Prim'X : Les bonnes pratiques pour la protection des donnÃ©es
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 17/12/2010 13:30:00

Suite aux vols dâordinateurs de journalistes liÃ©s Ã lâaffaire Â« Woerth-Bettencourt Â» et Ã lâaffaire Â« Ockrent Â» notamment, **Xavier Dreux**, responsable marketing **PrimâX** Technologies, Ã©diteur de solutions de sÃ©curitÃ© informatique a souhaitÃ© rÃ©agir face aux mÃ©thodes employÃ©es pour rÃ©cupÃ©rer de la donnÃ©e et surtout rappeler quelques **bonnes pratiques pour assurer la protection des informations sensibles**.

Qui vole en amateur, vole un ordinateur !

Voler un ordinateur pour dÃ©rober de la donnÃ©e est devenue une mÃ©thode archaÃ¯queâ¦ Aujourdâhui, il est en effet possible de rÃ©cupÃ©rer des donnÃ©es sans employer ce moyen visible au premier coup dâÅil, si les informations ne sont pas protÃ©gÃ©es. Mieux vaut donc prÃ©server la donnÃ©e en utilisant le chiffrement pour rendre celle-ci inexploitable, avant mÃªme que lâordinateur ne soit volÃ©.

Alors, comment protÃ©ger efficacement les donnÃ©es ? Faut-il protÃ©ger une partie des donnÃ©es seulement ? Faut-il ne rien laisser sur son ordinateur ? Si la solution fiable Ã 100 % nâexiste pas, voici tout de mÃªme quelques conseils par rapport Ã quelques fausses possibilitÃ©s de protÃ©ger ses donnÃ©es.

Ne laisser aucune donnÃ©e sensible sur son ordinateur et les conserver sur une clÃ© USB, pourquoi pas ? Mais Ã plusieurs conditions : ne pas perdre ou se faire voler ce pÃ©riphÃ©rique, et ne pas oublier de copier systÃ©matiquement les donnÃ©es sensibles sur la clÃ© USBâ¦

Pour palier au vol dâinformations placÃ©es sur pÃ©riphÃ©rique externe, il existe tout de mÃªme des solutions de protection qui permettent de chiffrer les donnÃ©es mises sur la clÃ© USB, les rendant inexploitables. Sauf quâil ne faut pas oublier dây stocker les bonnes donnÃ©es.

Mais pour Ã©viter que lâutilisateur nâoublie de mettre les donnÃ©es quâil souhaite

protÃ©ger sur la clÃ© USB, il nâ□□existe malheureusement aucune solution.

Alors la clÃ© USB avec un coffre-fort est-elle la solution idÃ©ale ?

Câ□□est en tout cas une premiÃ¨re Ã©tape pour rendre les informations stockÃ©es sur la clÃ© USB inexploitables par un tiers non autorisÃ©. MalgrÃ© tout, nous laissons lâ□□utilisateur crÃ©er sa propre politique de sÃ©curitÃ© et la libertÃ© de dÃ©cider quelle(s) donnÃ©e(s) il doit chiffrerâ□¦

Pourquoi ne faut-il pas laisser lâ□□utilisateur dÃ©cider des informations Ã sÃ©curiser ?

Laisser lâ□□utilisateur dÃ©cider des donnÃ©es quâ□□il souhaite protÃ©ger reprÃ©sente deux risques principaux. Tout dâ□□abord, lâ□□utilisateur peut oublier de mettre sur la clÃ© les informations sensibles. Ensuite, lâ□□utilisateur devient le seul juge en matiÃ¨re de confidentialitÃ© des informations. Mais est-il le mieux placÃ© pour faire ce choix ?

En entreprise, laisser lâ□□utilisateur dÃ©cider de ce quâ□□il faut protÃ©ger ou non peut rapidement devenir un casse-tÃªte chronophage et peu efficace. Le sensibiliser Ã la protection de lâ□□information, lui fournir une mÃ©thodologie peut Ãªtre une solution, mais ceci implique dâ□□interfÃ©rer dans son organisation de travail. Or, il est prouvÃ© que pour faire adhÃ©rer lâ□□utilisateur Ã une politique de sÃ©curitÃ©, il est nÃ©cessaire de ne pas changer ses habitudes de travail. Ainsi, il est prÃ©fÃ©rable de mettre en place une solution transparente et automatique.

Si la clÃ© USB simple ou avec coffre-fort ne se rÃ©vÃ¨le pas trÃ¨s efficace, pourquoi ne pas mettre un systÃ¨me de coffre-fort directement sur lâ□□ordinateur ?

Cela permettrait en effet de limiter le risque de perte de clÃ© USB. Le disque virtuel entiÃ¨rement chiffrÃ© est ainsi directement sur lâ□□ordinateur, ouvert et refermÃ© par lâ□□utilisateur dÃ¨s quâ□□il le souhaite. Impossible donc, Ã premiÃ¨re vue, dâ□□accÃ©der aux informations qui ont Ã©tÃ© placÃ©es dans ce coffre-fort, si le mot de passe a correctement Ã©tÃ© crÃ©Ã©. MalgrÃ© tout, ce schÃ©ma nâ□□Ã©vite pas lâ□□Ã©cueil du libre choix de lâ□□utilisateur Ã protÃ©ger ce que bon lui semble.

Lâ□□idÃ©al est sans doute de pouvoir protÃ©ger lâ□□ensemble des donnÃ©es, sans distinction, et oÃ¹ quâ□□elles se trouvent.

Si lâ□□utilisateur ne doit pas Ãªtre le dÃ©cideur principal du type de donnÃ©es Ã chiffrer et de la protection des informations de lâ□□entreprise, peut-on donner les pleins pouvoirs au service informatique ?

Effectivement, lâ□□administrateur systÃ¨me doit-il Ãªtre affranchi de toute limite et avoir accÃ¨s aux donnÃ©es sensibles de lâ□□entreprise sous prÃ©texte quâ□□il administre le systÃ¨me dâ□□information ? Bien entendu, la rÃ©ponse est non. Le service informatique doit pouvoir avoir accÃ¨s aux machines des diffÃ©rents services, mais sans pouvoir prendre connaissance des documents utilisÃ©s par ces derniers.

Qui plus est, si il a en son sein des Ã©lÃ©ments outsourcÃ©s ou bÃ©nÃ©ficie du support externe dâ□□entreprises de services.

Les donnÃ©es ne doivent effectivement pas Ãªtre lisibles par une personne non habilitÃ©e.

Droit dâ□□accÃ¨s ne doit pas signifier droit de lecture.

Alors, peut-on rÃ©soudre deux problÃ©matiques majeures liÃ©es au chiffrement des donnÃ©es Ã©voquÃ©es prÃ©cÃ©demment : Ã savoir oÃ¹ doit-on chiffrer la donnÃ©e et quelles sont les donnÃ©es que lâ□□on doit chiffrer ?

Il semble intÃ©ressant dâ□□Ã©tudier la possibilitÃ© suivante : plutÃ´t que de chiffrer certaines donnÃ©es sur un espace dÃ©diÃ©, nâ□□est-il pas plus sÃ»r de chiffrer la donnÃ©e en permanence, oÃ¹ quâ□□elle se trouve.

Les affaires de vol dâ□□ordinateurs ou de donnÃ©es ayant rÃ©cemment Ã©maillÃ©es lâ□□actualitÃ© ne sont sans doute pas les derniÃ¨res. PlutÃ´t que dâ□□empÃªcher le vol de donnÃ©es, la solution la plus pragmatique reste de rendre ces donnÃ©es inexploitables par les voleurs. Une donnÃ©e protÃ©gÃ©e est une donnÃ©e cryptÃ©e.