CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Gestion et contrôle des privilèges d'administrateur

Juin 2024 **ITSAP.10.094**

Une utilisatrice ou un utilisateur ayant des privilèges d'administrateur a plus de contrôle pour modifier, personnaliser ou supprimer des données sur un système informatique ou un réseau. Souvent, les organismes accordent ces privilèges élevés aux comptes utilisateur généraux. Cette pratique offre aux auteures et auteurs de menace externes, de même qu'aux menaces internes et non intentionnelles, un autre moyen de compromettre les réseaux de l'organisme. Quand votre organisme gère et contrôle mieux ses privilèges d'administrateur, il peut réduire son exposition aux cybermenaces communes.

Pourquoi les auteures et auteurs de menace ciblent les privilèges d'administrateur

Si des auteures et auteurs de menace obtiennent l'accès à un compte d'administrateur, ils seront en mesure de faire ce qui suit :

- utiliser les privilèges élevés pour nuire à l'environnement opérationnel de votre organisation;
- détériorer ou interrompre un trafic réseau;
- accéder à de l'information sensible.

Les auteures et auteurs de menace peuvent aussi découvrir quels mécanismes de détection et de reprise sont en place sur vos systèmes, ce qui les aide à les contourner et vous empêche de prévenir d'autres attaques.

Techniques utilisées pour accéder aux privilèges d'administrateur

Les auteures et auteurs de cybermenace ont recours à différentes techniques pour obtenir des informations d'identification de compte qu'ils pourront utiliser afin d'accéder à des réseaux et à des systèmes. Les compromissions initiales découlent souvent des activités normales d'une utilisatrice ou un utilisateur, comme ouvrir des pièces jointes malveillantes dans des courriels ou visiter des sites Web non sécurisés. Les auteures et auteurs de menace peuvent aussi exploiter des vulnérabilités connues pour élever leurs privilèges ou utiliser des justificatifs d'identité volés pour accéder aux comptes d'administrateur.

Certaines méthodes d'attaques courantes mènent à la compromission des comptes d'administrateur.

Maliciels et hameçonnage : Les auteurs et auteurs de menace accèdent aux comptes d'administrateur locaux ou de domaines en envoyant un courriel contenant des pièces jointes malveillantes ou des liens vers des sites malveillants. Lorsqu'une utilisatrice ou un utilisateur ayant des privilèges d'administrateur ou étant connecté en tant qu'administratrice ou administrateur ouvre le courriel ou visite le site, l'auteure ou auteur de menace peut alors exploiter les justificatifs d'identité d'administrateur pour déployer des maliciels sur votre système.

Cassage de mot de passe : Les auteures et auteurs de menace peuvent tenter d'accès aux comptes directement en menant des attaques par cassage de mot de passe, comme les suivantes :

- une **attaque par force brute** dans le cadre de laquelle une ou un auteur de menace utilise des outils automatisés pour trouver un mot de passe en essayant des combinaisons courantes;
- une **attaque par dictionnaire** dans le cadre de laquelle une ou un auteur de menace emploie une liste de mots souvent utilisés pour deviner le mot de passe.

Élévation des privilèges : Les auteures et auteurs de menace exploitent les vulnérabilités de votre système ou de votre réseau en tirant avantage des applications et des dispositifs auxquels les plus récents correctifs de sécurité n'ont pas été appliqués pour obtenir des privilèges élevés dans vos systèmes d'information.

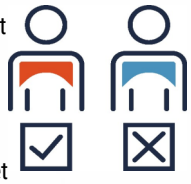
Attaque « Pass-the-Hash » : Les auteures et auteurs de menace peuvent réinsérer les justificatifs d'authentification hachés de l'utilisatrice ou utilisateur, comme un mot de passe, sur un poste de travail compromis. Ces justificatifs d'identité hachés permettent à l'auteure ou auteur de menace de se déplacer latéralement dans le réseau. Le hachage des justificatifs d'identité consiste à modifier les données lisibles qu'ils contiennent en caractères désordonnés au moyen d'un algorithme. Sans des mesures d'atténuation appropriées, des justificatifs d'identité hachés peuvent toutefois être réinsérés pour créer une nouvelle session de connexion.

SÉRIE SENSIBILISATION

No de cat. D97-1/10-094-2024F-PDF
ISBN 978-0-660-69995-0

Facteurs à considérer pour sécuriser les comptes d'administrateur

Votre organisme doit prendre les mesures suivantes lorsqu'il assigne des comptes d'administrateur ou des privilèges d'accès aux utilisatrices et utilisateurs :



- respecter le principe du droit d'accès minimal en accordant uniquement les accès nécessaires afin que l'utilisatrice ou utilisateur puisse accomplir ses tâches;
- créer des comptes d'administrateur qui sont distincts des comptes d'accès réguliers des utilisatrices et utilisateurs et qui n'ont pas accès à Internet ou aux courriels :
  - s'assurer que les tâches administratives sont effectuées sur des consoles administratives dédiées;
  - s'assurer que l'accès à distance aux comptes privilégiés s'effectue à partir de consoles dédiées;
- utiliser des méthodes d'authentification robustes :

  - utiliser une authentification multifacteur pour tous les comptes d'administrateur;
  - utiliser un mot de passe ou une phrase de passe unique pour chaque compte privilégié;
  - modifier les mots de passe par défaut pour les applications et les dispositifs;
  - authentifier les utilisatrices et utilisateurs avant qu'ils obtiennent l'accès aux applications ou aux dispositifs;
- mettre en place l'intégrité par deux personnes (TPI pour Two-Person Integrity) et la double authentification :

  - au moins deux personnes autorisées doivent simultanément accéder au système pour effectuer une tâche critique conformément au principe de la TPI;
  - au moins deux personnes autorisées doivent approuver les changements avant qu'ils ne soient apportés au système;
- veiller à ce que des comptes uniques et identifiables soient remis à chaque utilisatrice ou utilisateur;
- consigner et surveiller les activités effectuées sur les comptes privilégiés;
- offrir de la formation sur les comportements attendus aux utilisatrices et utilisateurs de comptes privilégiés;

- supprimer ou retirer les privilèges d'accès spéciaux quand une utilisatrice ou un utilisateur n'en a plus besoin.

Gestion des comptes non administratifs

Les auteures et auteurs de menace ne veulent pas uniquement accéder aux comptes d'administrateur. Ils exploiteront le moindre compte d'utilisateur dans le but d'obtenir un accès au plus grand nombre de comptes possible.

Le fait que votre organisme gère et contrôle les comptes et les privilèges d'administrateur crée un environnement opérationnel à la fois stable, fiable et plus facile à soutenir. Une bonne gestion des comptes et un contrôle approprié des accès font en sorte que moins d'utilisatrices et utilisateurs peuvent apporter des changements importants à l'environnement opérationnel.

Si les utilisatrices et utilisateurs n'ont accès qu'aux systèmes et aux renseignements dont ils ont besoin pour exécuter leurs tâches, votre organisation sera mieux protégée contre les auteures et auteurs de menace externes. Gérer les autorisations des utilisatrices et utilisateurs permettra également de limiter les répercussions de menaces internes non intentionnelles ou malveillantes.

Renseignements supplémentaires

Pour obtenir de plus amples renseignements, veuillez consulter nos autres publications :

- *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.189)*
- *Les 10 mesures de sécurité des TI :No 3 – Gestion et contrôle des privilèges d'administrateur (ITSM.10.094)*
- *Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)*
- *Comment protéger votre organisation contre les menaces internes (ITSAP.10.003)*
- *Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)*
- *Étapes à suivre pour déployer efficacement l'authentification multifacteur (ITSAP.00.105)*
- *Offrir aux employés une formation sur mesure en cybersécurité (ITSAP.10.093)*

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.