ENTRETIEN AVEC UN ANALYSTE D'IDC

Sally Hudson
Research Director, Security Products and Services

Limiter les risques grâce aux solutions de gouvernance des accès

Mai 2012

Pour les entreprises, la gouvernance des accès fait partie d'une approche intégrée en termes de gouvernance, gestion des risques et conformité (GRC). Selon la définition d'IDC, une approche GRC implique l'adoption d'une vue complète et globale des trois composants (gouvernance, gestion des risques et conformité) dans une optique opérationnelle mais aussi stratégique. Processus permettant de renforcer les opérations, la gestion et les niveaux de performances d'une entreprise tout en limitant les incertitudes, la gouvernance des accès revêt une importance croissante pour les entreprises.

NetIQ a posé les questions suivantes de la part de ses clients à Sally Hudson, Research Director, Security Products and Services chez IDC.

Q. Pourquoi les entreprises doivent-elles développer leurs infrastructures existantes de gestion des identités et des accès (IAM) de manière à y intégrer une gouvernance des accès rigoureuse ?

R. Aujourd'hui, la majorité des systèmes de gestion des identités ou de provisioning déployés ne sont malheureusement connectés qu'à une fraction des systèmes et applications disponibles dans l'entreprise. Les grandes entreprises ont lourdement investi en matière de provisioning informatique, de contrôle d'accès et de sécurité. Selon les données IDC, dans le domaine IAM, le seul revenu des licences et de la maintenance représentait plus de 4 milliards de dollars américains en 2011. Et c'est sans compter les services. Par conséquent, de nombreux responsables informatiques doutent de la nécessité d'installer un composant ou une couche fonctionnelle supplémentaire pour atteindre leurs objectifs.

Cependant, pour respecter les réglementations officielles et sectorielles en matière de conformité, les entreprises ont besoin d'une gouvernance des accès exhaustive. En réalité, beaucoup d'entreprises ne prennent conscience de leur vulnérabilité que lorsque celle-ci est révélée lors d'un audit ou, pire encore, lorsqu'une grave violation des accès est révélée publiquement. Un grand nombre d'entreprises bien connues ont déjà fait la une de l'actualité pour cette raison. Il est d'ailleurs troublant de constater que les entreprises ayant ce triste privilège semblent se renouveler régulièrement.

Par ailleurs, seule une minorité des systèmes de gestion des identités sont capables de traiter les requêtes d'accès. Or, lorsque les utilisateurs peuvent effectuer des demandes d'accès, le centre d'assistance, souvent débordé, peut souffler un peu. La question qui se

pose alors est la suivante : comment assurer l'autonomie des utilisateurs en évitant de compromettre la sécurité du système ou violer les stratégies de contrôle d'accès ? Dans cette situation, une solution de gouvernance des accès à la fois flexible et évolutive permet d'alléger considérablement la tâche du service informatique et de l'entreprise en général. Il faut pour cela réussir à définir une stratégie de privilège minimal pour les utilisateurs, avec suffisamment de flexibilité pour permettre certaines exceptions nécessaires et approuvées. Pour toutes les instances de provisioning et déprovisioning, des rapports doivent être créés automatiquement, de même qu'une attestation de l'autorité appropriée.

Q. Pourquoi les solutions ponctuelles ne produisent-elles pas de résultats satisfaisants dans ce domaine ?

R. Les solutions ponctuelles de gouvernance des identités et des accès sont limitées en matière de provisioning et d'automatisation. Cette limitation peut découler du fait que les solutions ponctuelles sont développées selon un ensemble spécifique de critères. De plus, leur fonctionnalité est souvent dirigée vers certaines plates-formes, voire à des secteurs verticaux. Les sociétés devraient privilégier une solution offrant une plus large assise, capable de fournir des informations centralisées et automatisées qui englobent tous les aspects de l'environnement d'entreprise.

Q. Comment la gouvernance des accès permet-elle de réduire le profil de risque de mon entreprise ?

R. Il est indispensable que les sociétés sachent en permanence qui a accès à quelles données ou informations au sein de l'entreprise. Une surveillance constante est nécessaire pour assurer l'adéquation entre les privilèges d'accès et les stratégies, de même que la certification des transactions. Outre la pertinence de l'accès, la gouvernance des accès permet aux entreprises d'effectuer le suivi de leurs stratégies et de certifier l'accès.

La première étape consiste bien sûr à créer un profil précis indiquant qui peut accéder à quoi. Il s'agit d'une étape essentielle car elle permet aux entreprises de comprendre quels utilisateurs représentent le risque le plus élevé en raison de leur niveau d'accès.

Q. Comment les entreprises peuvent-elles utiliser la gouvernance des accès pour en tirer des renseignements utiles aux processus d'entreprise en général ?

R. La gouvernance des accès permet de créer un entrepôt d'identités où sont stockées les informations relatives aux accès, aux événements, aux droits, etc. À partir de cette riche zone de stockage d'informations, vous pouvez ensuite exécuter des rapports et des analyses. Les données et rapports complets de ce type sont indispensables pour certifier avec précision que le service informatique respecte les procédures requises afin d'assurer la conformité aux réglementations en matière de sécurité et de confidentialité. La collecte de données et la surveillance des accès à des fins d'attestation pourraient sembler constituer une approche a posteriori. En réalité, cette approche est à la fois proactive et prédictive. L'utilisation de contrôles et de données de gouvernance des accès permet aux entreprises de savoir qui a accédé à quelles ressources et à quel moment. Elles peuvent ainsi identifier immédiatement les utilisateurs bénéficiant de privilèges excessifs.

Les violations commises par les utilisateurs sont très souvent involontaires (par exemple dues à des privilèges d'accès excessifs ou à une erreur humaine). Lorsque les gestionnaires sont obligés de procéder manuellement à des attestations des modifications, des erreurs involontaires peuvent également se produire. Dans la plupart des cas, ce processus est trop détaillé et fastidieux pour être géré manuellement sans multiplier les risques d'erreurs.

L'automatisation des attestations et des contrôles de stratégies permet d'identifier les anomalies. Par ailleurs, elle permet aux responsables de la stratégie commerciale et aux

gestionnaires informatiques de travailler ensemble afin de combler les écarts existant entre les stratégies et les privilèges au sein du système.

Q. De quelles fonctions/caractéristiques une bonne solution de gouvernance des accès doit-elle être dotée ?

R. Outre tous les éléments abordés précédemment, la facilité d'utilisation est une qualité essentielle de toute bonne solution de gouvernance des accès. Les attestations reposent en grande partie sur les gestionnaires et responsables commerciaux. Si le logiciel est compliqué ou contraignant, ils éviteront de l'utiliser, ce qui entraînera une augmentation des risques. C'est pourquoi les fonctions et caractéristiques suivantes devraient figurer sur votre liste de la démonstration de faisabilité :

- Logiciel dont l'interface est intuitive et conviviale
- Scores de risque afin d'identifier les zones critiques
- Prise en charge d'une large gamme de plates-formes, bases de données et serveurs Web
- Puissantes fonctions de provisioning automatisé
- Capacité à générer de la valeur rapidement conformément aux objectifs du projet (approche itérative plutôt que de type « big bang »)

Enfin, lors de l'évaluation d'une solution de gouvernance des accès, n'oubliez pas qu'il s'agit d'un processus continu et itératif, qui doit pouvoir évoluer en même temps que les objectifs du projet. Il ne s'agit pas d'un déploiement de type « big bang ». Les processus et stratégies doivent changer au rythme de l'évolution des besoins commerciaux et des impératifs de sécurité et de conformité. La solution de gouvernance des accès doit être en mesure de prendre en charge cette perpétuelle mutation.

À PROPOS DE CETTE ANALYSTE

Sally Hudson est directrice de recherche du groupe Security Products and Services d'IDC, et se concentre sur les produits de gestion des identités et des accès (IAM). Elle analyse et prévoit les tendances du marché de façon à partager une perspective d'expert sur l'évolution du paysage en matière de sécurité. De plus, Mme Hudson mène chaque année de nombreuses études de marché approfondies. Elle travaille à l'élaboration et à la mise en œuvre de stratégies informatiques efficaces en collaboration avec les fournisseurs et les utilisateurs.

À PROPOS DE CETTE PUBLICATION

Cette publication a été réalisée par IDC Go-to-Market Services. En l'absence de mention spécifique au soutien d'un fournisseur, les opinions, analyses et résultats de recherche inclus dans les présentes
proviennent de recherches et d'analyses plus détaillées qui ont été réalisées et publiées de façon indépendante par IDC. Les contenus IDC proposés par IDC Go-to-Market Services sont disponibles dans un large éventail de formats pour distribution par
différentes sociétés. L'octroi d'une licence de distribution de contenu IDC ne signifie pas qu'IDC apporte son soutien au titulaire de licence ou émet une opinion à son sujet.

Siège international : 5 Speen Street, Framingham, MA 01701 États-Unis. Tél. : 508.872.8200 Fax : 508.935.4015
www.idc.com