Business & Decision | avis d'expert

BUSINESS INTELLIGENCE | CUSTOMER INTELLIGENCE | E-BUSINESS | MANAGEMENT CONSULTING

La sécurité des systèmes d'informations : bien gérer les identités et les rôles dans le respect des contraintes réglementaires

*par **Jérôme Chagnoux et Jean-Luc Rizk***
Agence IT, Groupe Business & Decision

Bien gérer l'identité, les accès et les habilitations** de chaque utilisateur s'avère être la bonne méthode pour augmenter le niveau de sécurité global. On constate aujourd'hui que c'est également l'un des axes d'évolution pour le respect des lois et réglementations auxquelles sont soumises les entreprises : **Sarbanes-Oxley, Basel II, LSF…

En effet, le système d'information est aujourd'hui au cœur de l'activité économique de l'entreprise. Le nombre et la diversité des applications sont la réponse de l'entreprise à des contraintes de productivité et d'innovation constante. Au fil du temps, la sécurité du système d'information est devenue vitale, au-delà même de la problématique de sécurité réseau et des télécommunications.

Les solutions apportées par la gestion d'identité

« Qui est qui ? », « qui fait quoi ? », « qui accède à quoi ? », « qui a donné le droit à qui de faire quoi ? »… Avant même de savoir ce qui se passe au sein du système d'information, il est essentiel d'être capable de répondre à ces questions simples, mais souvent oubliées.

Une problématique dont la complexité augmente puisque les applications sont de plus en plus ouvertes aux acteurs de l'entreprise étendue : collaborateurs, prestataires, clients, fournisseurs…

La solution passe par la mise en œuvre d'une architecture basée sur trois éléments essentiels :

- L'élément de base est avant tout un **référentiel qui stocke les composantes de l'identité numérique** : des attributs classiques comme le numéro de téléphone ou la fonction, jusqu'à tout élément permettant de caractériser un individu dans l'organisation : département d'appartenance, sites géographiques, bureaux…
- Des **solutions de synchronisation** complètent cette infrastructure pour garantir l'industrialisation de la mise **à jour intelligente des données**, calée sur des évènements tels que la création d'une entrée dans le système RH, une mutation, l'affectation d'un téléphone…
- Une **infrastructure de gestion des droits d'accès et des habilitations** qui vise à concevoir un outil qui permettra de **structurer la sécurité du système d'information (SI)** autour d'un modèle d'habilitation proche de l'organisation de l'entreprise. Partie intégrante d'une infrastructure de gestion d'identité, elle vient s'appuyer sur le cycle de vie de l'identité pour assurer le provisioning des référentiels utilisateurs des applications du système d'information.

On constate très vite plusieurs avantages à la mise en place d'une telle infrastructure, parmi lesquels :

- **la gestion**, pour un utilisateur donné, de ses **droits d'accès** (à une ressource informatique) et de ses **habilitations**, qui sont généralement liés à son rôle dans l'entreprise (notion de rôle métier) ;
- **la gestion des modifications de périmètre de responsabilités** dans l'applicatif, par un suivi détaillé de l'affectation des habilitations *(« qui a le droit de déléguer quoi »*, « *qui a délégué quoi à qui »*…) ;
- **le suivi des mouvements** d'un utilisateur : la révocation d'habilitations lors du départ ou de la mutation d'une personne, plus communément appelé le « de-provisioning » des utilisateurs ;
- **l'augmentation du niveau de service** rendu aux utilisateurs**.**

Ainsi, le système d'information est équipé d'un **référentiel mutualisé**, garant d'une identité de qualité, de sa traçabilité et de son auditabilité.

Un enjeu majeur : le respect des contraintes réglementaires

Les récents scandales financiers (Enron, Andersen, Worldcom ou Parmalat) ont fait apparaître un manque de contrôle dans les grandes organisations. C'est pour garantir ce contrôle que différentes réglementations nationales et internationales ont été créées avec pour objectif de réformer profondément la gouvernance d'entreprise. Qu'il s'agisse de *Sarbanes-Oxley*, de *Basel II* ou de la *LSF*, tout est organisé par le législateur pour assurer la transparence totale de l'activité financière de l'entreprise, ainsi que la responsabilisation des dirigeants. Les audits (internes et externes) sont devenus un laissez-passer obligatoire pour la réussite économique.

C'est dans ce contexte fortement règlementé que la traçabilité et l'auditabilité prennent tout leur sens. Au-delà d'une documentation fine des processus métiers de l'entreprise, il est avant tout nécessaire d'être capable d'identifier quelles personnes au sein d'une organisation ont tenté d'accéder à des données sensibles non autorisées. Face à ce constat, il est ensuite important de comprendre pourquoi ces tentatives d'accès sont en infraction au regard de la politique de gouvernance ou des contraintes réglementaires en vigueur.

Sans une vue détaillée de l'activité et du comportement de chaque personne, l'entreprise risque un usage frauduleux de son SI (détournement d'informations sensibles, destruction de documents, …) qui peut aboutir à des pertes financières significatives ou l'interruption de son activité économique.

De ce fait, l'entreprise doit **monitorer toute l'activité de son SI** pour identifier et investiguer sur toutes violations volontaires ou accidentelles des règles en vigueur, dans l'objectif final d'être conforme aux contraintes réglementaires.

Les infrastructures de gestion des droits d'accès et des habilitations apportent quelques éléments essentiels pour l'obtention de cette conformité. En s'assurant de l'intégrité des référentiels utilisateurs, il devient plus facile de contrôler les accès (provisioning et dé provisioning des comptes) et d'augmenter le niveau global de sécurité. Par l'adoption d'un modèle d'habilitation métier, l'implémentation des règles de séparation de responsabilités requises devient réalisable au niveau du système d'information.

Il devient ainsi possible d'être partie prenante dans un audit, en fournissant, par exemple, des rapports formatés à l'usage des auditeurs…

L'organisation de l'entreprise au cœur de la problématique

La démarche de mise en place, bien que complexe, se heurte le plus souvent à des contraintes liées à l'**organisation de l'entreprise** : il s'agit d'impliquer chaque acteur du système dans la sécurité par la description de processus génériques de gestion des habilitations et la description de rôles métiers.

L'approche méthodologique nécessaire à l'élaboration d'une telle infrastructure de gestion des habilitations, et notamment des éléments relatifs aux rôles métiers, nécessite une approche pragmatique par itération qui vise à améliorer sans cesse la qualité du système.

Il s'agit ici d'un modèle d'amélioration continue connu sous le nom de *« Roue de Deming »* (ou modèle PDCA). Après la définition des objectifs, des actions sont entreprises pour les atteindre. Ensuite, on vérifie la bonne qualité des résultats, puis on se fixe de nouveaux objectifs pour être toujours totalement efficace.

Un projet de gestion d'identité est donc avant tout un projet *« métier »* fortement lié à l'organisation de l'entreprise dont la réussite est intimement lié à la motivation de chaque acteur. Mené en bonne intelligence avec tous les responsables impliqués dans la conformité aux contraintes réglementaires, il devient un facteur clé de succès des projets de gouvernance d'entreprise.

Contacts *Agence IT*, Groupe Business & Decision

Jean-Luc Rizk – *Directeur d'Agence*
jean-luc.rizk@businessdecision.com

Tél : +33 0(1) 56 21 21 21
Fax : +33 0(1) 56 21 21 22

Jérôme Chagnoux – *Business Developer IAM*
jerome.chagnoux@businessdecision.com

A propos de Business & Decision :

Créé en 1992, Business & Decision est un Groupe international de conseil et d'intégration de systèmes spécialisé en Business Intelligence, Gestion de la Relation Client (CRM) et e-Business. Business & Decision accompagne les entreprises dans la mise en œuvre de systèmes informatiques pour le pilotage des structures et de la performance (reporting, tableaux de bord, consolidation, etc.) ; la connaissance et la gestion du client (outils pour les forces de vente, centres d'appels, gestion de campagnes, CRM analytique) ; et la relation via le Web (portails collaboratifs ou d'entreprises, annuaires et méta-annuaires, e-commerce, knowledge management, Open source…).

Avec plus de 1 800 personnes (en France et dans le Monde) qui développent une approche « projet complet » allant du conseil à la réalisation informatique, Business & Decision est reconnu pour son expertise fonctionnelle et technologique par les plus grands éditeurs de logiciels du marché avec lesquels elle a noué des partenariats. Business & Decision compte aujourd'hui plus de 1 200 clients.

Coté sur Euronext Paris depuis février 2001 (compartiment C / code Isin : FR 00000 7895 8 / mnémonique : BND), Business & Decision fait partie du segment NextEconomy et participe à l'indice IT-Cac (valeurs technologiques).

Pour plus d'informations, consultez les sites Internet : www.businessdecision.com & www.businessdecision.fr

Contact presse :

Isabelle Serra
Responsable communication
Business & Decision
Tél : 01 56 21 21 25
Fax : 01 56 21 21 22
E-mail : isabelle.serra@businessdecision.com