

9 conseils pour projet d'Identity and Access Management

Info

Posté par : JulieM

Publié le : 17/6/2015 11:00:00

De plus en plus d'incidents de sécurité informatiques impactent les entreprises, quels que soient leur secteur, leur taille, ou leur activité. Accidents non-autorisés, usurpations d'identités, fuites de données; les entreprises ne peuvent plus se permettre d'ignorer le risque de cyberattaques, ni partir du principe que les attaquants ne parviendront jamais à pénétrer le système d'information.

C'est pourquoi les principaux analystes (KuppingerCole, Pierre Audouin Conseil, Gartner) insistent sur la nécessité de déployer un système de gestion des identités et des accès pour compléter l'arsenal des mesures de sécurisation du système d'information de l'entreprise. Les projets IAM (Identity and Access Management) sont désormais une véritable priorité pour quiconque souhaite renforcer sa cybersécurité.

Pour autant, force est de constater que nombre d'initiatives sont freinées par les échecs rencontrés par d'autres entreprises. Il est donc capital de bien préparer son projet, tant sous ses facettes techniques que métiers ou organisationnelles. Voici quelques bonnes pratiques simples mais souvent négligées, qui permettent de mettre toutes les chances de son côté pour réussir son projet IAM.

Constituer une équipe projet mixte IT & Métier

Un projet IAM est un projet transversal qui requiert de solliciter de nombreux acteurs de l'entreprise (classiquement la DSI, mais également les RH et les directions métiers). Sous-estimer la nécessité de les impliquer peut suffire à faire échouer votre projet. En effet, votre projet ne peut être conduit uniquement sous l'angle technique.

Il est nécessaire d'obtenir l'adhésion et la coopération des directions métiers pour mobiliser les sachants autour du projet et pouvoir s'appuyer sur leurs connaissances des processus métiers de l'entreprise et de sa structure organisationnelle.

Définir la gouvernance et les objectifs du projet

Un projet IAM sans accords de gouvernance entre les parties prenantes et sans objectifs clairement définis arrive rarement à terme. Vous devrez en premier lieu déterminer les rôles et les responsabilités de chacun ainsi que les étapes de déploiement.

L'atteinte de vos objectifs implique un pilotage et un contrôle rigoureux ainsi qu'une étroite collaboration entre l'équipe projet et les consultants de l'éditeur IAM. Assurez-vous que les spécifications et objectifs sont mutuellement compris et documentés avant que ne commence le déploiement. Toute modification ultérieure tendrait le projet en temps et en coût d'installation de manière disproportionnée.

Réguler le sur-mesure au minimum

Lorsque vous choisissez une solution, les systèmes IAM standards et préconfigurés représentent la meilleure stratégie, notamment parce que cette approche capitalise l'expérience terrain acquise par l'éditeur IAM grâce à ses précédents déploiements et qu'elle simplifie grandement l'intégration de nouvelles fonctions au fur et à mesure de l'arrivée de nouvelles versions du logiciel.

Abandonner l'offre standard pour un système hautement personnalisé ne devrait être

qu'exceptionnel. Les produits standards de l'éditeur réduisent les coûts de mise en œuvre et de maintenance, et accélèrent la mise en production.

Déployer par étapes

Soyez pragmatique : vouloir déployer la solution IAM sur un large périmètre technique et fonctionnel peut enliser le projet. Privilégiez une approche quick-win en déployant par étapes, avec des objectifs intermédiaires réalisables. En limitant volontairement le périmètre initial à un nombre restreint de systèmes-cibles, d'utilisateurs et de fonctionnalités, vous obtiendrez des résultats plus rapidement, parfois en quelques mois. Ces premiers retours sur investissement vous aideront à renforcer l'adhésion de l'entreprise, à obtenir des budgets supplémentaires et ainsi à étendre le périmètre du projet.

Connecter les systèmes RH

Les évolutions de personnel (nouvel arrivant, départ, mobilité...) peuvent être signalées aux départements informatiques ou aux ressources humaines, avec un certain retard, voire pas du tout. Ces complications prennent davantage d'ampleur lorsque les tâches d'administration du personnel sont réalisées manuellement ou de manière décentralisée.

C'est pourquoi, dans un premier temps, la principale source de données RH doit être connectée de manière automatisée au système IAM, avec la clé des bénéfices rapidement quantifiables : accès simplifiés, gain de productivité, satisfaction des utilisateurs.

Nettoyer les données d'IAM

La qualité des données est la clé de tout projet IAM réussi. Mais très souvent, les données des droits accumulées ne sont plus maintenues depuis longtemps, et peuvent être désordonnées. En conséquence, des liens entre comptes et utilisateurs sont manquants, des comptes sont orphelins, d'autres sont erronés, etc...

C'est pourquoi un projet IAM commence nécessairement par la consolidation des identités des utilisateurs (user-ID). Dans cette étape, les comptes utilisateurs sont affectés aux personnes auxquelles ils correspondent dans le référentiel des identités. Rapidement, ce nettoyage montre un premier avantage : la consolidation des user-IDs réduit les comptes orphelins.

Déployer les rôles

Un rôle est un ensemble de droits d'accès individuels nécessaires pour une fonction particulière ou une tâche dans l'entreprise. Il est intimement lié aux métiers et aux processus propres à l'organisation. Les « groupes » de droits d'accès, appelés « rôles », réduisent significativement les efforts d'administration. Ils sont la clé pour l'automatisation des processus et la mise en place de règles de non-cumul de certains droits (Segregation of Duties ou SoD).

Mais la mise en œuvre des rôles exige plus qu'une simple définition de groupes de droits d'accès. Les rôles sont des objets vivants. Ils ont besoin d'être mis à jour et maintenus en permanence. Il est important de désigner un « propriétaire » pour chaque rôle ; celui-ci sera le garant des évolutions du rôle. Par conséquent, les rôles devront être revus périodiquement pour s'adapter aux modifications d'organisations ou aux changements de systèmes informatiques.

Introduire l'évaluation du risque

Les systèmes IAM fournissent une quantité considérable de données qu'il est nécessaire de traiter pour faire apparaître les éléments les plus risqués. L'identification et l'évaluation de ces risques est un puissant outil pour classer les données d'accès, telles que les utilisateurs, les rôles et les comptes, en fonction du niveau de risques potentiels. Cependant, mettre en œuvre une mesure du risque pour l'ensemble de votre structure de droits d'accès demande du temps et des ressources.

En utilisant une approche top-down (du haut de la pyramide vers la base), vous pouvez rapidement obtenir de premières analyses de risque, en les classant par catégorie, et par score. Vous profiterez de la durée du projet pour étendre progressivement la portée de ces évaluations.

Fournir rapidement les principales fonctionnalités demandées par les métiers

Gardez à l'esprit que même si les systèmes IAM sont principalement sponsorisés par la direction informatique et par les auditeurs, les directions métiers sont elles aussi demandeuses. Présenter rapidement des premiers résultats concrets à votre direction générale peut vous permettre de gagner l'adhésion de l'ensemble de l'entreprise.

Pour cela, focalisez-vous d'abord sur les premières étapes du projet sur les fonctionnalités métiers destinées à faciliter la vie des utilisateurs finals : par exemple, un portail web pour re-certifier les droits de certaines personnes, ou un workflow pour automatiser l'approbation des demandes de droits. La satisfaction des utilisateurs métiers est un indicateur clé pour démontrer la réussite de votre projet IAM, a commenté Bastien Meaux, Responsable Marketing, Beta Systems.