Ã ce que les droits d'accÃ¨s inutiles soient rÃ©voquÃ©s en cas d'Ã©volution des fonctions d'un employÃ©.

â¢ Ã tablir une procÃ©dure d'examen des accÃ¨s : mettre en place des alertes d'accÃ¨s automatiques pour informer au moins deux administrateurs des changements relatifs aux accÃ¨s et aux employÃ©s ou d'autres problÃ¨mes critiques.

â¢ Assurer la conformitÃ© : mettre en Å uvre un contrÃ´le d'accÃ¨s et de sÃ©paration des tÃ¢ches, Ã©tablir, mettre en Å uvre et appliquer une politique de sÃ©curitÃ© couvrant tous les accÃ¨s aux systÃ¨mes.

Pour en savoir plus sur Quest One.