Risques dâ□□accÃ¨s non autorisÃ©s : les atouts dâ□□une solution IAM
Internet
PostÃ© par : JulieM
PubliÃ©e le : 5/2/2015 11:00:00

Comment l'entreprise peut-elle rÃ©duire ses risques informatiques liÃ©s aux droits dâ□□accÃ¨s des utilisateurs.
Tous les jours, les mÃ©dias font Ã©tat d'incidents de sÃ©curitÃ© informatique, tels que l'accÃ¨s non-autorisÃ© aux donnÃ©es de l'entreprise ou la violation de droits d'accÃ¨s. Dans ce contexte, les principaux analystes (Gartner, KuppingerColeâ□¦) sont de plus en plus insistants sur la nÃ©cessitÃ© de dÃ©ployer un systÃ¨me de gestion des identitÃ©s et des accÃ¨s.

Les projets IAM (Identity and Access Management) sont dÃ©sormais une vÃ©ritable prioritÃ© pour les entreprises de toutes tailles.

Comment l'entreprise peut-elle rÃ©duire son niveau de risque liÃ© aux droits dâ□□accÃ¨s des utilisateurs grÃ¢ce Ã l'approche IAM?

1-La visibilitÃ© est renforcÃ©e

Il est vital que l'entreprise sache Ã tout instant quel compte utilisateur appartient Ã quel employÃ©. L'entreprise doit pouvoir accÃ©der en temps rÃ©el aux informations de droits d'accÃ¨s de systÃ¨mes tels quâ□□Active Directory, Lotus ou SAP.

Les fonctionnalitÃ©s dâ□□Access Intelligence, intÃ©grÃ©e aux systÃ¨mes IAM les plus sophistiquÃ©s, lui permettent de sâ□□assurer que toutes les informations liÃ©es aux accÃ¨s (utilisateurs, rÃ´les, autorisationsâ□¦) sont capturÃ©es et documentÃ©es.

Ces fonctions de monitoring peuvent, pour les cas les plus extrÃªmes, nÃ©cessiter une historisation continue, de sorte que toute modification effectuÃ©e, dans le passÃ© ou en temps rÃ©el, soit identifiÃ©e, tracÃ©e et consultable en toute simplicitÃ©.

Ainsi lâ□□entreprise peut Ã tout instant rÃ©pondre Ã la question Â« Qui a donnÃ© accÃ¨s Ã quelle ressource et quand ? Â». Câ□□est pourquoi les meilleures solutions du marchÃ© incluent un moteur de workflow pour automatiser et tracer les demandes d'accÃ¨s, et faciliter les audits.

Par ailleurs, les droits d'accÃ¨s devraient Ãªtre rÃ©guliÃ¨rement recertifiÃ©s pour s'assurer que les employÃ©s ont les droits nÃ©cessaires et suffisants pour leurs responsabilitÃ©s, et que les personnes ayant quittÃ© l'entreprise nâ□□accÃ¨dent plus Ã ses diffÃ©rents systÃ¨mes et applications. Pour cela, une interface graphique conviviale facilitera les tÃ¢ches de recertification qui incombent aux responsables dâ□□Ã©quipes.

2-Les directions mÃ©tiers sont impliquÃ©es

Les solutions IAM d'aujourd'hui permettent aux Ã©quipes informatiques, aux responsables sÃ©curitÃ© (RSSI) et aux directions mÃ©tiers de partager la gestion des habilitations pour gagner en efficacitÃ©.

Les systÃ¨mes les plus avancÃ©s rÃ©unissent les utilisateurs mÃ©tiers et les responsables informatiques, dans la mesure oÃ¹ ils sont faciles Ã utiliser, alignÃ©s avec les besoins mÃ©tiers, et intÃ©grÃ©s aux organisations les plus complexes. Ce partage des tÃ¢ches simplifie l'administration des droits et rÃ©duit donc les risques potentiels.

3-La rÃ¨gle de sÃ©paration des tÃ¢ches est appliquÃ©e

Pour Ã©viter quâ□□un utilisateur enfreigne les directives internes, lâ□□entreprise devrait s'assurer quâ□□aucun nâ□□employÃ© ne cumule de droits dâ□□accÃ¨s allant au-delÃ du pÃ©rimÃ¨tre nÃ©cessaire Ã lâ□□exÃ©cution de leur fonction. Chaque employÃ© ne devrait disposer que des droits d'accÃ¨s correspondants Ã ses responsabilitÃ©s.

Les solutions avancÃ©es d'IAM incluent cette stricte sÃ©paration des tÃ¢ches (SOD - Segregation of Duties). Et pour renforcer la sÃ©curitÃ©, les rÃ´les et droits dâ□□accÃ¨s sont automatiquement contrÃ´lÃ©s par des vÃ©rifications croisÃ©es.

4-Les droits dâ□□accÃ¨s sont dÃ©finis en fonction des rÃ´les

CrÃ©er des autorisations d'accÃ¨s basÃ©es sur les rÃ´les (RBAC - Role-Based Access Control) rÃ©duit le risque d'erreur inhÃ©rent aux autorisations manuelles. Chaque dÃ©cision d'accÃ¨s est basÃ©e sur le rÃ´le auquel l'utilisateur est attachÃ©. Les utilisateurs exerÃ§ant des fonctions similaires peuvent Ãªtre regroupÃ©s sous le mÃªme rÃ´le.

Cette dÃ©marche peut dâ□□ailleurs inciter lâ□□entreprise Ã dÃ©finir plus largement lâ□□ensemble des rÃ´les nÃ©cessaires pour ses activitÃ©s. Les solutions IAM d'aujourd'hui incluent des autorisations basÃ©es sur les rÃ´les qui permettent de relier les informations utilisateurs dâ□□ordre techniques et organisationnelles. Elles donnent Ã lâ□□entreprise la flexibilitÃ© nÃ©cessaire pour crÃ©er Ã la fois des rÃ´les statiques et dynamiques.

5-La conformitÃ© informatique est assurÃ©e

Assurer la conformitÃ© de ses systÃ¨mes informatiques pour rÃ©pondre aux obligations lÃ©gales est une dÃ©marche complexe mais nÃ©cessaire. Pour mener Ã bien cet objectif, lâ□□entreprise privilÃ©giera un outil de gestion des accÃ¨s conÃ§u en parfaite adÃ©quation avec ces normes et rÃ©fÃ©rentiels dans le but de faciliter les audits tout en assurant un niveau de sÃ©curitÃ© maximal.

En particulier, pour se conformer avec plus de facilitÃ© Ã la norme ISO 2700X, lâ□□entreprise sâ□□appuiera sur une solution qui intÃ¨gre des tests de sÃ©curitÃ© et des procÃ©dures d'audit dynamique en ligne avec les exigences de la norme. Des procÃ©dures de contrÃ´le personnalisÃ©es pourront Ã©galement Ãªtre dÃ©finies pour faire appliquer la rÃ¨glementation interne de lâ□□entreprise.

6-Les processus de gouvernance sont confortÃ©s

Afin de mettre en Å□uvre une gouvernance informatique efficace, lâ□□entreprise cherche Ã connaÃ®tre les risques potentiels liÃ©s aux accÃ¨s des utilisateurs. A lâ□□aide de rapports dynamiques et dâ□□une interface graphique optimisÃ©e pour manipuler les donnÃ©es, lâ□□analyse intelligente des accÃ¨s associÃ©s aux utilisateurs permet dâ□□identifier dâ□□Ã©ventuelles failles et le niveau de risque gÃ©nÃ©rÃ©.

Un grand nombre de rapports standards doivent Ãªtre inclus. Ces tableaux de bords pourront Ã©galement Ãªtre personnalisÃ©s afin dâ□□offrir le niveau de dÃ©tail nÃ©cessaire en fonction de lâ□□utilisation qui en est faite par les auditeurs internes ou externes, les responsables sÃ©curitÃ© informatique, ou la Direction.

Dâ□□ailleurs, lâ□□entreprise aura dâ□□autant plus de facilitÃ© Ã contrÃ´ler la conformitÃ© des accÃ¨s si la solution permet de dÃ©centraliser lâ□□exÃ©cution des audits au profit dâ□□utilisateurs non-informaticiens comme les auditeurs ou les responsables mÃ©tiers. Ces outils dâ□□analyse favorisent ainsi la correction rapide d'erreur d'autorisation, pour une gouvernance amÃ©liorÃ©e et un niveau de risque rÃ©duit.

S'appuyer sur une solution IAM basÃ©e sur les risques aide lâ□□entreprise Ã analyser puis rÃ©soudre les problÃ¨mes potentiels avec plus de rapiditÃ©.

Les outils d'IAM sophistiquÃ©s comme SAM Enterprise Identity Manager et Garancy Access Intelligence Manager de Beta Systems permettent aux directeurs mÃ©tiers, aux responsables informatiques et aux auditeurs de contribuer Ã minimiser les risques Ã l'Ã©chelle de l'entreprise, confirme Bastien MEAUX â□□ Responsable Marketing Beta Systems Software France