Stockage amovibles, Menace rÃ©elle pour la sÃ©curitÃ© des informations en PME
Internet
PostÃ© par : JulieM
PubliÃ©e le : 6/7/2009 0:00:00

Ã vingt-neuf ans, Daniel Harrington, analyste dans une sociÃ©tÃ© internationale de services et dâingÃ©nierie informatique, nâaurait jamais imaginÃ© se retrouver au cÅur dâun scandale qui retentirait jusquâau gouvernement britannique. Fin octobre dernier, une unitÃ© de stockage amovible lui appartenant Ã©tait retrouvÃ©e dans un parking public Ã proximitÃ© dâun pub dans la ville anglaise de Cannock.

Cette affaire serait passÃ©e inaperÃ§ue si lâobjet en question nâavait Ã©tÃ© utilisÃ© pour stocker les mots de passe ultra-secrets permettant dâaccÃ©der Ã la base de donnÃ©es de services en ligne du gouvernement britannique.

Pour **Alexei Lesnykh,** responsable du dÃ©veloppement international et de la stratÃ©gie produit de DeviceLock, Ã©diteur de solutions logicielles pour contrÃ´ler et protÃ©ger les informations en entreprises, outre la nÃ©gligence, cet incident met en Ã©vidence une prÃ©occupation majeure dans le secteur de la sÃ©curitÃ© informatique : la diffusion de donnÃ©es confidentielles et sensibles nâa jamais Ã©tÃ© aussi simple.

Lâinformation est lâune des ressources les plus prÃ©cieuses des entreprises. Tout comme les autres actifs vitaux, elle doit Ãªtre protÃ©gÃ©e.

Depuis quelques annÃ©es, le Ponemon Institute Ã©value ces dommages. Selon un rapport publiÃ© en 2008, le prÃ©judice moyen rÃ©sultant dâun incident isolÃ© peut atteindre plusieurs millions de dollars. Les sociÃ©tÃ©s basÃ©es aux Ãtats-Unis sont les plus affectÃ©es : chaque brÃ¨che de sÃ©curitÃ© informatique leur coÃ»tant en moyenne 6,6 millions de dollars.

La fuite des donnÃ©es est ainsi devenue une prioritÃ© des services en charge de la sÃ©curitÃ© en entreprises.

Il semblerait cependant que la plupart des organisations nâadoptent pas la meilleure approche en la matiÃ¨re.

Lâexemple le plus simple en est peut-Ãªtre la focalisation gÃ©nÃ©rale sur la protection contre les Â« menaces extÃ©rieures Â», comme les logiciels malveillants (malware), le courrier publicitaire non sollicitÃ© (spam) et le piratage informatique. Si la rÃ©alitÃ© de ces menaces ne fait aucun doute, elles ne reprÃ©sentent, selon le Ponemon Institute, pas plus de 7% du nombre total des incidents (aux Ãtats-Unis).

La cause des 93% des failles de sÃ©curitÃ© restantes est liÃ©e Ã des actions du personnel en place, en dâautres termes des collaborateurs disposant des droits dâaccÃ¨s Ã des informations confidentielles.

Quelques solutions

Chaque sociÃ©tÃ© doit commencer par dÃ©terminer si la valeur de ses donnÃ©es justifie une interdiction dâutilisation totale de dispositifs amovibles au niveau de ses points dâaccÃ¨s terminaux. En thÃ©orie, il est possible de dÃ©sactiver tous les ports et les lecteurs des PCs avant leur remise aux employÃ©s.

Ainsi, avant dâ□□envisager une stratÃ©gie de protection des donnÃ©es stockÃ©es sur des clÃ©s USB, des tÃ©lÃ©phones intelligents capables de se synchroniser sur les postes de travail et dâ□□autres types dâ□□appareils mobiles Ã connectivitÃ© plug-and-play, il convient de se poser la question suivante :

Â« Les avantages liÃ©s Ã lâ□□utilisation de ces outils sont-ils supÃ©rieurs aux risques de fuite de donnÃ©es associÃ©s ? Â».

Ã□ en juger par les pratiques actuelles, la plupart des entreprises ne souhaitent pas priver leurs collaborateurs de ces dispositifs, qui sont souvent synonymes dâ□□augmentation de la productivitÃ©. Cela se comprend facilement : sans clÃ© USB, il ne serait pas toujours possible dâ□□animer une prÃ©sentation ou de travailler occasionnellement depuis son domicile.

Câ□□est pour cette raison que les solutions radicales telles que la dÃ©sactivation totale des ports physiques ou lâ□□installation dâ□□un matÃ©riel pour les rendre inopÃ©rants ne sont que trÃ¨s rarement utilisÃ©es, et seulement dans certains services oÃ¹ sont traitÃ©es des informations ultra-confidentielles.

Ã□ la place, les entreprises prÃ©fÃ¨rent dÃ©ployer des logiciels de protection reconnus pour leur efficacitÃ© et leur ergonomie.

[Tribune dâ□□**Alexei Lesnykh** Responsable du DÃ©veloppement International et de la StratÃ©gie Produit de DeviceLock]