Business

Cet article appartient à la chaîne thématique **Gestion des Identités et des Accès**.

# IAM : dépenser moins pour gagner plus

*Par **Bruno Vincent**, le 27 oct 2008 à 20:49:53.*

**Une phrase d'Eric Domage, d'IDC, interpelait récemment décideurs et acteurs du marché sur l'importance des coûts et le peu de ROI découlant des projets d'IAM. Bruno Vincent nuance voire réfute en partie, ces propos.**

«***Un projet d'IAM, c'est cher, long et peu profitable***». Il va s'en dire que pour bien des acteurs de l'IAM (Identity & Access Management, soit Gestion des Identités et des Accès, en français), cette petite phrase n'est pas passée inaperçue ! Et pourtant, il est vrai que dans le petit monde des consultants et des éditeurs spécialisés, tout le monde connaît au moins un projet de gestion des identités patinant depuis des mois dans la semoule d'un déploiement chaotique ou d'un cahier des charges hasardeux. Pour autant, une fois ce constat effectué, faut-il jeter le bébé de l'IAM avec l'eau du bain des problèmes de la DSI ? Clairement non. L'IAM ne porte pas intrinsèquement le poids du coût, de la lenteur et du peu de retour sur investissement. Tout comme l'EAI, la SOA ou la gouvernance de la donnée ne les portent pas non plus, et pourtant ce même petit monde des consultants et des éditeurs spécialisés pourrait également citer une ribambelle de projets sclérosés sur ces thématiques. Il convient donc de regarder le sujet de plus près, d'une part en identifiant ce qui ne marche pas chez les uns, et d'autre part en proposant des méthodes ou des alternatives qui marchent chez les autres.

**Première question : un projet d'IAM est-il nécessairement cher ?** Il est vrai qu'un décideur débutant son analyse sous l'angle du coût logiciel aura de quoi être surpris par les tarifs pratiqués par quelques-uns des grands éditeurs du marché. Après tout, comme son nom l'indique, l'IAM ne fait que gérer et utiliser des données d'identités somme toute assez sommaires (ex : logins, rôles, place dans l'organisation etc.). Pas de CRM, pas de système RH, pas d'ERP, et pourtant les zéros ont tendance à rapidement s'accumuler sur les propositions commerciales. S'il ne s'agit évidemment pas de rentrer dans une bataille de chapelles ou dans une grande croisade contre les logiciels propriétaires que ces éditeurs représentent, il convient de rappeler (ou d'apprendre) que l'offre de gestion des identités et des accès ne se limite pas à un simple quart de carré du Gartner. De l'Open Source "communautaire" (ex : Apache Directory Project, CAS, Spring-Security, OpenID) à l'Open Source "éditeur" (ex : Sun Java System Identity Management), en passant par des acteurs de niche (ex : Atlassian Crowd, ManageEngine PasswordManager) - certes centrés sur des problématiques ciblées, mais proposant des solutions largement moins coûteuses et tout aussi interopérables - l'offre globale se révèle être un peu plus large que certaines "photos" du marché voudraient bien le faire croire.

**Deuxième question : un projet d'IAM est-il nécessairement long ?** Et on serait tenté de dire, pour compléter le point précédent, « *c'est surtout cher parce que c'est long !* ». Car si le coût logiciel est une composante du coût global, il s'accompagne systématiquement d'un fort coût humain (en jours hommes donc), tant en termes de prestations externes (consultants, intégrateurs spécialisés etc.) que d'utilisation des ressources internes (MOA, MOE, RSSI etc.) de l'entreprise. Mais pourquoi donc certains projets d'IAM s'enlisent-ils ? Le plus souvent, et comme dans d'autres secteurs, par manque de méthode et de concertation. Dans certaines organisations, le sujet est en effet encore cloisonné à une sphère de personnes isolées et/ou ne le traitant que sous l'angle technique de la sécurité. Dans d'autres, l'IAM est bien compris dans sa globalité et procède également bien d'une démarche d'entreprise collaborative, mais ne dispose pas d'une feuille de route pragmatique pour assurer son déploiement. Du coup les projets se chevauchent, et l'IAM patine.

Un schéma directeur de sécurité applicative ou de gestion des identités, n'a pourtant de sens que s'il s'accompagne d'une roadmap réaliste et basée sur deux éléments essentiels :

- les besoins métier
- le respect des priorités issues de l'analyse des risques (le plus souvent menée par le RSSI)

Dans le premier cas, il s'agit de privilégier les « *quick wins* » à (forte) valeur ajoutée pour le métier, comme par exemple un SSO pour les applications B2C Internet accédées par les clients finaux. Outre la valeur fonctionnelle apportée aux applications, de tels « *quick wins* » favorisent également l'adhésion du métier et sa transformation en sponsor de poids pour la poursuite des autres thématiques d'IAM. Dans le second cas, il s'agit de mettre l'effort sur les risques avérés ou potentiels les plus dommageables pour l'entreprise, comme par exemple la possibilité de modifier les données de l'application «

CARTES BLANCHES

IAM : dépenser moins pour gagner plus
Bruno Vincent

Une phrase d'Eric Domage, d'IDC, interpelait récemment décideurs et acteurs du marché sur l'importance des coûts et le peu de ROI découlant des projets d'IAM. Bruno Vincent nuance voire réfute en partie, ces propos.

Organisation et sécurité: en finir avec le cloisonnement !
Bruno Vincent

DSI,RSSI et Métiers ont encore du mal à collaborer efficacement. Pourtant, l'organisation s'avère être, une fois de plus, la pierre angulaire d'un Système d'Information sûr et aux coûts maîtrisés.

Les RSSI du monde bancaire à l'aube d'une vague de démissions ?
Monsieur RSSI

Rien ne semble changer en matière de risques et sécurité dans le monde bancaire. Constat désabusé et inquiet d'un RSSI du secteur.

Rififi en vue chez les identités
Bruno Vincent

Alors qu'OpenID attise l'intérêt des géants de l'informatique, l'acquisition de Credentica par Microsoft laisse augurer d'une possible guerre des « standards » en matière de gestion des identités sur le Web.

>> Plus de Cartes Blanches

Les thématiques

Quel socle de connaissances pour le RSSI ?
Les services managés de sécurité à l'age adulte
Les botnets se mettent au Web 2.0
Antivirus : la révolution *in the cloud*

*compte de résultat* » avec un simple login/mot de passe (le *deprovisioning* des comptes Exchange n'est alors pas oublié pour autant, mais bien positionné sur un semestre ultérieur !).

**Troisième question : un projet d'IAM ne peut-il pas être profitable ?** L'argument de non profitabilité ne peut être compris - et probablement accepté - qu'en le replaçant sur l'un des axes historiques de motivation des projets de *provisioning*, à savoir la diminution des coûts liés au *help-desk*. En clair, plutôt que de payer un *help-desk* ou une équipe d'administrateurs à créer régulièrement, supprimer périodiquement, et débloquer quotidiennement des comptes, la DSI préfère investir dans un outil automatisant ces tâches en lieu et place des humains. De ce seul point de vue, et après quelques années de retours d'expériences, il s'avère assez clair que toutes les entreprises n'y ont pas trouvé leurs comptes. Pour autant, il ne s'agit là que d'un des axes de motivation de ces projets, et en cette fin d'année 2008, les DSI sont largement aussi désireuses de répondre à des impératifs de conformité réglementaire (SOX, PCI-DSS etc.), ainsi que de réduire les failles de sécurité que l'affaire Kerviel a dévoilé au grand jour. Sur ce dernier point, la question du ROI de l'IAM rejoint d'ailleurs l'éternel débat, plus général, sur le ROI de la sécurité informatique. Les uns le jugent calculable, les autres pensent que la question est sans fondement. Pour ce qui est de l'IAM, et aux vues des affaires ayant défrayé la chronique cette année, on ne peut pourtant s'empêcher de penser à la fameuse phrase de Dennis Hoffman (RSA, EMC Group): « *The day before a breach, the ROI is zero. The day after, it is infinite* » (en français, « *La veille d'un incident, le retour sur investissement d'un système de sécurité est nul. Le lendemain, il est infini*. »)


**A Propos de l'Auteur**

Bruno Vincent est co-fondateur du cabinet de conseil ITekia, spécialiste de l'architecture, du pilotage et de la sécurité des Systèmes d'Information.

Diplômé de l'université britannique d'Aston et de l'Ecole Nationale Supérieure d'Informatique pour l'Industrie et l'Entreprise (ENSIIE), Bruno Vincent a débuté sa carrière chez EADS Sycomore, puis a rejoint le cabinet Octo Technology où il y a dirigé l'offre sécurité. En 2008, il cofonde ITekia et en assure la Direction Technique.

Bruno Vincent a coécrit l'ouvrage "*Gestion des Identités : Une Politique pour le Système d'Information*" et enseigne l'architecture de SI à l'Ecole Nationale Supérieure de Techniques Avancées (ENSTA).