Novell : Gestion des risques : Lâ□□urgence est Ã la flexibilitÃ©
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 6/10/2010 11:24:26

MalgrÃ© plus dâ□□une dÃ©cennie dâ□□efforts, et des milliards de dollars investis dans la sÃ©curitÃ© et la conformitÃ© informatique, lâ□□**entreprise est encore et toujours la proie de failles de sÃ©curitÃ©**, de constats dâ□□audit rÃ©glementaires nÃ©gatifs, et de coÃ»ts liÃ©s aux atteintes portÃ©es aux donnÃ©es.

Pourquoi ? Parce que la plupart dâ□□entre-elles restent trop concentrÃ©es sur les incidents de sÃ©curitÃ© et de conformitÃ© qui se produisent au quotidien. Comment pourrait-on expliquer autrement les donnÃ©es de coÃ»t alarmantes qui continuent Ã Ãªtre publiÃ©es ? Prenez par exemple les conclusions de lâ□□Etude 2009 du Ponemon Institute : Cost of a Data Breach (Le coÃ»t de la violation des donnÃ©es), qui estime le coÃ»t par enregistrement Ã 204 dollars. Multipliez ce coÃ»t par des milliers, voire des centaines de milliers dâ□□enregistrements, et câ□□est Ã des millions de dollars que se chiffrent les dommages de ces atteintes et manquements.

Les approches ad hoc de sÃ©curitÃ© et de conformitÃ© sont inopÃ©rantes

Personne ne peut nier que la sÃ©curitÃ© et la conformitÃ© sont onÃ©reuses et dÃ©licates Ã obtenir et Ã maintenir. Pendant ce temps, les rÃ©glementations et les menaces de sÃ©curitÃ© persistent. Et bien que les dÃ©penses et dommages engendrÃ©s par les amendes et atteintes Ã la protection des donnÃ©es soient considÃ©rables, on peut relever un point positif : une bonne approche de la gestion de la conformitÃ© et des risques est moins coÃ»teuse que les mesures que prennent les entreprises pour rÃ©gler ces problÃ¨mes aujourdâ□□hui.

Pensez Ã lâ□□accroissement des risques de sÃ©curitÃ©, des coÃ»ts de gestion, et du nombre de constats dâ□□audit nÃ©gatifs quâ□□entraÃ®neront des incidents sâ□□ils se multiplient Ã travers une entreprise. Ils peuvent englober les politiques de mot de passe, le provisionnement de workflow, les droits dâ□□accÃ¨s, les configurations systÃ¨me, les politiques de gestion des journaux, ainsi que de nombreux autres contrÃ´les sÃ©curitaires et rÃ©glementaires. Câ□□est comme cela que de trÃ¨s petites insuffisances rÃ©glementaires se muent en problÃ¨mes coÃ»teux et systÃ©miques en se rÃ©pandent Ã travers lâ□□entreprise et lâ□□infrastructure informatique.

Si les entreprises sont dÃ©jÃ confrontÃ©es Ã ces types de dÃ©fis en matiÃ¨re de gouvernance et de gestion des risques, comment comptent-elles rÃ©duire le moment venu les risques et administrer les architectures dynamiques qui dÃ©pendront encore plus quâ□□aujourdâ□□hui de la virtualisation ? A un horizon plus lointain, comment gÃ©reront-elles un environnement de cloud computing bien plus nÃ©buleux que leurs systÃ¨mes actuels ?

La rÃ©ponse est simple : elles doivent construire une infrastructure de gouvernance unifiÃ©e et flexible, qui attÃ©nuera les risques et rÃ©duira les coÃ»ts du momentâ□□ tout en prÃ©parant

lâ□□entreprise Ã une dÃ©pendance encore plus lourde vis-Ã -vis de la virtualisation et Ã lâ□□adoption Ã terme de lâ□□informatique sur le cloud.

Le passage Ã une structure unifiÃ©e et flexible de gestion de la conformitÃ© et des risques

La premiÃ¨re Ã©tape consiste Ã sâ□□Ã©loigner de lâ□□approche ad hoc, de la gestion de la conformitÃ© rÃ©glementaire et des risques. Pour cela, le meilleur moyen est de recenser lâ□□ensemble des processus et contrÃ´les de gestion du risque de lâ□□entreprise, puis de vÃ©rifier quâ□□ils sont clairement dÃ©finis et documentÃ©s. Cela peut sâ□□avÃ©rer un travail long et pÃ©nible, compte tenu des centaines, voire des milliers de contrÃ´les et de politiques en vigueur au sein de lâ□□entreprise selon sa taille. Mais cela en vaut la peine.

Une fois lâ□□inventaire effectuÃ©, il convient de simplifier et consolider les contrÃ´les rÃ©glementaires partout oÃ¹ câ□□est possible, puis de mapper ces contrÃ´les sur les systÃ¨mes et donnÃ©es de lâ□□entreprise. PlutÃ´t que de dÃ©ployer un ensemble de contrÃ´les totalement distinct pour PCI DSS, HIPAA et autres lois et normes, il est prÃ©fÃ©rable de dÃ©terminer les contrÃ´les communs et dâ□□unifier ces politiques au sein dâ□□une infrastructure unique capable de rÃ©pondre Ã toutes les exigences rÃ©glementaires et de politique de sÃ©curitÃ© interne. Enfin, pour surveiller de maniÃ¨re continue lâ□□efficacitÃ© des politiques et contrÃ´les mis en place, lâ□□utilisation dâ□□outils informatiques est recommandÃ©e. Cela concernera la surveillance des journaux, des rapports de gestion des identitÃ©s et des accÃ¨s, la gestion des informations et Ã©vÃ©nements de sÃ©curitÃ©, entre autres applications de sÃ©curitÃ© et de conformitÃ©.

Combien de contrÃ´les redondants peut-on trouver ? Beaucoup, selon le nombre de rÃ©glementations et de domaines dâ□□activitÃ© de lâ□□entreprise. Est-il nÃ©cessaire dâ□□appliquer des politiques de mot de passe distinctes au sein dâ□□une sociÃ©tÃ© ? Il vaut mieux se limiter Ã une seule politique de mot de passe pouvant Ãªtre appliquÃ©e de faÃ§on homogÃ¨ne Ã travers lâ□□entreprise. Il en sera de mÃªme pour le provisionnement du workflow, lâ□□Ã©tablissement des droits dâ□□accÃ¨s, la gestion et la surveillance des journaux des Ã©vÃ©nements, et pour la plupart des autres politiques.

DÃ¨s lors, si une nouvelle obligation rÃ©glementaire fait son apparition â□□demande de saisie dâ□□un mot de passe dâ□□une certaine longueur, par exempleâ□□ il suffit de mettre Ã jour cette politique plutÃ´t que de remanier cinq politiques sÃ©parÃ©es, chacune avec sa propre couche de supervision et de gouvernance.

Les avantages des infrastructures virtualisÃ©es et Â« sur le cloud Â»

Maintenant, songez Ã lâ□□impact de cette infrastructure unifiÃ©e et flexible de gestion des risques et de la conformitÃ© sur les environnements virtualisÃ©s. La sÃ©curitÃ© et la conformitÃ© sont considÃ©rablement modifiÃ©es lorsque la virtualisation est introduite dans les systÃ¨mes de production. Comment les politiques sont-elles mappÃ©es sur les machines virtuelles correspondantes ? Comment le basculement dâ□□une charge de travail virtualisÃ©e entre deux tÃ¢ches peut-il faire Ã©chouer les contrÃ´les rÃ©glementaires ? Comment les contrÃ´les politiques et de sÃ©curitÃ© de ces charges de travail sont-ils mis Ã jour lorsque les rÃ©glementations ou les menaces de sÃ©curitÃ© Ã©voluent ?

Nul doute quâ□□une infrastructure unifiÃ©e et flexible de gestion des risques et de la conformitÃ© aidera les entreprises Ã gÃ©rer la conformitÃ© et la sÃ©curitÃ© de ces charges de travail virtualisÃ©es bien plus intelligemment.

Il en va de mÃªme pour le passage au cloud computing. Ce travail entrepris permettra de vÃ©rifier la mise en place effective de systÃ¨mes de contrÃ´le dâ□□accÃ¨s appropriÃ©s Ã travers les systÃ¨mes informatiques physiques, virtuels et Â« sur le cloud Â». Il sera possible de vÃ©rifier que les bons journaux sont gÃ©rÃ©s, que les contrÃ´les de confidentialitÃ© des donnÃ©es sont en

place, et que dâ□□autres politiques de sÃ©curitÃ© sont appliquÃ©es, et ce que le travail ait lieu dans le datacenter principal, sur un systÃ¨me virtuel installÃ© dans un bureau distant, ou dans les installations dâ□□un fournisseur de services sur le cloud, nâ□□importe oÃ¹ dans le monde.

La construction dâ□□une infrastructure flexible de gestion de la conformitÃ© et des risques peut sâ□□avÃ©rer dÃ©licate et onÃ©reuse, mais jamais autant que le prix Ã payer pour lâ□□atteinte Ã la protection des donnÃ©es, les amendes pour non conformitÃ©, et la mobilisation de main-dâ□□Å□uvre pour rÃ©pondre aux urgences rÃ©glementaires et liÃ©es Ã la sÃ©curitÃ©. Tout cela est possible en bÃ¢tissant une infrastructure de gestion des risques au moins aussi flexible que lâ□□infrastructure informatique.Â

Â

[Par **Jay Roxe**, Directeur Marketing, IdentitÃ© et SÃ©curitÃ©, Novell]