Sécuriser les accès et les identités : 4 questions pour maitriser l'IAM

L'Identity and Access Management (IAM) est un élément crucial des systèmes d'information. À quoi sert-il ?, comment fonctionne-t-il ? , comment le piloter ?, peut-il être accessible sur le Cloud ? Voici les 4 questions/réponses pour aborder votre projet.

Selon une étude de septembre 2018 de Grand View Research, le marché de l'IAM (Identity and access management) ou Gestion des identités et des accès est promis à un bel avenir. Il devrait ainsi passer de 8,85 milliards de dollars en 2017 à 22,68 milliards de dollars en 2025, soit une croissance annuelle moyenne de 12,7 %.

Le renforcement des obligations réglementaires ne sera pas le seul moteur de cette croissance. La progression du Cloud, des terminaux mobiles et, prochainement, des objets connectés de la mouvance IoT vont faire exploser la complexité de la gestion des identités et des accès.
Sans compter les changements ayant lieu au sein des entreprises, comme le recours toujours plus important à des consultants ou au télétravail, qui sont autant de casse-têtes sécuritaires à résoudre.

Un phénomène de rattrapage fait que certains pays (Chine et Inde en tête) et certaines industries (Cloud et IoT) devraient connaitre une croissance plus forte que les autres. Même les TPE et PME pourraient s'y mettre, à travers probablement des offres Cloud, plus aisées à mettre en place et à administrer.

Une autre étude, signée One Identity, montre que plus de 30 % des entreprises s'appuient encore sur des méthodes manuelles pour gérer leurs comptes administrateurs et que deux tiers fournissent des comptes à privilèges à leurs partenaires et sous-traitants.
Dans 44 % des cas, le provisionnement de nouveaux comptes utilisateurs peut prendre des jours, alors que leur suppression ne peut être garantie chez 20 % des entreprises. Il est donc urgent d'agir.

1 – Gouvernance : tout part de la RH et des métiers

Une solution d'IAM se compose de deux branches complémentaires : la gestion des identités et la gestion des accès. La première fait le pont entre la personne, son rôle dans l'entreprise et les informations auxquelles elle peut accéder. La seconde se charge de l'accès aux ressources elles-mêmes, via une solution globale d'authentification (Single Sign-On – SSO).

La gouvernance des identités adopte aujourd'hui majoritairement un modèle de type RBAC (Role-Based Access Control). Ce sont les rôles des employés au sein de l'entreprise qui vont ainsi définir les droits d'accès aux différentes ressources informatiques.

« Tout part du référentiel RH, explique Matthieu Filizzola, consultant cybersécurité ESEC, en charge des activités IAM en Île-de-France chez Sogeti. Des informations comme le poste d'un employé et le

nom de son manager permettent de définir les droits d'accès et la personne chargée de valider ces droits. Le rôle du service RH est important, car c'est lui qui va prendre en compte les joiners (nouvelles embauches), movers (personnes changeant de poste) et leavers (celles quittant l'entreprise). »

L'IAM entre ici en piste. Il fait le rapprochement entre un rôle métier et un profil technique, donnant à chaque métier une palette de droits d'accès. Mais qui définit les droits en fonction des métiers et applications ? Ce sont les services métiers justement, en coordination avec la DSI. En résumé, la RH définit le métier de chaque employé et les métiers définissent les droits d'accès aux applications du SI.

« À gauche nous trouvons le référentiel RH des employés, avec leur rôle au sein de l'entreprise. À droite se placent les référentiels (Active Directory, LDAP, etc.) qui recensent des identités techniques (utilisateurs + droits). Et au centre, l'IAM va créer un pont entre les deux », résume notre expert. L'IAM peut donc être vu comme l'orchestrateur de ces différents référentiels, auxquels il va envoyer des instructions.

Les nouvelles législations, comme le RGPD, peuvent-elles complexifier l'attribution des droits d'accès aux ressources ? Pas forcément, estime Matthieu Filizzola, qui pense même que cela peut se révéler positif : « Le cadre réglementaire est très moteur, car il déclenche beaucoup de réflexions très pertinentes et bénéfiques.

2 – Gestion des accès : une fausse simplicité

La gestion des accès peut sembler simple de prime abord : un badge pour accéder aux bureaux et un mot de passe pour l'ordinateur. Mais dans ce domaine tout peut devenir rapidement assez complexe.

Il est normal qu'un employé se connectant depuis son PC professionnel situé dans son bureau puisse avoir accès à tout ce que sa fonction autorise. Mais il est logique aussi qu'en cas de télétravail certaines ressources critiques lui soient interdites d'accès. Ou au moins que la procédure d'authentification soit renforcée.

Une double problématique se pose donc : celle de l'authentification forte et celle de l'authentification renforcée suivant la situation. Matthieu Filizzola sépare les utilisateurs en trois grandes classes principales, pour lesquelles la stratégie appliquée va complètement différer :

* Les clients

* Les employés

* Les prestataires

Pour les clients, la priorité est de maximiser l'expérience utilisateur. Pas question de les faire fuir avec des procédures d'authentification trop complexes. Cela n'empêche pas, toutefois, d'imposer une authentification renforcée lorsque la connexion parait suspecte : depuis un smartphone différent de celui utilisé habituellement, à des heures inhabituelles, depuis l'étranger ou un opérateur Internet différent.

Dans le monde mobile, une authentification forte est par chance possible sans trop d'impact sur l'expérience utilisateur, en utilisant par exemple le capteur d'empreintes digitales intégré à certains smartphones.

Pour les employés, il est possible d'imposer plus de contraintes, sans toutefois aller trop loin. Sinon, gare au risque de rébellion. Le bon point est que l'employé travaille souvent au sein des bureaux de l'entreprise. Un badge d'accès sera donc un moyen efficace de protéger à la fois l'accès au bâtiment et aux données importantes. Avec bien entendu la possibilité d'utiliser un mot de passe en complément sur le PC. Ceci n'est plus valable dès que le salarié se trouve en mobilité ou en télétravail, quoique l'utilisation d'outils certifiés par l'entreprise (par exemple un téléphone professionnel) permettra de limiter les risques.

Pour les prestataires, qu'ils travaillent sur site ou à distance, il convient d'imposer plus de restrictions, tant en termes de renforcement des procédures de connexion que de limitation des droits accordés. L'accès aux ressources critiques de l'entreprise, ainsi qu'aux processus de production et de pré-production doit leur être interdit. Contrainte qui vaut d'ailleurs aussi pour les employés en mobilité ou télétravail.

3 – Aller au-delà du modèle RBAC ?

La problématique de l'authentification des utilisateurs peut rapidement devenir inextricable. Au point qu'il peut être judicieux d'adopter un modèle ABAC (Attribute-Based Access Control) qui va prendre en compte les attributs de l'utilisateur, ceux associés à l'application et les conditions environnementales.

Nous venons de voir qu'en fonction du lieu de connexion, un même utilisateur ne doit pas avoir accès aux mêmes ressources. Mais il est possible d'aller plus loin, en définissant une note qui traduira le niveau de confiance de la connexion. « La notion de note est cruciale, explique Matthieu Filizzola. Celle-ci dépendra de l'environnement physique, de l'environnement informatique et du niveau d'authentification. »

Nous pouvons ainsi imaginer un niveau minimal d'authentification – saisie d'un identifiant et d'un mot de passe – permettant d'accéder à une ressource de base : le compte de courrier électronique de l'utilisateur.

Pour accéder aux autres ressources, la note devra grimper, sur la base de facteurs comme :

* L'utilisateur est dans son bureau ;

* L'utilisateur emploie son PC professionnel ;

* Le système d'exploitation et l'antivirus sont à jour ;

* Une double authentification a été faite ;

A contrario, d'autres éléments sont susceptibles de faire descendre la note :

* L'utilisateur n'est pas dans son bureau ;

* L’utilisateur se connecte depuis son PC personnel ;

* La connexion se fait hors des heures de bureau ;

* Le verrouillage automatique de l’écran a été désactivé ;

Autre difficulté qu’il faudra résoudre lors de la mise en place d’une solution IAM : l’attribution des droits. « Le vrai problème n’est pas l’intégration technique, mais la conduite du changement et l’attribution des droits, confirme Matthieu Filizzola. Il est difficile d’appliquer des étiquettes à des gens qui disposent par essence de toutes les connaissances spécifiques. »

« L’avantage du modèle RBAC est qu’il permet de repérer les profils isolés et d’alerter ainsi la direction sur le besoin de faire évoluer l’organisation en formant d’autres personnes à ces compétences spécifiques. »

4 – L’IAM as a Service, c’est possible !

Une solution IAM peut tout à fait être hébergée dans le Cloud. « Il n’est pas rare de proposer des appliances capables de requêter le SI RH et de donner des ordres aux AD depuis le Cloud », confirme Matthieu Filizzola.

« Tous les éditeurs ont une solution Cloud, annoncée, fonctionnelle ou disponible. L’adhésion des grandes entreprises à ce modèle reste à voir : pour des raisons réglementaires, beaucoup doivent garder cette brique en interne. Mais les PME, qui ont souvent négligé ce secteur, pourraient adopter l’IAM grâce au Cloud. »

Et de nous confier que certains comptes « d’une taille raisonnable » commencent à avoir des logiques Cloud. Pour des raisons réglementaires justement, car certains fournisseurs de Cloud sont plus en avance que les entreprises dans ce domaine.

Bien évidemment, nous parlons ici d’acteurs français (ou allemands, pays où la réglementation est plus exigeante), comme OVH, Online, Orange, etc. De petits acteurs comme Jaguar Network se sont même fait une spécialité de ces Cloud souverains strictement gérés.

Il est à noter que l’intégration entre les SI RH, SI métiers et IAM est souvent facilitée par les éditeurs. Etat de fait d’autant plus avéré que les ténors du monde de l’IAM sont, pour la plupart, des sociétés spécialisées, comme SailPoint, Ping Identity, RSA, Gemalto ou encore Okta.

Bref, des acteurs différents de ceux fournissant les solutions métiers et RH des entreprises. L’interopérabilité avec des offres tierces fait donc partie de leur ADN.