Kingston : Pratiques et risques associÃ©s aux ClÃ©s USB en PME
Accessoire
PostÃ© par : JPilo
PubliÃ©e le : 19/1/2012 13:00:00

Kingston Digital Europe Ltd, premier constructeur indÃ©pendant mondial de produits mÃ©moire rÃ©vÃ¨le les meilleures pratiques et les risques associÃ©s Ã un manque de **politiques de sÃ©curitÃ© dans les organisations utilisant des clÃ©s USB** contenant des donnÃ©es confidentielles dâ□□une entreprise.

Â« *Les donnÃ©es sont l'ADN de toute sociÃ©tÃ© et doivent Ãªtre protÃ©gÃ©es Ã tout moment et manipulÃ©es avec prÃ©caution et Ã bon escient* Â», a dÃ©clarÃ© Jim Selby, Directeur Marketing Produit Europe, Kingston Technology. Â« *Les donnÃ©es sur les pÃ©riphÃ©riques USB devraient Ãªtre garanties et les politiques mises en oeuvre pour s'assurer que l'information est sauvegardÃ©e, stockÃ©e, tÃ©lÃ©chargÃ©e et partagÃ©e avec les seules parties autorisÃ©es. Ne pas respecter ces politiques expose une entreprise Ã des consÃ©quences nÃ©gatives, y compris le non-respect, les amendes, la perte financiÃ¨re et le manque de confiance de ses clients.* Â»

BasÃ© sur l'expÃ©rience considÃ©rable de Kingston du marchÃ© et du retour client, l'entreprise a identifiÃ© le top des meilleures pratiques que les organisations devraient suivre pour protÃ©ger les donnÃ©es confidentielles. Dans le climat Ã©conomique actuel, il est encore plus important que les entreprises favorisent une meilleure comprÃ©hension de sÃ©curitÃ© USB parmi leur personnel et de mettre en oeuvre la bonne politique pour s'assurer qu'ils ne seront pas les prochains faisant les gros titres.

Recommandations de Kingston pour les entreprises en matiÃ¨re de sÃ©curitÃ© pour les donnÃ©es transportables :

Construire un plan de clÃ©s USB cryptÃ©es : ProtÃ©ger & Respecter

Le meilleur moment pour Ã©laborer un plan de clÃ©s USB cryptÃ©es est avant tout de prouver que vous en avez un â□□ incorporer les clÃ©s USB sÃ©curisÃ©s et les politiques dans la stratÃ©gie globale de sÃ©curitÃ© de votre organisation.

Identifier les clÃ©s USB les plus appropriÃ©es pour votre organisation

DÃ©terminer la fiabilitÃ© et l'intÃ©gritÃ© des clÃ©s USB en vÃ©rifiant la conformitÃ© aux

normes de sÃ©curitÃ© de pointe et d'assurer qu'il n'y a pas de code malveillant sur eux.

Former et Ã©duquer

Ã□tablir un programme de formation qui sensibilise les employÃ©s sur l'utilisation acceptable et inacceptable des clÃ©s USB. Tour dâ□□horizon des incidents et des violations des utilisateurs et d'autres consÃ©quences nÃ©gatives qui se produisent lors de l'utilisation non sÃ©curisÃ©e de clÃ©s USB.

Ã□tablir et appliquer des rÃ¨glements

Si vous n'avez pas les bonnes politiques mises en place, les clÃ©s USB peuvent potentiellement Ãªtre lâ□□Ã©chec de votre stratÃ©gie de sÃ©curitÃ© des donnÃ©es. La dÃ©finition d'une politique est la premiÃ¨re Ã©tape dâ□□une extrÃªme importance. Soulignant la nÃ©cessitÃ© d'Ã©tablir et d'appliquer des rÃ¨glements, les rÃ©sultats de lâ□□Ã©tude Ponemon rÃ©vÃ¨lent que prÃ¨s de 50% des organisations ont confirmÃ© avoir perdu des clÃ©s contenant des informations sensibles ou confidentielles dans les 24 derniers mois.

Fournir des clÃ©s USB approuvÃ©es par lâ□□entreprise

BasÃ© sur un hardware encryptÃ© utilisant le Standard dâ□□encryptage avancÃ© (AES) 256 sÃ©curisÃ© fournissant portabilitÃ© et encryptage supÃ©rieur sur tous les logiciels.

GÃ©rer les clÃ©s USB autorisÃ©es et bloquer les appareils non approuvÃ©s

Les donnÃ©es sensibles peuvent Ãªtre copiÃ©es sur ces dispositifs et partagÃ©es avec des personnes extÃ©rieures Ã lâ□□entreprise mettant ainsi votre organisation dans les prochaines statistiques de donnÃ©es perdues ou volÃ©es.

Crypter les donnÃ©es confidentielles

Si vous ne cryptez pas les donnÃ©es avant qu'elles ne soient enregistrÃ©es sur clÃ©s USB, les pirates peuvent contourner votre anti-virus, pare-feu ou autres contrÃ´les, rendant ainsi vos informations vulnÃ©rables.

Certifier protection anti-virus prÃ©sent Ã chaque point d'entrÃ©e

S'assurer que les systÃ¨mes informatiques en tout point sont Ã©quipÃ©s dâ□□une mise Ã jour de logiciel anti-virus. Les failles de sÃ©curitÃ© continuent globalement et beaucoup sont le rÃ©sultat d'une clÃ© USB perdue ou non sÃ©curisÃ©e. En novembre, le Ponemon Institute a publiÃ© un projet de recherche parrainÃ© par Kingston Technology,Â "L'Ã©tat des clÃ©s USB sÃ©curisÃ©es en Europe", qui a interrogÃ© 2942 professionnels de l'informatique et des responsables de la sÃ©curitÃ© informatique des entreprises basÃ©es au Danemark, en Finlande, France, Allemagne, Pays-Bas, NorvÃ¨ge, Pologne, SuÃ¨de, Suisse et Royaume-Uni. Le rapport a rÃ©vÃ©lÃ© que bien que les entreprises comprennent que la

Â«nÃ©gligenceÂ» des employÃ©s met leurs organisations Ã risque, beaucoup de ces entreprises ne prennent pas les mesures nÃ©cessaires pour sÃ©curiser l'utilisation des clÃ©s USB et dÃ©finir des politiques appropriÃ©es.

Â Le rapport a constatÃ© que sur ces personnes interrogÃ©es seulement 48% considÃ¨rent que la protection des informations confidentielles et sensibles sur les clÃ©s USB est une grande prioritÃ© pour leur organisation, mÃªme si 63% d'entre eux estiment que les violations de donnÃ©es sont causÃ©es par la perte de clÃ©s USB.

Le rapport rÃ©vÃ¨le que les entreprises sont encore Ã©tonnamment laxistes quand il s'agit de dâ□□USB sÃ©curisÃ©e, malgrÃ© la reconnaissance des dangers et des consÃ©quences nÃ©gatives. MÃªme si 68% confirment que leurs organisations ont une politique d'utilisation acceptable, moins de la moitiÃ© d'entre eux affirment qu'ils ne sont pas tenus d'adopter des pratiques de sÃ©curitÃ© telles que l'utilisation de mots de passe, de verrouillage total, virus et malware scan etcâ□¦

Â«*Les solutions pour la sÃ©curisation des clÃ©s USB et pour obtenir le soutien et respect des employÃ©s des rÃ¨gles et politiques ne devraient pas Ãªtre complexes et coÃ»teuses, elles ne devraient pas rÃ©duire la productivitÃ© des employÃ©s* Â», dÃ©clare **Selby**. Â« *Notre objectif est d'aider les entreprises Ã rÃ©duire l'Ã©cart de sÃ©curitÃ© en comblant avec de meilleures pratiques pour les clÃ©s USB, et de les rendre aussi transparentes et simples que possible*. Â»

Pour consulter le rapport complet : **The State of USB Drive Security**