REVUES DES DROITS ET HABILITATIONS IAM/PAM

1. Objectifs du projet de revue des comptes des droits et des habilitations

L'idée de ce projet est de construire une base de données IAM et PAM de chaque application utilisée au sein de l'établissement. Ces informations centralisées permettront de réaliser des revues de comptes et privilèges indispensables pour le Système de Management des Systèmes d'Informations (SMSI).

Nous disposons de 2 annuaires principaux qui sont :

- l'Active Directory (AD) de notre Domaine autorisant l'accès à notre réseau et nos serveurs de fichiers
- l'annuaire des agents pris en charge par le système RH.

Concernant l'AD compatible LDAP, elle devrait permettre de généraliser l'authentification des utilisateurs par lien LDAP avec les applications métier.

Il apparait donc indispensable de veiller à la synchronisation de l'annuaire des agents RH et de notre AD et toutes les autres bases annuaires non liées à cette AD (distincts). Le premier contrôle essentiel sera par de croiser les données de l'AD avec la base des agents RH définissant leur situation pour propager cette situation à l'ensemble des annuaires distincts.

La revue de droits et des habilitations devraient donc permettre de garantir la validité des comptes utilisés et de recenser les habilitations afin d'assurer le respect des politiques sécurités définies et de la réglementation RGPD et ISO 27001.

Volontairement, il est ici décidé de se limiter à l'extraction de données, et pas à l'injection de données qui ne concerne plus à la revue de comptes et habilitations mais un projet de type SSO. Ce travail restera cependant un support indispensable à ce type de projet.

Dans un second temps, Il sera nécessaire d'identifier pour chaque Annuaires les processus de maintenance, d'identifier et propager la situation RH des agents (Actif, Suspendu, Sortie, Temporaire, Limité, etc…) et de vérifier et garantir l'usage de ces règles.

La solution reposera sur une modélisation* générale (en base de données) des droits et habilitations que l'on pourra spécifier par applications, en lien avec le matricule agent, et en classifiant les habilitations et le caractère des données conformément au RGPD. Nous pourrons ainsi imaginer toutes sortes de revues de donnés en fonctions de la situation de l'agent et des données gérées.

Iso 27001

SECTION A9: CONTRÔLE D'ACCÈS

« Les utilisateurs ne devraient avoir accès qu'au réseau et services réseau qu'ils ont été spécifiquement autorisés à utiliser. L'accès doit être contrôlé par une procédure de connexion sécurisée et restreinte conformément à la politique de contrôle d'accès. »

SECTION A12: SÉCURITÉ DES OPÉRATIONS

- Voir chapitre 5 Modèles d'accès

« Les journaux d'événements enregistrant les activités des utilisateurs, les exceptions, les défauts et les événements de sécurité de l'information doivent être produits, conservés et régulièrement révisés. »

2. La gestion des identités et des accès (IAM)

Autrefois limitée à la simple administration informatique de comptes utilisateurs, la gestion des identités des utilisateurs et de leurs droits d'accès aux applications est devenue au fil des années un outil de gestion central.

Utilisé tout autant par les directions métiers et IT, l'outil IAM permet la mise en œuvre de règles de sécurité communes et structurantes à l'échelle de l'entreprise, avec pour objectif le contrôle des habilitations des utilisateurs et la réduction des risques.

Plus précisément, une solution IAM centralise et maintient en cohérence les données provenant des RH, des annuaires et des systèmes cibles. En définissant des rôles pour les utilisateurs, représentatifs de leurs fonctions dans l'entreprise, on contrôle leurs droits d'accès selon le principe de moindres privilèges, en s'assurant qu'aucune combinaison de rôles ne donne lieu à un risque élevé. Des règles de gouvernance et des workflows automatisent la gestion du cycle de vie des utilisateurs. L'outil IAM permet aussi des analyses approfondies à des fins d'audits et d'investigations forensiques. Enfin, la recertification des droits d'accès des utilisateurs garantit leur conformité à tout instant.

3. La gouvernance des droits d'accès aux données (DAG)

On estime que près de 80% des données de l'entreprise sont dites non structurées, c'est-à-dire sans format prédéfini (serveurs de fichiers, emails, ressources SharePoint…). Gérer et sécuriser les droits d'accès à ces serveurs de fichiers est primordial pour toute entreprise cherchant à contrôler les risques de fuite de données.

C'est ce que proposent les solutions de gouvernance des droits d'accès aux données (Data Access Governance – DAG), grâce auxquelles l'entreprise administre les structures d'autorisations, délègue le contrôle des droits aux propriétaires de ressources et automatise les processus d'attribution/révocation de permissions par des workflows. Ainsi, un utilisateur pourra transmettre une demande de permissions au propriétaire. Ce dernier quant à lui est responsable des accès à ses données : il définit et contrôle en toute autonomie « qui a la permission de faire quoi et sur quoi ». L'outil DAG est également très utile lorsqu'il s'agit de fournir des analyses et des rapports nécessaires aux audits, permettant de répondre aux questions « qui a approuvé tel accès et quand » ou encore « qui est propriétaire de telle ressource ».

Par contre, les rôles et les autres droits d'accès aux applications de l'utilisateur ne sont pas pris en considération par la solution DAG en tant que telle. La sécurité est alors menacée par la multiplicité des comptes utilisateurs, ou encore l'accumulation de permissions.

Il s'agit alors de combiner les systèmes IAM et DAG ; l'identité de l'utilisateur étant naturellement le dénominateur commun. Cette approche permettra de corréler toutes les informations nécessaires sur l'utilisateur pour une prise de décision éclairée et une gestion « de bout en bout » de ses droits d'accès.

4. La gestion des comptes à privilèges (PAM)

Il est nécessaire de distinguer les droits d'accès issus de besoins métiers, par exemple pour effectuer une transaction financière, de ceux issus de besoins techniques, dédiés notamment à l'administration des applications. Les comptes utilisateurs disposant de ces droits d'accès techniques possèdent alors des privilèges élevés, et représentent un risque important pour l'entreprise. Or la majorité des comptes à privilèges ne sont pas définitivement assignés à une personne. Les comptes « root », « admin » ou « système » sont fréquemment partagés entre les administrateurs informatiques. Le contrôle et la traçabilité des tâches effectuées à partir de ces comptes deviennent alors difficiles, voire impossibles.

C'est ici qu'interviennent les solutions de gestion des comptes à privilèges (Privileged Account Management – PAM). Grâce à la définition de règles de gouvernance, l'outil permet d'administrer les groupes qui bénéficient de

droits d'accès à ces comptes spécifiques, puis d'attribuer et de contrôler des droits d'accès temporaires. Enfin, l'enregistrement des sessions permet de connaître exactement les actions effectuées, facilitant ainsi la compréhension de tout évènement anormal.

Cependant, l'outil PAM, lorsqu'il fonctionne en silo, ne donne aucune visibilité sur les autres droits d'accès de l'utilisateur bénéficiant de ces privilèges. Comment réduire ses habilitations au strict minimum si l'on ne dispose pas d'une vue d'ensemble ? On imagine aisément le risque que représente un utilisateur ayant un accès temporaire au compte « admin » d'une application métier, pour laquelle il possède parallèlement un compte utilisateur et un certain nombre de prérogatives. De même, qu'en est-il des autres comptes partagés qui restent en dehors du périmètre de l'outil PAM ?

Pour remédier à cette problématique, il faut une fois de plus se tourner vers la notion d'identité afin de rassembler toutes les informations relatives à l'utilisateur (groupes, rôles, comptes…). C'est en associant ses systèmes PAM et IAM que l'entreprise sera en mesure de contrôler les droits d'accès à la fois métiers et techniques de ses utilisateurs, en s'appuyant sur un référentiel commun de règles de gouvernance.

5. Génération de modèles d'accès (SOURCE NIST)

a. Discretionary Access Control (DAC/ACL)

Ce modèle consiste à octroyer des droits (idéalement spécifiques ou exceptionnels quand des profils métiers ont été déployés) de manière unitaire en utilisant un workflow d'administration et d'approbation qui permet d'imputer les responsabilités à des acteurs clairement identifiés.

Pour simplifier la revue de ces droits spécifiques et exceptionnels :

- Des dates d'échéance définies par la Gouvernance doivent être appliquées,
- La référence de l'UO dans laquelle l'habilitation a été octroyée doit être obligatoire. Ainsi, en cas de transfert, il sera possible d'identifier simplement les habilitations à révoquer après une période et des modalités définies par la Gouvernance.

b. Role Based Access Control (RBAC)

Ce modèle consiste à occuper des rôles métiers auxquels sont associés :

- Des rôles techniques auxquels sont associés des droits,
- Ou des droits.

Des hiérarchies de rôles peuvent être établies ainsi que des règles de séparation de rôles.

Il est possible de constituer des abstractions de rôles en y associant par exemple la référence d'une UO, d'une fonction et d'un type d'employé.

Un employé peut être désigné comme occupant de rôles statiques dans un workflow de gestion. Des règles peuvent définir une occupation de rôle(s) statique(s).

Des attributs de l'employé peuvent être exploités pour définir l'occupation de rôles dynamiques.

c. Attribute Based Access Control (ABAC)

Ce modèle consiste à combiner des attributs auxquels sont associés :

- Des rôles techniques auxquels sont associés des droits,
- Ou des droits.

Les attributs de l'employé peuvent être exploités :

- Par des règles ABAC/XACML auxquelles sont associées des habilitations,
- Pour rechercher des groupes de sécurité dont les valeurs, l'identifiant par exemple, sont

identiques à celle d'un jeu d'attributs,

- Pour rechercher des groupes d'employés dont les attributs sont identiques, préalablement à l'analyse des habilitations respectueuses du principe du moindre privilège (ABAC dynamique).

d. Policy Based Access Control (PBAC)

Ce modèle d'appuie sur le modèle ABAC et le complète en y intégrant des attributs et des règles correspondant à des politiques de sécurité exploitables notamment vis-à-vis des applications SaaS notamment.

e. Risk Adaptive Access Control (RadAC)

Ce modèle d'appuie sur les modèles précédents et intègre les notions de contexte et de risques associés et supporte des modèles d'habilitation dynamiques.

Ces propositions seront étudiées afin l'identifier le modèle le plus adapté à notre projet. Il apparait cependant nécessaire d'y ajouter des informations liées au GRPD, aux applications particulières, aux workflows à mettre en place, à horodatage et la gestion/centralisation de traces ou preuves, etc.

6. Modélisation d’un méta annuaire IAM/PAM