

Risques d'accès non autorisés : les atouts d'une solution IAM

Internet

Posté par : JulieM

Publié le : 4/2/2015 14:27:49

Comment l'entreprise peut-elle réduire ses risques informatiques liés aux droits d'accès des utilisateurs.

Tous les jours, les médias font état d'incidents de sécurité informatique, tels que l'accès non-autorisé aux données de l'entreprise ou la violation de droits d'accès. Dans ce contexte, les principaux analystes (Gartner, KuppingerCole) sont de plus en plus insistants sur la nécessité de déployer un système de gestion des identités et des accès.

Les projets IAM (Identity and Access Management) sont désormais une véritable priorité pour les entreprises de toutes tailles.

Comment l'entreprise peut-elle réduire son niveau de risque lié aux droits d'accès des utilisateurs grâce à l'approche IAM?

1-La visibilité est renforcée

Il est vital que l'entreprise sache à tout instant quel compte utilisateur appartient à quel employé. L'entreprise doit pouvoir accéder en temps réel aux informations de droits d'accès de systèmes tels qu'Active Directory, Lotus ou SAP.

Les fonctionnalités d'Access Intelligence, intégrées aux systèmes IAM les plus sophistiqués, lui permettent de s'assurer que toutes les informations liées aux accès (utilisateurs, rôles, autorisations) sont capturées et documentées.

Ces fonctions de monitoring peuvent, pour les cas les plus extrêmes, nécessiter une historisation continue, de sorte que toute modification effectuée, dans le passé ou en temps réel, soit identifiée, tracée et consultable en toute simplicité.

Ainsi l'entreprise peut à tout instant répondre à la question « Qui a donné accès à quelle ressource et quand ? ». C'est pourquoi les meilleures solutions du marché incluent un moteur de workflow pour automatiser et tracer les demandes d'accès, et faciliter les audits.

Par ailleurs, les droits d'accès devraient être régulièrement recertifiés pour s'assurer que les employés ont les droits nécessaires et suffisants pour leurs responsabilités, et que les personnes ayant quitté l'entreprise n'accèdent plus à ses différents systèmes et applications. Pour cela, une interface graphique conviviale facilitera les tâches de recertification qui incombent aux responsables d'équipes.

2-Les directions métiers sont impliquées

Les solutions IAM d'aujourd'hui permettent aux équipes informatiques, aux responsables sécurité (RSSI) et aux directions métiers de partager la gestion des habilitations pour gagner en efficacité.

Les systèmes les plus avancés réunissent les utilisateurs métiers et les responsables informatiques, dans la mesure où ils sont faciles à utiliser, alignés avec les besoins métiers, et intégrés aux organisations les plus complexes. Ce partage des tâches simplifie l'administration des droits et réduit donc les risques potentiels.

3-La règle de séparation des tâches est appliquée

Pour éviter qu'un utilisateur enfreigne les directives internes, l'entreprise devrait s'assurer qu'aucun employé ne cumule de droits d'accès allant au-delà du périmètre nécessaire à l'exécution de leur fonction. Chaque employé ne devrait disposer que des droits d'accès correspondants à ses responsabilités.

Les solutions avancées d'IAM incluent cette stricte séparation des tâches (SOD - Segregation of Duties). Et pour renforcer la sécurité, les rôles et droits d'accès sont automatiquement contrôlés par des vérifications croisées.

4-Les droits d'accès sont définis en fonction des rôles

Créer des autorisations d'accès basées sur les rôles (RBAC - Role-Based Access Control) réduit le risque d'erreur inhérent aux autorisations manuelles. Chaque décision d'accès est basée sur le rôle auquel l'utilisateur est attaché. Les utilisateurs exerçant des fonctions similaires peuvent être regroupés sous le même rôle.

Cette démarche peut d'ailleurs inciter l'entreprise à définir plus largement l'ensemble des rôles nécessaires pour ses activités. Les solutions IAM d'aujourd'hui incluent des autorisations basées sur les rôles qui permettent de relier les informations utilisateurs d'ordre techniques et organisationnelles. Elles donnent à l'entreprise la flexibilité nécessaire pour créer à la fois des rôles statiques et dynamiques.

5-La conformité informatique est assurée

Assurer la conformité de ses systèmes informatiques pour répondre aux obligations légales est une démarche complexe mais nécessaire. Pour mener à bien cet objectif, l'entreprise privilégiera un outil de gestion des accès conçu en parfaite adéquation avec ces normes et réglementaires dans le but de faciliter les audits tout en assurant un niveau de sécurité maximal.

En particulier, pour se conformer avec plus de facilité à la norme ISO 2700X, l'entreprise s'appuiera sur une solution qui intègre des tests de sécurité et des procédures d'audit dynamique en ligne avec les exigences de la norme. Des procédures de contrôle personnalisées pourront également être définies pour faire appliquer la réglementation interne de l'entreprise.

6-Les processus de gouvernance sont confortés

Afin de mettre en œuvre une gouvernance informatique efficace, l'entreprise cherche à connaître les risques potentiels liés aux accès des utilisateurs. À l'aide de rapports dynamiques et d'une interface graphique optimisée pour manipuler les données, l'analyse intelligente des accès associés aux utilisateurs permet d'identifier d'éventuelles failles et le niveau de risque généré.

Un grand nombre de rapports standards doivent être inclus. Ces tableaux de bords pourront également être personnalisés afin d'offrir le niveau de détail nécessaire en fonction de l'utilisation qui en est faite par les auditeurs internes ou externes, les responsables sécurité informatique, ou la Direction.

D'ailleurs, l'entreprise aura d'autant plus de facilité à contrôler la conformité des accès si la solution permet de centraliser l'exécution des audits au profit d'utilisateurs non-informaticiens comme les auditeurs ou les responsables métiers. Ces outils d'analyse favorisent ainsi la correction rapide d'erreur d'autorisation, pour une gouvernance améliorée et un niveau de risque réduit.

S'appuyer sur une solution IAM basée sur les risques aide l'entreprise à analyser puis résoudre les problèmes potentiels avec plus de rapidité.

Les outils d'IAM sophistiqués comme SAM Enterprise Identity Manager et Garancy Access Intelligence Manager de Beta Systems permettent aux directeurs métier, aux responsables informatiques et aux auditeurs de contribuer à minimiser les risques à l'échelle de l'entreprise, confirme Bastien MEAUX, Responsable Marketing Beta Systems Software France