# Sécurité des comptes d’administration

*Mis à jour le 08/10/2024*

## Qu'est-ce qu'un compte d'administration ?

**Les comptes d'administration** sont des comptes dotés de privilèges étendus et d'autorisations spécifiques dans un SI.

- Ces comptes sont utilisés par les administrateurs pour effectuer des tâches de gestion, de configuration et de maintenance.
- Ils permettent un accès privilégié à des fonctions sensibles et à des ressources critiques, telles que la création de comptes utilisateur, l'installation de logiciels, la configuration des paramètres, etc.

## Risques associés à la compromission des comptes d’administration :

La compromission des comptes d'administration entraîne des risques majeurs :

- **Accès non autorisé :** Les attaquants peuvent exploiter les comptes compromis pour accéder à des ressources sensibles, avec la possibilité d'escalade de privilèges et de contournement des contrôles de sécurité.
- **Fuites de données :** Les comptes administrateurs ayant potentiellement accès à des données critiques non accessibles aux utilisateurs standard, ils représentent un risque plus élevé de fuite de données.
- **Interruptions de service :** Les attaquants peuvent perturber les services essentiels en bloquant l'accès à des utilisateurs légitimes ou en perturbant les opérations métier.
- **Impact sur les services critiques :** La compromission des comptes d'administration peut avoir un impact direct sur les services critiques, pouvant entraîner des conséquences graves telles que des pertes financières et une détérioration de la réputation de l'organisation.
- **Compromission étendue du SI** : Du fait de leurs droits et accès privilégiés, la compromission des comptes d’administration peut s’étendre plus largement à l’ensemble du système.


## Bonnes pratiques dans le cadre de la gestion des comptes d’administration

Pour minimiser les risques associés à la compromission des comptes d’administration, il est essentiel de mettre en place certaines pratiques :

- **Limiter le nombre de comptes d’administration :** Restreignez les droits d’administration uniquement aux individus nécessitant un tel accès, et ce, uniquement pour la durée strictement nécessaire.
- **Principe du moindre privilège :** Accorder uniquement les privilèges nécessaires à chaque utilisateur afin de limiter les risques de sécurité en réduisant la surface d'attaque potentielle.
- **Gradation des privilèges :** Tout compte possédant des droits plus élevés n’est pas nécessairement administrateur.
- **Séparation des environnements de travail :** Les administrateurs doivent utiliser des postes de travail dédiés exclusivement aux tâches d’administration.
- **Authentification multi-facteurs (MFA) :** Mettez en œuvre de l'authentification multi-facteurs pour renforcer la sécurité de la connexion des comptes d’administration.
- **Surveillance des journaux d'événements :** Il est important de surveiller régulièrement les actions effectuées par les comptes d’administration afin de détecter toute activité suspecte : heures et statuts des connexions, usages, outils… L’information doit être collectée en détails et être consultée.
- **Tenue à jour de l'inventaire des comptes à privilèges :** Assurez-vous que l'inventaire des comptes à privilèges est constamment à jour pour garantir une gestion efficace de ces comptes.
- **Suppression des comptes inutilisés :** Les comptes des utilisateurs à privilèges qui quittent l'entreprise doivent être immédiatement désactivés pour éviter tout risque de compromission future.

## Ressources pertinentes

- Guide de **l’ANSSI** autour des bonnes pratiques de la gestion de l’administration [PDF]