



Management La DRH au cœur de la problématique de sécurité

Cruciale pour la sécurité, la gestion des droits d'accès aux diverses ressources informatiques passe logiquement par la prise en compte du rôle de chacun dans l'entreprise. Une gestion par profils que la DRH est, a priori, bien placée pour superviser efficacement...

A peine les DRH ont-elles mis leur informatique à l'heure de l'intranet – avec, pour les plus audacieuses, la formule du libre-service qui ouvre leur système d'information (SIRH) à la contribution des salariés – que les voilà interpellées par un défi en matière de sécurité qui dépasse de loin la protection des données de leur seule fonction. Un défi que les consultants férus d'anglicismes résumant sous les termes *identity management* ou *e-provisioning* (gestion automatisée des habilitations).

L'intention est claire. Face à la multiplication des contrôles d'accès aux messageries, intranets et autres applications métier reposant sur divers annuaires difficilement tenus à jour, il s'agit d'introduire une certaine cohérence en partant de la source d'identification des personnes qui a le plus de chances d'être actualisée : l'annuaire du SIRH. "Il est rare qu'un salarié ayant quitté l'entreprise continue de recevoir son salaire, alors que, bien souvent, il garde accès à la messagerie et à l'intranet plusieurs semaines après son départ", remarque Olivier Le Guillou, directeur marketing de la société Amalthis, promoteur d'une démarche et de solutions rationalisant la gestion des annuaires. Avec



Dans l'entreprise, les données nécessaires à la gestion automatisée des habilitations des employés (badge d'accès, mots de passe, e-mail...) sont détenues par la DRH, et non par les informaticiens.

l'e-provisioning, cette démarche est poussée un cran plus loin. Elle vise à automatiser l'affectation des ressources informatiques selon le profil du salarié (voire du partenaire ou de l'intervenant extérieur). Qu'un employé arrive dans l'entreprise, qu'il change de site ou de poste ou qu'il rende son tablier, un logiciel (serveur central) se charge de régler sans délai (ou de supprimer) toutes les habilitations (numéro de téléphone, badge, adresse électronique, mots de passe) dont il a besoin pour l'exercice de son métier. Là encore, l'origine la plus logique de cet automatisme tient dans les

quelques données introduites ou modifiées au sujet de cette personne dans le SIRH.

Un besoin reconnu mais...

Objectif utopique ? Relais de croissance pour une offre en mal de débouchés ? De fait, les manœuvres en cours chez les fournisseurs ne trompent pas. Par exemple, la récente fusion de Netegrity, spécialiste de la sécurisation des accès, avec Business Layers, spécialiste de l'e-provisioning, ou encore le partenariat qui a permis à l'éditeur Meta4 d'intégrer à son progiciel de GRH la technologie de

gestion des annuaires de Calendra. Pourtant, à l'été 2002, selon une étude IDC auprès de 340 grands et moyens comptes français, la méconnaissance de la notion d'annuaire centralisé (SIRH ou autre) était encore flagrante. Ne serait-ce qu'au vu du décalage entre les vertus sécuritaires qu'on lui accorde – notamment la synchronisation et l'homogénéisation des données d'identification – et les applications qui y sont reliées. Quand il existait (pour une moitié du panel), le serveur d'annuaire était souvent cantonné au rôle de référentiel pour la messagerie, et moins d'une fois sur trois connecté à la GRH.

Depuis ce constat, gel des investissements aidant, la situation n'a guère évolué. "Souvent, le point d'entrée se trouve du côté des informaticiens passionnés d'innovation ou chargés de la veille technologique qui en ont saisi l'intérêt", reconnaît Serge Casarus, consultant expert du cabinet Cedar, et ancien directeur de projet RH du groupe Alstom. L'argument d'un suivi facilité et sécurisé par le biais des logiciels de gestion des habilitations proposés par Novell, Computer Associates, BMC ou IBM trouve un écho auprès de ces informaticiens. Mais rares sont les DRH qui s'intéressent aux enjeux de la gestion électronique des identités au point de s'impliquer dans sa mise en œuvre. Non qu'elles en nient le besoin. Au contraire. Mais cela reste du domaine de l'intendance, donc des informaticiens.

Et c'est là que le bât blesse. Car si, techniquement, la mise en œuvre de ces dispositifs n'a rien de trivial et si, ensuite, leur gestion relève bien de l'administration des systèmes, "les informaticiens se rendent vite compte que, n'étant pas à l'origine des données qui leur permettent d'ouvrir ou de fermer des comptes, ils n'ont aucun moyen de juger de la fiabilité de ces données", rappelle Serge Casarus. Que dire alors de la sécurité ? "Souvent,

MARC GUILLOT



on se fie à la caution d'un supérieur hiérarchique, sans vérifier si lui-même est habilité. Sans parler des organisations matricielles, et des divergences possibles entre filières hiérarchiques/opérationnelles et fonctionnelles", ajoute ce consultant expert.

D'ailleurs, ni les DSI ni les DRH ne sont vraiment dupes à ce sujet. Car s'il s'agit, comme l'explique Serge Casarus, "d'appuyer directement les droits d'accès aux ressources sur les données clés des personnes" (à tel emploi type, tel site, tel service, tel niveau de responsabilités... correspond telle ou telle habilitation), encore faut-il au préalable avoir calibré et validé ces critères. Un travail de détermination de profils, de préparation de la gestion par profils, qui implique d'aménager le SIRH en conséquence. Mais aussi de se donner les moyens (passerelles...) de tenir compte de la diversité des références dans le découpage de l'entreprise (les tables de référence de la fonction financière ne sont pas celles de la production, par exemple) et le suivi de son activité (par pays, établissements, équipes...).

Ainsi, qu'il s'agisse de faire remonter et de synchroniser les données pertinentes entre des annuaires spécifiques et un annuaire central (ou méta-annuaire) ou, dans le sens inverse, de pousser le suivi des comptes utilisateurs vers les équipements concernés (e-provisioning), les entreprises disent appréhender le coût autant que les contraintes de ces préparatifs incontestables. "Comme pour l'implantation des progiciels de gestion intégrés, ce n'est pas la technologie qui est mise en cause dans ce genre de projet, mais le volet organisationnel qui fait peur. C'est l'argument que l'on nous oppose le plus souvent", constate Guillaume Absi, ingénieur avant-vente de Netegrity.

De plus, si, comme le préconise Serge Casarus, le SIRH devient la "source officielle" des données nécessaires à la gestion par profils, il en découle une contrainte opérationnelle majeure. "Puisque l'accès de chacun à ses outils de travail, depuis le login du PC et sa connexion au réseau local, à la boîte aux lettres et à l'intranet, jusqu'aux fonctionnalités des applications métier, dépend de ces données, et puisque ainsi le SIRH



Serge Casarus, consultant expert du cabinet Cedar : **"N'étant pas à l'origine des données qui leur permettent de gérer des comptes, les informaticiens ne peuvent juger de leur fiabilité."**

devient de facto le cœur opérationnel de l'entreprise, il est impératif que ces données soient tenues à jour en temps réel", explique cet expert. Il faut donc veiller de près à la qualité de gestion des données de la fonction RH.

Stratégie de contournement classique, les entreprises mettent le pied à l'étrier (organisationnel) en commençant par la synchronisation de gestion de compte de quelques applications. "En Europe, 90% des investissements en e-provisioning sont encore décidés sur cette base, sachant que cela signifie une utilisation anémique du potentiel de la technologie", note Guillaume Absi. Le coût des licences logicielles (serveur, annuaire, bases de données) pour un projet d'e-provisioning couvrant les habilitations de 2 500 utilisateurs sur une dizaine de systèmes cibles est d'environ 300 000 euros. Auquel s'ajoute le travail d'analyse

Olivier Le Guillou, directeur marketing de la société Amalthis : **"Souvent, un ex-salarié garde accès à la messagerie et à l'intranet bien après son départ."**



et d'intégration (de trois à six mois-hommes, selon l'état des lieux et l'envergure de la cible). Pour les très grands comptes, ce genre de projet peut dépasser le million d'euros.

L'argument du RSI

Pour sa part, l'éditeur Amalthis a prudemment le parti de faciliter l'implication de la DRH, en proposant une formule de portail (We-Soft) qui non seulement permet l'actualisation d'un référentiel unique des salariés, interconnecté avec l'existant le plus à jour (systèmes de paie, de gestion des temps et d'activité), mais qui encore en rend la consultation "dûment autorisée et sécurisée" utile aux salariés. Ce qui a permis, notamment à RTE (Réseau de transport d'électricité, 8 000 agents, division d'EDF indépendante depuis 2000) de mettre en place une animation, avec correspon-

dants locaux, autour d'un annuaire sur intranet distinct de celui d'EDF, qui, de plus, relègue au passé la manipulation de multiples Bottin papier régionaux. Après une phase pilote de juin à septembre 2002, le déploiement généralisé s'est fait en trois mois, avec l'équivalent de deux personnes sur un trimestre, pour l'organisation, le suivi des développements et du déploiement, et la mise en place de l'administration au niveau national.

Certes, la DRH, comme l'entreprise, doit y trouver son compte, n'est-ce qu'en gain de productivité administrative. Et c'est encore aujourd'hui l'argument le plus porteur. "Il n'y a pas pires coûts que les coûts cachés. La mise en commun des données dans un annuaire central, qui met fin à l'anarchie d'une gestion dispersée, se justifie aisément avec un retour sur investissement en quelques mois", remarque Serge Casarus. Mais il n'empêche que cette qualité de gestion de données RH, dont dépend la sécurité de l'entreprise, ne dépend pas seulement de la précision du travail administratif, ni même du bon vouloir de la DRH. La mise en place des mécanismes de gestion par profils puis de remontée des informations passe par une coordination transversale avec les autres directions, dont la DSI. Autant dire que ce contexte idéal, où la DRH dispose des moyens d'en assumer pleinement la contrainte organisationnelle et opérationnelle, est encore l'exception. "Il suffit d'observer la faiblesse actuelle de la représentation des DRH aux comités de direction", conclut le consultant de Cedar. ●

ANNE-MARIE ROUZÉ

BIG BROTHER OU EFFICACITÉ DE GESTION ?

Mettre en commun les données dans un annuaire, ce n'est pas mettre tout sous la coupe d'une structure centrale qui déciderait de tout, note Serge Casarus, consultant du cabinet Cedar. Où a-t-on vu que le SIRH d'une entreprise multisite, administré de façon centralisée afin de profiter d'économies d'échelle, supprime la possibilité de gérer en local la formation, le recrutement, la sécurité ou la paie ? Ce n'est jamais le cas parce que totalement contre-productif. Centralisation et automatisation des habilitations et contrôles d'accès ne signifient pas flicage. "Certes, les relations d'un éditeur avec la Cnil se placent toujours dans le contexte d'une utilisation normale, non détournée, de la technologie", observe Olivier Le Guillou. Mais, selon ces consultants, le principe de ces outils est précisément de permettre à une politique d'entreprise de s'exprimer. Et ce au travers du paramétrage fin, du trombinoscope ou de l'organigramme, où ne figurent que les éléments souhaités, à l'attribution et au filtrage des droits d'accès à telle ou telle source d'information. Le personnel, à travers ses représentants, peut avoir son mot à dire. Mais, officiellement, "l'entreprise est fondée à organiser la publication interne des données concernant les salariés (dans le respect de la loi, bien sûr) qui s'avèrent utiles à l'efficacité de sa gestion", explique Serge Casarus, pour qui cette information "calibrée et validée" n'est, que la partie émergée de l'iceberg, le reflet d'une qualité de gestion plus ou moins valorisée par l'état-major et par la DRH. "C'est quand le flou subsiste autour de la définition des responsabilités et des rôles dans l'entreprise que peuvent se générer et s'entretenir des zones de tension."

POUR UNE APPROCHE PRAGMATIQUE DES ANNUAIRES D'ENTREPRISE

Objectifs

- Assurer la cohérence des données entre différentes applications.
- Éviter les doubles saisies.
- Viser un retour sur investissement rapide.
- Respecter les exigences de sécurité, de performances.

Conduite pratique

Selon les règles générales d'une démarche d'urbanisation

de SI, qui tient compte de l'existant, de son hétérogénéité, il faut :

- identifier les populations associées aux annuaires (établissement, statut...) en tenant compte des frontières "politiques" entre entités ;
- identifier les informations associées aux personnes ;
- bien comprendre le champ d'application des technologies d'annuaire (LDAP, Light

Directory Access Protocol) ;

- décider d'une répartition des données entre les divers annuaires qui satisfasse les exigences fonctionnelles, sécuritaires, opérationnelles ;
- choisir un annuaire maître et l'entité responsable de sa mise à jour.

Analyse du consultant Serge Seletzky, de MDBA Conseil (Source : séminaire Amalthis).