Kingston : Pratiques et risques associés aux Clés USB en PME
Accessoire
Posté par : JPilo
Publiée le : 19/1/2012 13:00:00

Kingston Digital Europe Ltd, premier constructeur indépendant mondial de produits mémoire révèle les meilleures pratiques et les risques associés à un manque de **politiques de sécurité dans les organisations utilisant des clés USB** contenant des données confidentielles d'une entreprise.

« *Les données sont l'ADN de toute société et doivent être protégées à tout moment et manipulées avec précaution et à bon escient* », a déclaré Jim Selby, Directeur Marketing Produit Europe, Kingston Technology. « *Les données sur les périphériques USB devraient être garanties et les politiques mises en oeuvre pour s'assurer que l'information est sauvegardée, stockée, téléchargée et partagée avec les seules parties autorisées. Ne pas respecter ces politiques expose une entreprise à des conséquences négatives, y compris le non-respect, les amendes, la perte financière et le manque de confiance de ses clients.* »

Basé sur l'expérience considérable de Kingston du marché et du retour client, l'entreprise a identifié le top des meilleures pratiques que les organisations devraient suivre pour protéger les données confidentielles. Dans le climat économique actuel, il est encore plus important que les entreprises favorisent une meilleure compréhension de sécurité 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 matière de sécurité pour les données transportables :

Construire un plan de clés USB cryptées : Protéger & Respecter

Le meilleur moment pour élaborer un plan de clés USB cryptées est avant tout de prouver que vous en avez un incorporer les clés USB sécurisés et les politiques dans la stratégie globale de sécurité de votre organisation.

Identifier les clés USB les plus appropriées pour votre organisation

Déterminer la fiabilité et l'intégrité des clés USB en vérifiant la conformité aux normes de sécurité de pointe et d'assurer qu'il n'y a pas de code malveillant sur eux.

Former et éduquer

Établir un programme de formation qui sensibilise les employés sur l'utilisation acceptable et inacceptable des clés USB. Tour d'horizon des incidents et des violations des utilisateurs et d'autres conséquences négatives qui se produisent lors de l'utilisation non sécurisée de clés USB.

Établir et appliquer des règlements

Si vous n'avez pas les bonnes politiques mises en place, les clés USB peuvent potentiellement être l'échec de votre stratégie de sécurité des données. La définition d'une politique est la première étape d'une extrême importance. Soulignant la nécessité d'établir et d'appliquer des règlements, les résultats de l'étude Ponemon révèlent que près de 50% des organisations ont confirmé avoir perdu des clés contenant des informations sensibles ou confidentielles dans les 24 derniers mois.

Fournir des clés USB approuvées par l'entreprise

Basé sur un hardware encrypté utilisant le Standard d'encryptage avancé (AES) 256 sécurisé fournissant portabilité et encryptage supérieur sur tous les logiciels.

Gérer les clés USB autorisées et bloquer les appareils non approuvés

Les données sensibles peuvent être copiées sur ces dispositifs et partagées avec des personnes extérieures à l'entreprise mettant ainsi votre organisation dans les prochaines statistiques de données perdues ou volées.

Crypter les données confidentielles

Si vous ne cryptez pas les données avant qu'elles ne soient enregistrées sur clés USB, les pirates peuvent contourner votre anti-virus, pare-feu ou autres contrôles, rendant ainsi vos informations vulnérables.

Certifier protection anti-virus présent à chaque point d'entrée

S'assurer que les systèmes informatiques en tout point sont équipés d'une mise à jour de logiciel

anti-virus. Les failles de sécurité continuent globalement et beaucoup sont le résultat d'une clé USB perdue ou non sécurisée. En novembre, le Ponemon Institute a publié un projet de recherche parrainé par Kingston Technology, "L'état des clés USB sécurisées en Europe", qui a interrogé 2942 professionnels de l'informatique et des responsables de la sécurité informatique des entreprises basées au Danemark, en Finlande, France, Allemagne, Pays-Bas, Norvège, Pologne, Suède, Suisse et Royaume-Uni. Le rapport a révélé que bien que les entreprises comprennent que la

«négligence» des employés met leurs organisations à risque, beaucoup de ces entreprises ne prennent pas les mesures nécessaires pour sécuriser l'utilisation des clés USB et définir des politiques appropriées.

Le rapport a constaté que sur ces personnes interrogées seulement 48% considèrent que la protection des informations confidentielles et sensibles sur les clés USB est une grande priorité pour leur organisation, même si 63% d'entre eux estiment que les violations de données sont causées par la perte de clés USB.

Le rapport révèle que les entreprises sont encore étonnamment laxistes quand il s'agit de d'USB sécurisée, malgré la reconnaissance des dangers et des conséquences négatives. Même si 68% confirment que leurs organisations ont une politique d'utilisation acceptable, moins de la moitié d'entre eux affirment qu'ils ne sont pas tenus d'adopter des pratiques de sécurité telles que l'utilisation de mots de passe, de verrouillage total, virus et malware scan etc…

«*Les solutions pour la sécurisation des clés USB et pour obtenir le soutien et respect des employés des règles et politiques ne devraient pas être complexes et coûteuses, elles ne devraient pas réduire la productivité des employés* », déclare **Selby**. « *Notre objectif est d'aider les entreprises à réduire l'écart de sécurité en comblant avec de meilleures pratiques pour les clés USB, et de les rendre aussi transparentes et simples que possible*. »

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