

Les clés USB non sécurisées : un risque pour les entreprises

Les DSI peuvent commencer à s'angoisser ! Car les résultats de cette étude font froid dans le dos. 77% des utilisateurs interrogés déclarent avoir utilisé des clés personnelles à des fins professionnelles. Or, consultés sur cette même question, les responsables informatiques estiment cette proportion à seulement 35%.

Les utilisateurs citent, parmi les données les plus susceptibles d'être copiées sur une clé flash personnelle, des fichiers clients (25%), des informations financières (17%), des business plans (15%), des fichiers d'employés (13%), des plans marketing (13%), des éléments de propriété intellectuelle (6%) et du code source de logiciel (6%).

Les résultats de l'enquête indiquent que la portabilité des clés flash USB représente un risque significatif de perte de données. Environ un dixième (12%) des utilisateurs en entreprise signale avoir trouvé une clé flash égarée dans un lieu accessible au public.

En outre, interrogés sur ce qu'ils feraient en pareil cas, 55% ont répondu qu'ils en examineraient le contenu.

Les résultats de l'enquête révèlent que, si certaines entreprises ont pris des mesures pour mettre en oeuvre des règles et sensibiliser leurs employés à l'utilisation appropriée des clés flash USB, ces mesures sont principalement réactives.

Plus de deux tiers (67%) des responsables informatiques consultés mettent ou ont mis en place une charte à la suite d'une fuite de données ou d'une atteinte à la sécurité dans leur entreprise.

Par ailleurs, à peine plus de la moitié (52%) d'entre eux ont mis en oeuvre une solution de sécurisation des postes de travail.

La formation : un moyen de plus pour lutter contre la perte de données

La connaissance de l'existence de règles concernant l'emploi des clés flash USB dans l'entreprise varie parmi les personnes interrogées.

23% des utilisateurs ne sont pas du tout au courant de l'existence de telles règles ou, s'ils le sont, en ignorent les détails spécifiques.

Parallèlement, près de la moitié (44%) des utilisateurs pensent que, à leur connaissance, leur entreprise n'a pas instauré de règle interdisant la copie de données professionnelles sur des clés flash personnelles USB. 16% ignorent l'existence d'une telle règle, tandis que 40% déclarent que leur entreprise a effectivement formulé une interdiction de ce type.

Les réponses des responsables informatiques vont dans le même sens. 21% jugent « limitée » la compréhension des règles par les employés ; 33% la jugent « moyenne », 28% « bonne » et 19% « complète ».

Interrogés quant à la formation, les responsables informatiques consultés indiquent que les employés reçoivent une formation aux règles d'utilisation des clés flash USB une fois par an (33%), plusieurs fois par an (24%), uniquement au moment de leur embauche (22%), au cas par cas (17%) ou bien pas de formation du tout (3%).

Environ 41% des responsables informatiques se disent au minimum mal à l'aise à propos du degré d'utilisation des clés flash USB dans leur entreprise, ce qui dénote un niveau non négligeable de risque potentiel.

Les utilisateurs confirment ces préoccupations en indiquant, dans une proportion d'un pour cinq (21%), être peu ou pas conscients des risques que présente le transport d'informations de l'entreprise sur des clés USB, signe d'un risque significatif de perte de données.