Internet : Les 5 grandes idÃ©es fausses sur la protection des donnÃ©es
Internet
PostÃ© par : JulieM
PubliÃ©e le : 9/12/2010 13:00:00

La derniÃ¨re tendance de la sÃ©curitÃ© informatique concerne la protection des donnÃ©es. DÃ©sormais, les donnÃ©es constituent les ressources les plus prÃ©cieuses quâ□□un dÃ©partement informatique doit protÃ©ger, et la technologie a Ã©voluÃ© pour satisfaire cet impÃ©ratif

Les technologies de cryptage et les solutions de protection contre les fuites contribuent Ã renforcer le stockage de donnÃ©es des entreprises.

Toutefois, Ã mesure que les entreprises ajustent leurs stratÃ©gies de protection des donnÃ©es, elles deviennent la proie dâ□□idÃ©es fausses quant Ã leur dÃ©fense. Il est impÃ©ratif pour les responsables de la sÃ©curitÃ© quâ□□ils connaissent la vÃ©ritÃ© et dÃ©veloppent un programme de protection des donnÃ©es bien Ã©quilibrÃ©.

IdÃ©e fausse nÂ°1 : La menace extÃ©rieure pÃ¨se bien plus que la menace intÃ©rieure.

Les risques de fuite des donnÃ©es sont classÃ©s en deux catÃ©gories principales : la perte de donnÃ©es et leur vol. Les gros titres aujourdâ□□hui se rapportent gÃ©nÃ©ralement Ã la premiÃ¨re catÃ©gorie, le plus souvent du fait de donnÃ©es ayant disparues suite Ã la perte dâ□□ordinateurs portables, de bandes de sauvegarde et de pÃ©riphÃ©riques. Dans ce cas, seule la valeur du matÃ©riel fait lâ□□objet dâ□□un vol.

La fuite des donnÃ©es est plus dangereuse pour lâ□□entreprise. Les individus malveillants cherchent des moyens dâ□□accÃ©der aux donnÃ©es et Ã les utiliser Ã leur avantage car ils connaissent leur valeur. Depuis lâ□□extÃ©rieur, grÃ¢ce Ã des programmes malveillants, ils installent des portes dÃ©robÃ©es dans lâ□□entreprise. A lâ□□intÃ©rieur, il sâ□□agit tout simplement de charger les donnÃ©es sur un pÃ©riphÃ©rique externe pour lâ□□emmener chez soi. Pour Ã©viter toutes attaques, les entreprises ont mis en place une protection complexe et performante visant les attaques extÃ©rieures mais celles internes sont le plus souvent ignorÃ©es et laissent les entreprises vulnÃ©rables. Beaucoup nâ□□ont aucune mÃ©thode de protection pour empÃªcher les salariÃ©s de charger des donnÃ©es sur des pÃ©riphÃ©riques externes. Ce type de fuite reprÃ©sente le risque le plus dangereux car ces personnes ont accÃ¨s aux informations clÃ©s de lâ□□entreprise, en connaissent la valeur et ce quâ□□il faut en faire.

Si les entreprises veulent hiÃ©rarchiser la sÃ©curitÃ© en fonction de la gravitÃ© du

risque, elles doivent placer la protection contre les menaces internes en tÃªte de liste. Elles doivent Ãªtre en mesure dâ□□auditer automatiquement ce processus de protection. Sans la visibilitÃ© de lâ□□audit, les entreprises ne peuvent quantifier les risques que posent les fuites de donnÃ©es. Elles ne sauront pas si les donnÃ©es ont transitÃ© entre les postes de travail, desquelles il sâ□□agissait, ni la quantitÃ© ayant subi une fuite. Pour Ãªtre efficace, lâ□□audit doit Ãªtre intÃ©grÃ© Ã la technologie de protection des donnÃ©es pour en tirer pleinement avantage.

IdÃ©e fausse nÂ°2 : Les fuites de donnÃ©es constituent le seul aspect de la protection des donnÃ©es dont les entreprises doivent se soucier.

Les fuites de donnÃ©es ont un potentiel dÃ©vastateur. MÃªme si elles ne tombent pas aux mains de personnes malintentionnÃ©es, câ□□est un Ã©vÃ©nement pÃ©nible. La protection de leur confidentialitÃ© nâ□□est quâ□□une facette de leur prÃ©servation. Deux composants jouent un rÃ´le crucial : la protection de lâ□□intÃ©gritÃ© des donnÃ©es et la disponibilitÃ©.

Les capacitÃ©s de surveillance du contenu et dâ□□audit ont un rÃ´le essentiel dans le processus de garantie de lâ□□intÃ©gritÃ© des donnÃ©es ce qui offre un contrÃ´le des actions malveillantes en sachant oÃ¹ les donnÃ©es transitent et sont modifiÃ©es. La gestion des vulnÃ©rabilitÃ©s, des correctifs logiciels et la sÃ©curisation des configurations des postes de travail sont primordiaux pour garantir lâ□□intÃ©gritÃ© des donnÃ©es. En effet, les applications et machines non gÃ©rÃ©es permettent la propagation de programmes malveillants et dâ□□enregistreurs de frappe susceptibles de compromettre lâ□□intÃ©gritÃ© et la disponibilitÃ© des donnÃ©es.

IdÃ©e fausse nÂ°3 : La protection de la messagerie Ã©lectronique Ã©vitera tous les problÃ¨mes potentiels de fuite de donnÃ©es.

La plupart des entreprises tiennent compte des avertissements concernant le risque liÃ© aux fuites de donnÃ©es par mail. Les experts de la sÃ©curitÃ© ont compris la brÃ¨che que reprÃ©sente la messagerie non surveillÃ©e si une personne interne dÃ©cidait de transmettre des informations sensibles Ã lâ□□extÃ©rieur. Ainsi, la plupart des entreprises ont comblÃ© ce fossÃ© avec des outils de filtrage et de surveillance de la messagerie.

La protection de la messagerie nâ□□est pas le seul et unique moyen pour se protÃ©ger contre la fuite de donnÃ©es : les utilisateurs peuvent consulter des sites malveillants, provoquant lâ□□installation de portes dÃ©robÃ©es non dÃ©tectÃ©es sur leur systÃ¨me. Pire, les utilisateurs sortent des informations confidentielles grÃ¢ce Ã des pÃ©riphÃ©riques. Ainsi, le colmatage des fuites de donnÃ©es ne sâ□□arrÃªte pas Ã la messagerie Ã©lectronique.

IdÃ©e fausse nÂ°4 : Les entreprises peuvent contrÃ´ler les fuites de donnÃ©es liÃ©es Ã des supports amovibles en interdisant ces derniers.

Lorsque les analystes ont averti des risques posÃ©s par les supports amovibles, des responsables informatiques ont crÃ©Ã©s des politiques interdisant lâ□□usage des pÃ©riphÃ©riques optiques et USB. Cette interdiction relÃ¨ve dâ□□une mauvaise politique, car ces pÃ©riphÃ©riques sont utiles et permettent de mieux accomplir les tÃ¢ches. Cette interdiction entrave les activitÃ©s au quotidien. Les entreprises doivent Ã©laborer des politiques de sÃ©curitÃ© qui interdisent uniquement le comportement risquÃ© par lequel les supports amovibles reprÃ©sentent une menace et doivent recourir Ã une technologie suffisamment flexible pour mettre en vigueur ces politiques.

IdÃ©e fausse nÂ°5 : Il suffit dâ□□une technologie de filtrage du contenu et de cryptage pour protÃ©ger les donnÃ©es.

Le filtrage du contenu a amÃ©liorÃ© la protection des donnÃ©es mais il comporte une lacune flagrante. La solution type de filtrage du contenu surveille lâ□□activitÃ© du rÃ©seau ou de la messagerie Ã©lectronique, mais une fois que les informations sont transfÃ©rÃ©es sur la machine en local, elle ne surveille pas ce que lâ□□utilisateur fait des donnÃ©es. Or, celui ayant des intentions malveillantes peut transfÃ©rer des donnÃ©es sur la machine en local, puis les copier sur une clÃ© USB sans que la solution de filtrage du contenu en avertisse les responsables de la sÃ©curitÃ©.

De mÃªme, le cryptage a ses points faibles. La plupart des solutions de cryptage protÃ¨gent les donnÃ©es en cas de vol ou de perte dâ□□un ordinateur ou dâ□□un pÃ©riphÃ©rique. Le cryptage de ces pÃ©riphÃ©riques empÃªche une personne extÃ©rieure dâ□□accÃ©der aux donnÃ©es quâ□□ils contiennent. Par contre, aprÃ¨s avoir autorisÃ© et saisit son mot de passe, lâ□□utilisateur a un accÃ¨s libre aux donnÃ©es. Le cryptage ne protÃ¨ge pas les informations sur les postes de travail aprÃ¨s sâ□□Ãªtre authentifiÃ©.

Pour parvenir Ã une protection Ã©quilibrÃ©e, les entreprises doivent complÃ©ter le cryptage et le filtrage du contenu par une solution performante, capable de surveiller les utilisateurs et de mettre en vigueur les politiques de faÃ§on proactive sur les postes de travail. Ceux-ci sont devenus les nouvelles cibles pour obtenir un accÃ¨s aux donnÃ©es, car bon nombre dâ□□entreprises nâ□□a pas de politiques applicables et elles ne peuvent quantifier leur exposition aux fuites de donnÃ©es. La gestion de lâ□□usage des pÃ©riphÃ©riques amovibles et des flux de donnÃ©es vers et depuis ces pÃ©riphÃ©riques protÃ¨ge certes une entreprise contre le plus grand point de fuite des donnÃ©es, mais une stratÃ©gie complÃ¨te de protection des donnÃ©es doit intÃ©grer dâ□□autres technologies afin de sÃ©curiser les donnÃ©es mobiles et statiques.