GESTION DES IDENTITES ET DES ACCES
IAM

Définition

La gestion des identités et des accès (en anglais *identity and access management* ou IAM) est un ensemble d'outils et de procédures permettant de contrôler et organiser de façon rationnelle les droits d'accès aux ressources informatiques.

Avec un système IAM complet et bien géré, une organisation possède un référentiel fiable de ses utilisateurs internes et externes. Elle attribue automatiquement – souvent après validation hiérarchique, fonctionnelle et technique – des droits d'accès en fonction des besoins et du rôle de l'utilisateur dans l'organisation. Elle s'assure de l'identité de l'utilisateur au moment où il souhaite avoir accès à des données, ou utiliser des applications et systèmes. Les outils IAM permettent la gestion d'un cycle de vie de l'identité numérique au sein de l'organisation, en ouvrant les accès sur les ressources du système d'information quand cela est nécessaire, et en les supprimant ou modifiant quand l'utilisateur change de poste ou quitte l'entreprise.

Les outils d'IAM fournissent typiquement les fonctionnalités suivantes.

- **Gestion des identités** : rationaliser les identités des utilisateurs, auparavant dispersées dans plusieurs annuaires. Des fonctions de pages jaunes / pages blanches, sont présentent pour permettre l'identification rapide des personnes au sein de l'organisation.

- **Authentification forte** : contrôle d'accès aux ressources par carte à puce, biométrie, badge radio etc. Gestion des cartes et certificats, réinitialisation de mots de passe.

- **Authentification unique** (*single sign-on* ou SSO) : lie plusieurs mots de passe et certificats à un seul moyen d'authentification par utilisateur – typiquement un mot de passe ou une carte à puce.

- **Gestion de politique** : définit les droits d'accès en fonction de règles liées au rôle d'une personne dans l'organisation. Prise en compte de contraintes de séparation des tâches.

- **Circuit d'approbation** : conditionne la mise en place des droits d'accès déduits de la politique de sécurité à une validation, généralement hiérarchique.

- **Provisionnement** : se substitue automatiquement à l'administrateur d'une ressource pour y créer, modifier et supprimer des comptes d'utilisateur.

- **Audit et rapports** : propose une traçabilité des évènements liés aussi bien à l'usage des ressources qu'à l'affectation des droits (Evidences). Les rapports d'une manière plus large offrent des possibilités de réaliser des audits et d'assurer la conformité à des règles de bonnes pratiques, de règlementation métier, de standards ou de lois.

Exemples

Secteur bancaire

Dans les banques, l'IAM est utilisé dans le cas des accords de Bâle pour mesurer et réduire l'exposition à certains **risques opérationnels**.

L'accord Bâle II a en effet introduit la prise en compte des risques opérationnels dans l'évaluation des exigences minimales de fonds propres des banques. Parmi les méthodes d'évaluation de ces risques proposées par les accords, les Approches de Mesure Avancées (AMA) autorisent l'établissement financier à évaluer lui-même les risques opérationnels liés à son activité.

Une bonne méthodologie de gestion des risques opérationnels est indispensable pour mettre en œuvre une AMA. Cela est également un pré-requis pour mettre en place une approche standardisée. Pour cela, la banque doit mettre en place un dispositif de gestion du risque opérationnel et une entité chargée de sa mise en place et de sa gestion.

Le secteur de la santé

Un besoin fort de protection des données médicales, souvent appuyé par un cadre règlementaire (comme en France avec le décret de confidentialité pour les professionnels de santé) existe dans les hopitaux qui doivent assurer la confidentialité des données du patient tout en permettant un accès rapide et souvent sur des postes partagés dans des environnements critiques. L'association avec une carte CPS en France, ou NHS en Grande Bretagne, apporte une assurance sur l'identité et la signature des actes.

Cibles

La plupart des organisations peuvent mettre en place avec profit une gestion des identités et des accès. Trois facteurs principaux influent sur le bénéfice que l'on peut tirer d'une telle solution.

- **Taille de l'organisation** : la complexité de la gestion des droits d'accès dépend de façon exponentielle du nombre d'utilisateurs et de ressources - les combinaisons possibles sont en effet plus importantes. L'IAM permet de raisonner en termes de rôles, et non en termes d'individus.

- **Complexité de l'organisation** : l'hétérogénéité technique multiplie les outils d'administration. La présence de nombreuses filiales et sites rend très difficile la mise en place centralisée de règles locales. Face à cela, un outil d'IAM permet d'appliquer une politique (et de l'auditer) par une seule interface. Et l'on peut déléguer localement une partie de la définition des politiques et des droits.

- **Contraintes réglementaires** : des exigences légales d'intégrité, de confidentialité et de disponibilité peuvent contraindre les organisations, et souvent selon le secteur d'activité, à contrôler de façon rationnelle l'accès aux données. L'IAM sera donc mis en place dans ces organisations, au moins dans les départements concernés – soins aux patients et R&D pharmaceutique par exemple.

En conséquence, la plupart des organisations de taille moyenne ne déploieront généralement que quelques fonctions IAM - comme le SSO ou la gestion des identités. Mais si elles oeuvrent dans un secteur

réglementé (établissements de santé, industrie pharmaceutique ou finance par exemple), elles auront tendance à mettre en place une offre plus complète.

Les grandes entreprises et administrations ont souvent été pionnières dans la mise en place de la gestion des identités et des accès. A titre d'exemple l'Assurance Maladie a mis en place à l'échelle du pays un système de gestion des identités et des accès dès l'an 2000 avec le déploiement de la carte à puce pour l'ensemble des 80000 agents.

Cadre réglementaire

Dans une organisation, la mise en place d'une gestion des identités et des accès est souvent motivée par des contraintes légales et réglementaires. Celles-ci sont généralement de deux types :

- **Intégrité** : des textes imposent de mettre en place les mesures nécessaires pour assurer l'intégrité de certaines informations. Il peut ainsi s'agir des données de reporting financier (loi Sarbanes-Oxley aux USA, Lois sur la Sécurité Financière de 2003 en France) ou d'exigences sur les données accompagnant les demandes de mise sur le marché (règlement 21 CFR Part 11 aux USA).

- **Confidentialité** : les données personnelles sont protégées par de nombreuses lois. En Europe, celles-ci sont souvent des transpositions de la directive EU 95/46/CE du Parlement européen et du Conseil. On peut ainsi citer le Décret Confidentialité de 2007 couvrant les données médicales personnelles. Autre exemple (non législatif) : le standard de sécurité des données PCI DSS établi par un comité regroupant les principaux fournisseurs de cartes de paiement.

D'autres textes couvrent la disponibilité continue de moyens critiques : contrôleurs aériens ou chaînes de diffusion publiques par exemple. Dans ce cas, la protection de l'accès informatique visera à restreindre les risques de pannes d'origine humaine.

Enfin, certains textes (comme les accords de Bâle) imposent de mettre des ressources financières au bilan de banques en regard de leur exposition aux risques. L'IAM aura là un rôle de mesure et documentation de certains risques opérationnels, en complément de son rôle classique de prévention.

Evaluation des risques

Avec le développement exponentiel du numérique, la plupart des données qu'elles soient financières, liées aux processus métiers, ou de l'ordre de la propriété intellectuelle, sont contenues sur des supports informatiques. Il est donc essentiel de contrôler l'accès à ces ressources pour réduire les risques d'atteinte à la confidentialité, l'intégrité et la disponibilité des informations et moyens.

Parmi les risques que l'IAM peut adresser :

- **La fraude interne** (activité non autorisée, vol et fraude)

- **La fraude externe** (sécurité des systèmes, vol et fraude)
- **Le risque clients, produits et pratiques commerciales** (conformité, diffusion d'informations réglementée)
- **L'exécution, livraison et gestion des processus** (saisie, exécution et suivi des transactions, gestion des comptes clients)

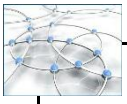
Une solution de gestion des identités et des accès peut ainsi apporter des avantages importants :

- Réduction rapide des risques opérationnels, en diminuant les possibilités de failles d'accès aux données informatiques.
- Information accessible et auditable sur (a) les accès autorisés ou illicites et (b) l'attribution des droits d'accès par les administrateurs.
- Possibilité de réaction immédiate sur détection d'une source de risque opérationnel. En effet, ces outils disposent d'une console centralisée de gestion de tous les droits d'accès.
- Simplification des concepts techniques. Les aspects purement techniques sont masqués pour permettre des procédures claires d'attribution des droits d'accès.

Moyens de protection

Sur le plan technique, une solution de gestion des identités et des accès se compose généralement d'un ou plusieurs des éléments techniques suivants :

- Logiciels **clients** sur poste de travail ou serveurs assurant l'authentification (forte) et le SSO.
- **Annuaires** recueillant les informations sur les ressources, les utilisateurs, leurs droits d'accès, leurs mots de passe chiffrés etc.
- Interface d'**administration** distribuée et déléguée
- **Passerelles** permettant de gérer le cas échéant des authentifications déléguées, de pare feu applicatifs, de provisionning vers les ressources cibles pour les informations utilisateur et droits d'accès.
- Mécanismes d'**authentification forte** telles que cartes à puce, biométrie, badges radio etc.



Liens utiles

Directive européenne 95/46/CE
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:fr:HTML

Norme PCI DSS
http://fr.pcisecuritystandards.org/minisite/en

Code 21 CFR Part 11 (Etats-Unis)
http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/cfrsearch.cfm?cfrpart=11

Loi sur la Sécurité Financière de 2003 (France)
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000428977

Etude Datamonitor sur l'IAM et les risques opérationnels
http://www.evidian.com/fr/iam/sectoriel/wp-datamonitor.php
Livre blanc sur IAM et les Accords de Bâle

http://www.evidian.com/fr/iam/sectoriel/wp-basel.php
Livre blanc : gérer les identités et les accès par réconciliation
http://www.evidian.com/fr/iam/wp-iam.php