

Résumé

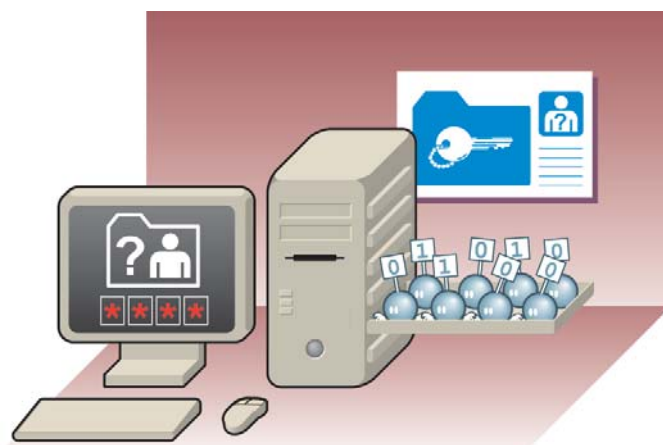
Les comptes utilisateurs constituent la clé de l'accès et d'utilisation des ressources des systèmes d'informations. Les tâches d'administration des systèmes informatiques nécessitent de disposer de privilèges particuliers à la différence des comptes des utilisateurs qui ne doivent disposer que de droits restreints. La gestion des comptes utilisateurs a pour but le maintien d'un niveau de sécurité élevé dans les différents processus de gestion

des identifiants d'accès aux systèmes et aux ressources. Les utilisateurs doivent être sensibilisés aux risques inhérents à l'utilisation des comptes utilisateurs.

Les objectifs principaux de la gestion des comptes sont la prévention et la limitation des fausses manœuvres réalisées par des utilisateurs identifiés et la prévention et/ou le contrôle d'accès par des personnes extérieures non autorisées.

Table des matières

- 1 Qu'entend-on par gestion des comptes ? →
- 2 Les faiblesses habituellement rencontrées →
- 3 Les impacts potentiels →
- 4 Les contre-mesures →



Cette fiche est à mettre en étroite relation avec celle consacrée à l'authentification des utilisateurs sur un système informatique. Toutefois, ce document est plus précisément consacré à la gestion des comptes utilisateurs et non pas à la combinaison identifiant/mot de passe.

Les objectifs principaux de la gestion des comptes sont la prévention et la limitation des fausses manœuvres réalisées par des

utilisateurs identifiés et la prévention et/ou le contrôle d'accès par des personnes extérieures non autorisées.

Les avis prodigués dans ce document sont plus particulièrement orientés vers les plates-formes Unix et Microsoft. Certaines fonctionnalités décrites ne sont applicables qu'à l'un ou l'autre des systèmes et leur configuration peut varier.

1 Qu'entend-on par gestion des comptes?

Sont reprises sous ce titre toutes les tâches liées à la création, la modification et la suppression des profils utilisateurs d'un système informatique, ainsi que des procédures de suivi des comptes.

1.1 Le compte utilisateur

En informatique, les systèmes d'exploitation permettent de gérer des sessions. Lors de la connexion au système, via un identifiant et un mot de passe, le système va ouvrir une session disposant des droits d'accès aux ressources hérités de l'utilisateur qui ouvre la session.

Le compte utilisateur est l'identification d'un utilisateur de façon à lui permettre d'ouvrir une session sur :

- ➔ le domaine réseau et d'accéder aux ressources disponibles sur ce réseau,
- ➔ son ordinateur local afin d'accéder aux ressources locales.

1.2 La création des comptes

Lors de l'installation du système, il y a automatiquement création d'un utilisateur ayant tous les droits sur le système. On parle du compte « administrateur » sur les plates-formes Microsoft et de l'utilisateur « root » sur les plates-formes Unix.

Ordinairement, un second compte de type « invité/guest » est créé. Cet utilisateur par défaut ne bénéficie pas de tous les droits sur le système, mais de droits équivalents à un utilisateur basique.

C'est le rôle de l'administrateur du système de créer les autres comptes pour les utilisateurs et de leur définir un certain niveau de droits sur le système.

→ suite

→ **CONSEIL:**

Ces deux utilisateurs présents par défaut sur toutes les implémentations sont des cibles pour les hackers. Il est donc vivement conseillé de ne pas utiliser ces comptes pour l'exécution de tâches ne nécessitant pas de privilèges particuliers et de renommer ces comptes utilisateurs privilégiés afin que ces noms par défaut connus de tous ne soient pas exploitables par des pirates informatiques et de supprimer les comptes utilisateurs qui ne sont plus utilisés soit par le départ ou la mutation d'un collaborateur soit par la création de comptes utilisateurs par défaut lors de l'installation ou de la configuration du systèmes ou d'applications.

1.3 Le profil

On parle de profil pour définir les droits donnés à un utilisateur.

Dans la pratique et pour gérer les utilisateurs de manière optimale, il est conseillé d'utiliser des groupes d'utilisateurs. Certains groupes sont d'ailleurs créés par défaut à l'initialisation du système.

Les droits sont alors appliqués au groupe et le seul fait d'appartenir à ce groupe fait hériter des pouvoirs de ce groupe. Cette méthode de travail permet de créer et de gérer plus facilement des utilisateurs selon leur fonction et limite la propagation de profils complexes ou uniques non gérables dans la pratique (RBAC pour Role-Bases Access Control).

1.4 Les noms à choisir

Dans ce domaine, il faut faire la part entre les soucis de sécurité et la facilité d'usage de ces identifiants. Toutefois, un grand principe de base est incontournable: l'identifiant devra absolument être unique au sein d'un domaine ou sur un ordinateur personnel.

Le choix s'oriente ordinairement vers une combinaison entre le nom de famille et les initiales du prénom.

→ **CONSEIL:**

Ne pas indiquer visiblement dans cet identifiant la fonction de l'utilisateur car cela permettrait à une personne mal intentionnée de cibler ses attaques sur une fonction offrant des avantages potentiels.

1.5 Les comptes critiques

Les comptes ne sont critiques que par les pouvoirs qui sont liés à leur profil. Toutefois, on peut dire que certains comptes revêtent toujours un haut niveau de criticité. Ce sont les comptes :

- administrateur du système, des équipements, des bases de données,
- utilisateurs bénéficiant d'un accès distant,
- des employés du service informatique,
- utilisés par des applications pour converser entre elles.

1.6 Les autres paramètres liés au compte utilisateur

En dehors des droits directement définis pour le compte, et des droits hérités par l'appartenance à certains groupes, on peut définir d'autres paramètres, tels que :

- un répertoire de stockage privé,
- une date de validité du compte,
- les caractéristiques du poste de travail (Microsoft : « my desktop »),
- différents paramètres de gestion du mot de passe.

2

Les faiblesses habituellement rencontrées

La faiblesse des comptes est une des failles principales exploitées lors d'attaques sur un système informatique. Ces faiblesses sont situées à deux niveaux :

- gestion des combinaisons identifiant/mot de passe,
- mauvaise gestion des comptes utilisateurs sur le système.

On trouve ci-dessous une liste non exhaustive des faiblesses les plus souvent rencontrées lors de missions de validation de systèmes informatiques :

2.1 Multiplication de comptes « partagés »

Pour différentes raisons fonctionnelles, il est courant de trouver des comptes partagés par plusieurs utilisateurs. Ce phénomène est souvent présent au sein des équipes informatiques et cela ne fait qu'augmenter le risque lié à cette situation.

Cet identifiant étant partagé, on remarque également que les changements du mot de passe associé ne sont pas fréquents.

2.2 Multiplication de comptes avec des droits d'administrateur

La multiplication de comptes administrateurs augmente le risque de problèmes de sécurité et de fiabilité de par la multiplicité des comptes disposants de privilèges importants et donc de la probabilité pour un pirate de trouver un compte administrateur doté d'un mot de passe suffisamment simple pour le deviner aisément et donc pouvoir disposer de droits privilégiés sur le système.

2.3 Sessions multiples par compte utilisateur

Il est possible d'autoriser l'ouverture de multiples sessions concurrentes avec un même compte. Il en résulte fréquemment que des sessions restent ouvertes sur des machines, sans être utilisées et donc utilisables par des personnes non-autorisées pouvant se révéler malintentionnées.

2.4 Absence complète de la gestion des comptes

Il n'est pas rare que la gestion des comptes soit carrément inexistante, ce qui a pour conséquence directe que des comptes

restent ouverts pour des personnes ne faisant plus partie de la société. Certains de ces comptes bénéficient parfois de hauts niveaux de pouvoir et même de possibilités d'accès distant.

Cet état de fait est également souvent lié à une absence de surveillance des logs qui permettraient de détecter d'éventuelles tentatives de connexions frauduleuses.

2.5 Inconsistance de la gestion des comptes

Le refus d'utilisation de la notion de groupes mène à la création de multiples profils personnels pouvant disposer de privilèges et de droits d'accès attribués empiriquement ce qui rend ces comptes utilisateurs uniques de par leurs accès aux systèmes, lesquels deviennent très difficiles, voire impossibles à gérer. La création de groupes en correspondance avec les fonctions des utilisateurs (service ventes, comptabilité, par exemple), permet d'attribuer, mais aussi de supprimer, des droits de façon très aisée, fiable et efficace.

3 Les impacts potentiels

Les impacts des faiblesses décrites dans le chapitre 2 sont assez faciles à imaginer puisque qu'ils reviennent à rendre public un système de traitement d'informations et toutes les données et applications qui le constituent.

Dans un scénario catastrophe, on peut imaginer la perte complète du contrôle du système sans autre solution que de tout recommencer à zéro en formatant le disque dur à cause de la corruption du système pouvant même jusqu'à rendre impossible la reprise du contrôle dudit système par les administrateurs.

4 Les contre-mesures

Quelques conseils de base quant à la gestion des comptes utilisateurs sont repris ci-après :

4.1 Mise en place d'une politique de gestion des comptes

Seule la mise en place de procédures de gestion des comptes et leur contrôle permettent d'assurer un niveau de sécurité par défaut satisfaisant pour la majorité des comptes. Les exceptions nécessitant ensuite une étude spécifique.

Le respect de ces procédures exige un minimum de collaboration entre le service informatique et celui des ressources humaines en charge des engagements, transferts et licenciements.

L'audit annuel de la gestion des comptes par des personnes extérieures à l'équipe en charge de l'informatique permet également de parer aux omissions et erreurs humaines en ce domaine en

apportant un œil neuf sur les processus en production et les droits et privilèges attribués aux utilisateurs.

4.2 Utilisation des fonctions d'audit intégrées

La plupart des systèmes offrent la possibilité de produire des fichiers d'audit du système reprenant les informations relatives aux comptes, aux tentatives de création, de modification, d'effacement et de connexion des utilisateurs.

La consultation de ces rapports peut mettre en avant des problèmes, des défauts et des aspects singuliers relatifs à la gestion des comptes tels que par exemple des comptes utilisateurs se connectant durant les horaires de fermeture de l'organisation (la nuit et le week-end) pouvant révéler une corruption de ces comptes utilisateurs. Une investigation sera alors à mener pour en comprendre les raisons.

[→ suite](#)

4.3 Éviter les connexions multiples et les comptes partagés

Il est préférable de créer des profils sur mesure en fonction du rôle des informaticiens, plutôt que d'utiliser un seul compte bénéficiant des pleins pouvoirs.

En effet, les pouvoirs limités permettent parfois de faire face à des réactions imprévues lors d'installations (effacement de fichiers).

De plus, l'utilisation de comptes non partagés peut permettre dans le respect des lois et de la réglementation en vigueur d'identifier l'auteur d'une erreur ou de malversations, alors que les comptes partagés empêchent tout pistage.

4.4 Utilisation de comptes séparés pour les connexions distantes

Il est courant que les informaticiens se connectent de leur domicile pour contrôler le bon fonctionnement de certains processus. Il est conseillé de créer des comptes dédiés à cet usage « remote » (à distance) et différents des comptes utilisés quand ces utilisateurs/administrateurs se connectent quand ils sont physiquement présents au sein de la société. Ces comptes d'accès à distance doivent bénéficier de fonctionnalités et de privilèges minimaux et doivent être soumis de la manière la plus stricte aux règles d'usage des identifiants et de l'utilisation des ressources mises à leur disposition de manière à éviter tout problème de part leur situation en dehors de la zone de sécurité mise en place pour les utilisateurs au sein la société, ce qui a pour effet de les positionner en première ligne pour d'éventuelles attaques de pirates informatiques.