***Six Ã©tapes Ã  suivre pour gÃ©rer efficacement les accÃ¨s aux donnÃ©es***
**Internet**
PostÃ© par : JPilo
PubliÃ©e le : 23/11/2011 13:00:00

Des processus bien dÃ©finis de contrÃ´le des transferts de donnÃ©es contribuent Ã  lever les obstacles qui empÃªchent la gouvernance complÃ¨te et dynamique des accÃ¨s aux donnÃ©es. Comme le rappellent certaines failles de sÃ©curitÃ© largement mÃ©diatisÃ©es, la gouvernance des accÃ¨s aux donnÃ©es est une nÃ©cessitÃ© absolue pour les entreprises.

Or, force est de constater des carences en la matiÃ¨re : le contrÃ´le des accÃ¨s aux informations critiques est souvent inefficace et n'a pas la souplesse requise pour s'adapter facilement au changement. Selon un rapport de Gartner sur la sÃ©curitÃ© et la gestion des risques, les dÃ©cisions relatives Ã  l'accÃ¨s aux donnÃ©es doivent Ãªtre fondÃ©es sur une Ã©valuation des risques et des avantages d'un niveau donnÃ© de partage des donnÃ©es, ainsi que des processus, personnes et technologies permettant ce partage en toute sÃ©curitÃ©.

Leader dans le domaine de la gestion des identitÃ©s et des accÃ¨s, **Quest Software** utilise un processus en six Ã©tapes pour guider les Ã©valuations et amÃ©liorer le contrÃ´le des accÃ¨s aux donnÃ©es.

Tweetez : @Quest recommande six mesures pour assurer la gouvernance efficace des accÃ¨s aux donnÃ©es. : /bit.ly/u9ed3l

**Six Ã©tapes pour une meilleure gouvernance :**

***1. RÃ©pertorier les utilisateurs et les ressources :*** cette premiÃ¨re Ã©tape consiste Ã  effectuer un inventaire de l'infrastructure pour rÃ©pertorier les donnÃ©es importantes (ou points d'accÃ¨s Ã  ces donnÃ©es), qui sont souvent Ã©parpillÃ©es sur diverses plates-formes, des pÃ©riphÃ©riques de stockage en rÃ©seau et des sites SharePoint, dans des groupes Active Directory, sur des appareils mobiles, etc. En particulier, il est Ã©galement important d'identifier les sources de donnÃ©es non structurÃ©es ou orphelines.

***2. Classer les donnÃ©es et attribuer des droits d'accÃ¨s*** : les donnÃ©es doivent Ãªtre classÃ©es en fonction de leur confidentialitÃ©, de leur corrÃ©lation avec les rÃ©glementations (par exemple, les numÃ©ros de carte de crÃ©dit), de leur pertinence gÃ©nÃ©rale et des besoins en matiÃ¨re d'archivage. Il faut Ã©galement passer en revue et Ã©valuer les propriÃ©taires des donnÃ©es pour vÃ©rifier leur conformitÃ© par rapport Ã  la politique de sÃ©curitÃ©.

***3. Associer les donnÃ©es Ã  des propriÃ©taires et des approbateurs*** : des propriÃ©taires doivent Ãªtre dÃ©signÃ©s en fonction du rÃ´le, du lieu et d'autres attributs. La sÃ©paration des tÃ¢ches doit Ãªtre prise en considÃ©ration pour assurer la conformitÃ© et la sÃ©curitÃ©.

***4. VÃ©rifier les accÃ¨s :*** planifier l'audit et le reporting des accÃ¨s afin d'assurer leur contrÃ´le continu Ã  l'Ã©chelle de l'entreprise et de garantir leur conformitÃ© et leur sÃ©curitÃ©.

***5. Automatiser les demandes d'accÃ¨s et la rÃ©solution des problÃ¨mes*** : l'automatisation des processus de traitement des demandes d'accÃ¨s en fonction des droits d'accÃ¨s et du rÃ´le du demandeur au sein de l'entreprise est recommandÃ©e pour des raisons de sÃ©curitÃ©. En outre, le traitement automatisÃ© des Ã©carts permet d'Ã©liminer proactivement des menaces ou infractions potentielles.

***6. EmpÃªcher les modifications illicites*** : verrouiller les donnÃ©es, groupes ou droits d'accÃ¨s qui ne doivent jamais Ãªtre modifiÃ©s. Toutes les modifications doivent Ãªtre consignÃ©es dans un rÃ©fÃ©rentiel sÃ©curisÃ© infalsifiable, afin d'assurer l'intÃ©gritÃ© des analyses.

**Protection et gestion proactives des donnÃ©es critiques**

***â¢ La gouvernance automatisÃ©e et multiplate-forme*** des accÃ¨s aux donnÃ©es permet d'Ã©liminer non seulement les obstacles qui empÃªchent l'application des rÃ©glementations, mais Ã©galement les accÃ¨s illicites aux donnÃ©es sensibles stockÃ©es sur des serveurs de fichiers virtuels et physiques, pÃ©riphÃ©riques de stockage en rÃ©seau, sites SharePoint, serveurs de fichiers Windows, etc.

***â¢ Le contrÃ´le efficace des accÃ¨s*** est essentiel pour la rÃ©duction et la prÃ©vention des menaces. Selon l'Ã©dition 2011 du rapport de Verizon sur les failles en matiÃ¨re de protection des donnÃ©es, 86 % des problÃ¨mes de sÃ©curitÃ© peuvent Ãªtre dÃ©tectÃ©s par les entreprises avant qu'un incident ne se produise.

***â¢ La visibilitÃ© complÃ¨te***, Ã  360 degrÃ©s, des accÃ¨s des utilisateurs Ã  l'Ã©chelle de l'entreprise procure aux responsables informatiques, aux dirigeants de l'entreprise et aux propriÃ©taires des donnÃ©es les informations requises pour l'application des politiques et des rÃ©glementations sans impact nÃ©gatif sur les opÃ©rations.

Citation :

â¢ **Nick Nikols**, Vice-PrÃ©sident et Directeur GÃ©nÃ©ral, Identity, Security and Windows Management, Quest Software

Â« *Notre vision de la gouvernance complÃ¨te des accÃ¨s aux donnÃ©es associe la dÃ©couverte, le contrÃ´le et l'automatisation pour aider les dÃ©cideurs au sein des entreprises Ã  dÃ©terminer qui a besoin d'accÃ©der Ã  des donnÃ©es critiques stockÃ©es dans des formats structurÃ©s au sein d'applications et de bases de donnÃ©es ou dans des formats non structurÃ©s au sein de documents et de feuilles de calcul, afin de rÃ©pondre aux besoins en constante Ã©volution de l'entreprise sans compromettre la sÃ©curitÃ© ou la conformitÃ© requise.* Â»