

Anticiper les risques avec la gestion des rôles

SÉCURITÉ DES ACCÈS. Le problème des habilitations est souvent laissé de côté faute d'avoir réussi à établir la passerelle entre directions métier et DSI. Méthodes et outils tentent d'apporter des solutions.

Glossaire

Gestion d'identité : solution logicielle qui permet de prendre en main la création d'identités informatiques via un système de workflow souvent associé, en fin de parcours, à des fonctionnalités de provisioning.

RACF (Resource Access Control Facility) : Créé en 1976, ce programme de protection des accès propose de gérer les accès mainframe par type d'utilisateur, type de groupe et type de ressource.

Role mining : solution logicielle qui effectue de façon automatique une découverte de rôles métier à partir de l'analyse complète des habilitations et des accès informatiques existant dans l'entreprise.

SOD (Segregation Of Duties) : séparation des tâches ou droits. Concept qui consiste à intégrer en dur l'impossibilité de cumuler certaines tâches au sein d'un même rôle.

Détournements de fonds, fraudes, abus de biens sociaux... Mises entre de mauvaises mains, certaines habilitations peuvent avoir des conséquences désastreuses. « *Il y a des rôles qui ne se cumulent pas* », assure Emmanuel Antigac, de Securway. Si cela paraît évident, la mise en application d'un tel constat ne l'est pas pour autant. Et pour cause. Les circuits de validation passent aujourd'hui, dans presque 100% des cas, par des circuits informatiques balisés par des affectations de droits dont la responsabilité incombe à celui qui maîtrise l'outil : le service informatique. Et c'est là que le bât blesse. Car, s'il est bien une problématique à laquelle le département informatique ne peut répondre, c'est celle des habilitations métier. Un administrateur système n'est pas censé savoir que pour la comptabilité fournisseur, il faut distinguer l'acheteur du payeur. Les erreurs deviennent ainsi monnaie courante, ouvrant ainsi une large porte à des infrac-

Des habilitations

UN RISQUE

Le flux d'achat met en parallèle deux processus métier distincts, ayant chacun sa propre séquence d'activités. Un salarié qui a les autorisations pour commander, réceptionner et inventorier des articles peut, par exemple, acheter 10 ordinateurs, en déclarer un perdu en stock et le prendre pour lui. Le vol passe ainsi inaperçu. Un salarié qui a les autorisations pour gérer les fournisseurs et les payer n'a qu'à créer un fournisseur écran, saisir son RIB et se régler ainsi des factures.

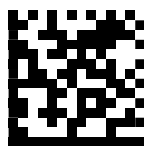
UNE SOLUTION

Les habilitations ont une granularité bidimensionnelle : elles donnent accès à des activités déterminées sur des périmètres organisationnels délimités. Elles sont contenues dans des rôles. Ici les rôles A et B sont incompatibles et doivent être assignés à deux personnes différentes. Aucun des deux utilisateurs ne pourra de la sorte abuser du système.

tions souvent difficiles à tracer. De célèbres affaires sont venues tirer la sonnette d'alarme. L'Etablissement français du sang et Cryospace (tous deux en environnement SAP) se retrouvaient confrontés à des détournements importants : 8 millions pour le premier et 13 pour le second. Pour la même raison : une séparation des droits non appliquée et un salarié qui effectue deux opérations cloisonnées dans l'organisationnel mais pas dans l'opérationnel.

Avant l'outil, une méthode

En réponse à cela, des normes sont d'abord apparues pour imposer aux entreprises des procédures de bonne conduite. Désormais, des méthodes et des outils les



2 QUESTIONS À...



Alexandre Garret,
directeur
des opérations
chez Atheos

Quelles sont les entreprises concernées ?

« Potentiellement toutes, mais cela nécessite quelques prérequis. Notamment, il faut que la gestion des identités soit déjà un minimum outillée. Attention, il ne s'agit pas de dire que cette dernière doit être aboutie, mais au moins entamée pour pouvoir commencer la définition des rôles. Notons cependant que les entreprises qui se sont les premières investies sont celles assujetties à des réglementations spécifiques. »

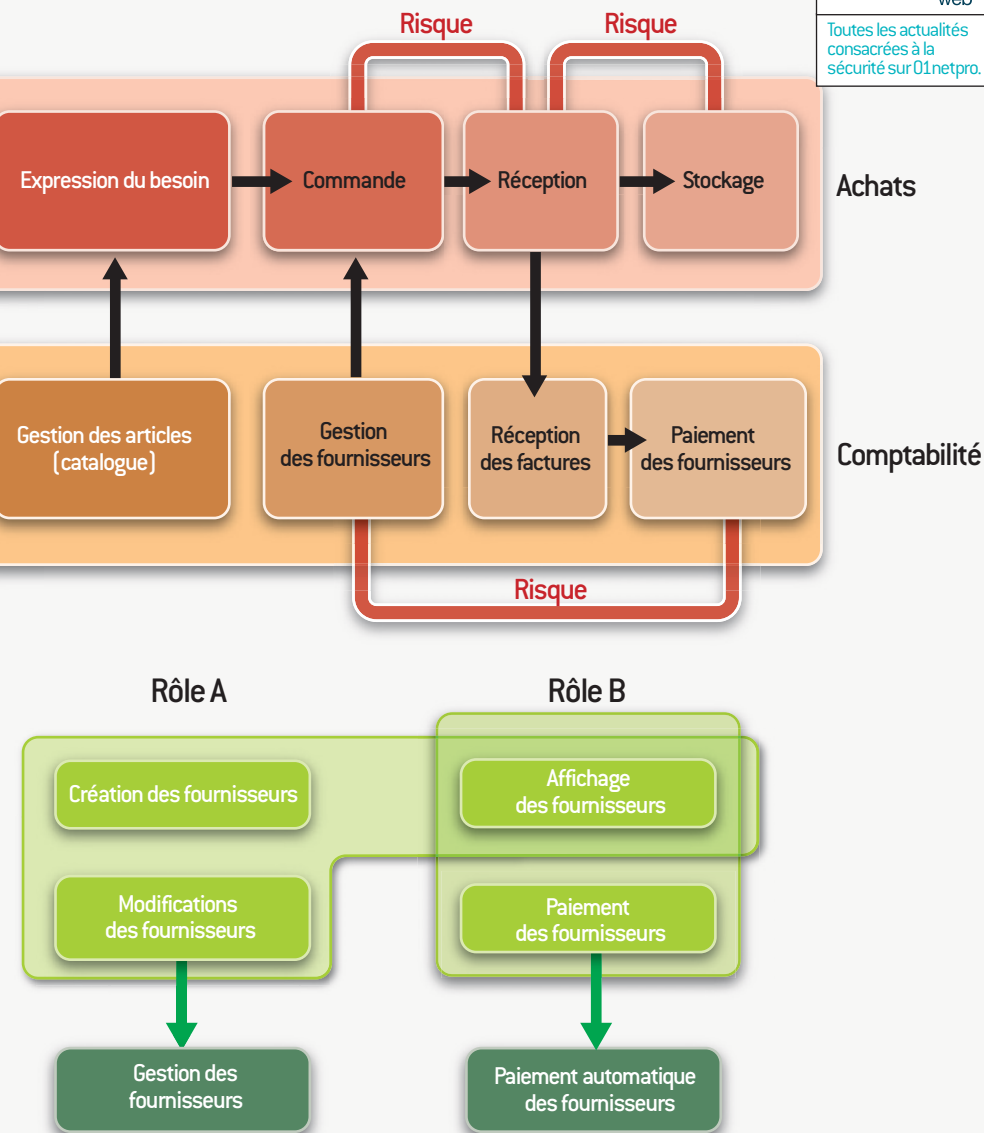
Quels conseils leur donneriez-vous ?

« Avant de se lancer dans l'achat d'un outil il faut d'abord savoir plusieurs choses : quel modèle de rôle retenir ? Quelle architecture organisationnelle ? Quels acteurs internes, de l'IT et des métiers, impliquer ? Ensuite, j'ajouterais qu'il est préférable de débiter par les métiers les plus structurés pour finir par les plus complexes, pour s'éviter un effet tunnel et donc un éventuel découragement. »

Une conduite du changement délicate dans le sens où certaines responsabilités peuvent être amenées à changer de mains. « Cela donne lieu à des échanges intermétiers. Le service informatique reste présent pour coordonner. Il joue son rôle de maître d'œuvre mais pas celui de maître d'ouvrage », ajoute Emmanuel Antignac.

De façon générale, les projets de gestion des rôles sont assez coûteux. Par exemple, pour un parc de 20 000 utilisateurs, il faut compter entre un et deux millions d'euros et le projet peut facilement s'étaler sur deux ans. Au-delà de la démarche, se posent les questions de l'outillage et, dans ce cas, de son acquisition : qui est propriétaire de l'application et qui en supporte les coûts ? Dans certains cas on pourrait, par exemple, supposer que la surveillance de la base de données utilisateurs incombe au contrôle interne, la DRH en l'occurrence, et non à l'informatique. Et on ne peut placer ●●●

à passer au peigne fin



Source : Securway

aident à les mettre en œuvre. La gestion des rôles en fait partie. Plus souvent connue comme étant une nouvelle brique technique de la gestion des identités, elle est avant tout une méthode, une approche, qui s'est concrétisée petit à petit par des offres d'éditeurs censées faciliter sa mise en place. Car aujourd'hui, aucun outil ne peut prétendre se substituer aux ressources humaines ou aux directions métier pour distinguer un rôle métier d'un autre. Seules ces dernières le savent et ont les réponses à ces questions.

Les outils qui existent n'ont donc pour unique fonction que d'ôter des mains de la DSI la charge d'affecter les habilitations aux employés et de les gérer informatiquement. « Jusqu'ici, les personnes décisionnaires

envoient leurs demandes à l'équipe technique. Par exemple, pour une centaine de demandes traitées manuellement, avec la gestion des rôles il n'y en a plus qu'une : l'exception. Une économie de temps considérable et donc, sur le long terme, d'argent », précise Emmanuel Antignac. Un rôle définit « ce que vous êtes, ce que vous faites », d'un point de vue fonctionnel comme organisationnel. En pratique, il faut d'abord passer en revue les processus et les habilitations déjà en place, ainsi que la façon dont ils se décomposent et à quelle ressource informatique ils correspondent, à partir de la liste des salariés. Cette cartographie des habilitations sert de support pour la définition ou la redéfinition des rôles, qui devront être réaffirmés de façon périodique.

●●● un risque sous contrôle tant qu'on n'a pas trouvé qui en assume la responsabilité.

Si la gestion des rôles ne s'applique pas à un secteur d'activité en particulier, les entreprises directement concernées par cette problématique sont en général d'assez grande envergure et avec des circuits de validations plutôt lourds. D'autre part, celles disposant d'un système de gestion centralisé tel qu'un PGI sont confrontées à l'obligation de définir des rôles métier pour chacun des utilisateurs avant de délivrer les accès.

Un temps d'avance pour l'univers du PGI

Elles ont donc un temps d'avance, sans pour autant pouvoir s'affranchir d'une démarche de refonte de la translation informatique des habilitations métier. Jean-Yves Kemplaire, directeur chez CHR Hansen, raconte que trois ans après le déploiement de SAP sur 25 pays pour 4 000 utilisateurs, il a été décidé de mettre en place la gestion des rôles. « *Les raisons sont nombreuses. En dehors des craintes de fraudes, il faut aussi tenir compte des problèmes opérationnels, comme des clients facturés par mégarde* », explique-t-il. Pour CHR Hansen, la première étape a donc été de passer par une redéfinition complète des rôles métier. « *En accord avec les directions, un travail lourd étalé sur un an a monopolisé 35 personnes de l'IT et un prestataire externe pendant six mois* », raconte Jean-Yves Kemplaire.

Une phase empirique, également, puisque Kemplaire et ses équipes ont travaillé sur des rôles organisationnels existants. Pour éviter les conflits de process ou autres erreurs de flux, les équipes de CHR Hansen ont décidé d'être plus souples au début et de refermer les portes au fur et à mesure que les erreurs faisaient leur apparition. Une gestion dynamique des exceptions. « *Si on ferme tout au départ on s'expose à ce que des utilisateurs ne puissent plus travailler, avec comme conséquence une production bloquée* », précise Jean-Yves Kemplaire.

Sortis du PGI, les projets de gestion des rôles se greffent, de façon générale, en aval de l'implémentation de solutions des gestion des identités. La raison est simple. Le rôle vient directement chapeauter l'identité et s'appuie sur un workflow mis en place par la brique de gestion d'identités, considérée, de fait, comme le socle de l'architecture. On pourrait pourtant partir du principe qu'il serait plus efficace de démarrer les deux en parallèle pour s'affranchir d'une démarche rétroactive de consolidation des identités créées et de la gestion des

CE QU'ILS EN PENSENT



Jean-François Relativo,

directeur de projet IAM chez HP Enterprise Services, rattaché à Alcatel-Lucent

« Un vrai apport pour les directions métier »

« Un des intérêts de la gestion des rôles est que, pour une fois, l'IT peut apporter quelque chose aux directions métier et pas uniquement d'un point de vue informatique. La DSI donne une solution métier aux métiers, car le rôle en lui-même est métier. Nous rendons nos directions autonomes, car ce sont elles qui doivent définir les rôles, les affecter, les gérer. Si nous n'avons pas encore fait le choix définitif de l'outil, la marche à suivre, elle, nous est acquise. Nous passons par une mise à plat des rôles à partir de l'existant. Ensuite viendra la mise en place d'un outil. Nous préférons éviter ceux fait maison, mais nous sommes favorables à un outil "user friendly" intuitif. Eurekify, de CA, est trop complexe. L'outil de Sun, un des premiers, est performant pour la modélisation des rôles et optimisé pour leur solution de gestion des identités. Toute cette étude de marché nous a fait comprendre que ce que nous cherchions était un outil de GRC [Governance Risk Compliance]. Sailpoint et Aveksa en sont de bons exemples. On peut créer, entre autres, des rôles dynamiques. Se dire que, suivant la région, ils auront telle dénomination et donneront accès à des applications qui ne sont pas disponibles selon le pays... »



Eric Doyen,

RSSI du Crédit Immobilier de France

« La DSI peine à gérer les demandes d'habilitations »

« Nous avons beaucoup d'entités qui fusionnaient et pléthore de systèmes. Mais nous n'avons pas de culture gros système, pas d'outil comme RACF sur mainframe et un foisonnement d'environnements : Active Directory, des outils de messagerie, du collaboratif. Pas non plus de produit comme le PGI qui oblige, de fait, à se structurer. Sans mécanismes de workflow, la DSI est aujourd'hui incapable de refuser les demandes. Jusqu'ici, chaque structure avait plus ou moins son mode opératoire, déterminé par sa taille. En pratique, au-delà de 100 collaborateurs, il est impossible de connaître l'ensemble des chefs de services, ce qui empêche la réalisation des dérogations implicites quant aux flux entrants et sortants [arrivée ou départ des collaborateurs]. Nous recensons pour l'instant une centaine de rôles pour 3 000 identités sur 12 sites principaux et 280 agences. On a 57 profils métier, liés à l'opérationnel, et 43 profils propres au décisionnel. On est parfois obligé de créer deux rôles avec le même contenu technique, uniquement pour respecter les voies de la hiérarchie. Il est très facile de réussir à obtenir les informations sur les rôles métier de la part des départements, car il y a une vraie demande de leur part. »

habilitations qui leur sont liées. Mais, les deux démarches étant assez lourdes, les experts s'accordent à dire que le projet doit être découpé en deux phases.

La gestion des identités comme brique de départ

La première consiste à mettre en place la brique technique (gestion des identités). La seconde à lui greffer la brique fonctionnelle permettant aux directions métier de prendre la main. Pour alléger cette consolidation, une fonctionnalité non négligeable est devenue partie intégrante de la gestion

des rôles : le role mining. Celui-ci se charge d'effectuer automatiquement une analyse complète des comptes pour en extraire d'éventuels rôles existants. Cette étape n'est en aucun cas définitive mais sert de base de travail avant de lancer la phase de consultation des directions métier.

Si la France a pris du retard face à ses voisins outre-Atlantique, de nombreux projets sont en cours. Fortement sensibilisées à la question, les entreprises sollicitent de plus en plus experts et consultants pour des audits visant l'adoption d'une démarche qui pourra, à terme, leur éviter de fâcheux désagréments. ■

STÉPHANE BELLEC