Gestion des identités et des accès (IAM)

Qu'est-ce que la gestion des identités et des accès ?

L'Identity Access Management (IAM) ou Gestion des Identités et des Accès désigne les processus internes et briques SI liées permettant à une entreprise de **connaitre**, **administrer** et **gérer** les comptes des utilisateurs (collaborateurs internes et prestataires, partenaires, clients, comptes critiques) de son réseau et d'y associer des droits d'accès aux applications et systèmes.

L'IAM permet donc de répondre à plusieurs enjeux clés pour une entreprise : **savoir qui accède à quoi** (et tenir à jour son annuaire pour réévoquer / adapter les droits d'un utilisateur ayant quitté l'entreprise ou simplement changé de poste), **protéger son SI**, **préserver les services critiques ou exposés** de l'entreprise et **assurer une traçabilité** rendue obligatoire par les dernières réglementations (notamment le RGPD).

Quelles sont les ressources mises à disposition pour vous aider à monter en compétences sur le sujet :

- Gestion des habilitations d'accès au SI – PGSSI-S (PDF) ;
- Fiches pédagogiques sur l'authentification (PDF) ;
- Recommandations pour la mise en place d'un cloisonnement système (PDF) ;
- Référentiel général de sécurité de l'ANSSI (PDF).

Les bonnes pratiques et mesures de sécurité :

Afin de protéger son SI, la gestion des identités et des habilitations doit être revue de manière **régulière** pour l'ensemble du périmètre SI.

Principes de gestion des identités & des accès

Identifier : En s'appuyant sur des référentiels, les collaborateurs accédant au SI de l'entreprise doivent être connus. Les utilisateurs sont ceux qu'ils prétendent être à l'aide d'une authentification multi-facteur. Cela combine au moins 2 facteurs indépendants et dont au moins un est non rejouable (sur la base d'un facteur de connaissance, d'un facteur d'appartenance et d'un facteur de possession).

Gestion des autorisations : Des autorisations théoriques doivent être attribuées en fonction des besoins de l'entreprise pour les utilisateurs soit par des règles automatiques, soit par un processus de demande d'autorisation. Ces autorisations correspondent aux autorisations que l'utilisateur doit avoir dans le SI et sont stockées dans un outil de gestion des demandes d'autorisation.

Réconciliation : Sur la base des autorisations théoriques, des autorisations sont appliquées aux utilisateurs du SI. Une réconciliation régulière permet de minimiser les écarts entre les autorisations réelles et théoriques afin de garantir que les utilisateurs disposent uniquement des autorisations légitimes.

Revue des autorisations : La revue des droits permet d'inventorier l'ensemble des autorisations d'un utilisateur et de décider quelles autorisations doivent être conservées, retirées ou modifiées. Selon les revues, la décision peut être prise par le manager de l'utilisateur ou par le responsable du service numérique.

Remédiation : Les modifications effectuées dans le cadre de la revue des autorisations doivent être répercutées dans l'ensemble du SI. Les autorisations théoriques sont donc modifiées au même titre que les droits dans les différents services et applications.