Devolutions

7 types de comptes privilégiés que les organisations doivent protéger et surveiller

LE TEMPS MOYEN POUR DÉTECTER UNE VIOLATION EST DE 197 JOURS

Les entreprises s'appuient sur des comptes privilégiés pour accroître leur productivité et leur efficacité. Malheureusement, les pirates s'appuient également sur des comptes privilégiés vulnérables pour s'en prendre aux réseaux, accéder aux systèmes critiques et voler des données confidentielles - souvent tout en restant cachés pendant des mois, voire des années. Une enquête mondiale réalisée par le Ponemon Institute pour le compte d'IBM a révélé que le temps moyen pour détecter une violation est de 197 jours et qu'il faut en moyenne 69 jours supplémentaires pour contenir les dommages.

Compte tenu de tout ça - c'est-à-dire que les entreprises s'appuient de plus en plus sur des comptes privilégiés, tandis que les pirates les ciblent de plus en plus - il n'est pas surprenant que Gartner ait identifié la gestion des accès privilégiés (PAM) parmi ses 10 principaux projets de sécurité pour 2019.

Plus précisément, Gartner recommande que les projets PAM incluent des comptes de systèmes humains et non humains, tout en prenant en charge une combinaison d'environnements en nuage, locaux et hybrides, ainsi que des API pour l'automatisation.

Malgré l'importance vitale de la gestion des comptes privilégiés pour garantir la sécurité et le fait que 74% des violations de données proviennent d'une utilisation frauduleuse d'identifiants de comptes privilégiés, le rapport 2019 de Thycotic sur l'état de la gestion des accès privilégiés a révélé les faits surprenants et alarmants suivants :

- 55 % des organisations ne savent pas combien ils ont de comptes privilégiés et où ils sont situés.
- Plus de 50% des comptes privilégiés dans les organisations n'expirent jamais ou ne sont pas supprimés.
- 72% des organisations ne stockent pas tous leurs comptes privilégiés dans un coffre sécurisé ou dans un gestionnaire de mots de passe.

De nombreux facteurs contribuent à cette négligence par rapport à la gestion des comptes privilégiés (au grand plaisir des pirates informatiques). Par exemple, le fait que de nombreuses organisations - en particulier les PME qui n'ont pas assez de personnel spécialisé en cybersécurité à l'interne - ne comprennent pas clairement quels types de comptes sont considérés comme « privilégiés ».

Pour combler ce manque de connaissances, voici sept types de comptes privilégiés que toutes les organisations doivent sécuriser et surveiller afin de protéger leurs données, leurs clients et leur réputation :

1. Comptes d'administrateurs de domaine

Les comptes d'administrateurs de domaine détiennent les « clés du royaume », parce qu'ils ont le contrôle de l'ensemble du domaine Active Directory (tous les contrôleurs, postes de travail et serveurs membres). Il va sans dire - mais il n'y a pas de mal à le répéter - que l'accès aux comptes d'administrateurs de domaine devrait être accordé seulement si nécessaire. N'oubliez pas : il y a une raison pour laquelle les comptes d'administrateurs de domaine compromis sont largement reconnus comme le pire scénario dans le monde de la sécurité informatique. Pour bien comprendre, imaginez le scénario le plus catastrophique et multipliez-le par 10.

2. Comptes d'utilisateurs privilégiés

Comme son nom l'indique, les comptes d'utilisateurs privilégiés accordent plus de privilèges - et donc plus de risques - que les comptes d'utilisateurs ordinaires sur un ou plusieurs systèmes. Par exemple, les utilisateurs peuvent modifier ou supprimer des logiciels, changer les configurations d'application, etc.

Dans de nombreux cas, les comptes d'utilisateurs privilégiés ne sont pas attribués à un utilisateur spécifique, mais ils sont plutôt partagés entre les administrateurs. La règle de base est la suivante: tout compte qui accorde aux utilisateurs autre chose qu'un compte standard est considéré comme un compte privilégié et doit être géré et surveillé en conséquence. En fait, de nombreux experts en sécurité de l'information estiment que les comptes d'utilisateurs privilégiés représentent le type d'accès privilégié le plus risqué, parce qu'ils sont courants, accordent un accès aux données sensibles et peuvent être facilement compromis par des pirates informatiques.

3. Comptes administrateur locaux

Les comptes administrateur locaux accordent un accès de niveau administrateur aux appareils locaux et sont généralement utilisés par les équipes informatiques pour configurer de nouveaux postes de travail et effectuer des tâches de maintenance. Les pirates ciblent souvent les comptes administrateur locaux vulnérables pour établir un point d'ancrage à l'intérieur d'un réseau. À partir de là, ils évaluent les outils et systèmes de défense de la cybersécurité de leurs victimes avant de lancer une attaque.

4. Comptes d'accès d'urgence

Beaucoup de gens cachent une clé de rechange quelque part à l'extérieur de leur maison, « juste au cas où » ils s'embarreraient dehors. Dans le même esprit, de nombreuses entreprises créent des comptes d'accès d'urgence pour les systèmes sécurisés. Ceux-ci sont généralement désactivés par défaut jusqu'à ce qu'un incident critique se produise - comme une cyberattaque. Dans ce cas, certains utilisateurs spécifiques peuvent accéder à ces comptes pour restaurer les systèmes et récupérer les journaux d'utilisation. Les comptes d'accès d'urgence (parfois appelés comptes «break glass » ou comptes « firecall ») sont hautement privilégiés et doivent absolument être gérés via une stratégie et une solution PAM.

5. Comptes d'application

Les comptes d'application sont utilisés par les applications pour accéder à diverses ressources fonctionnelles comme les bases de données et les réseaux. Ils sont également utilisés pour effectuer des tâches automatisées comme les mises à jour logicielles. Habituellement, les mots de passe du compte d'application sont stockés dans des fichiers texte non chiffrés sur le réseau, afin qu'ils puissent être rapidement et facilement récupérés par les utilisateurs au sein de l'entreprise. Malheureusement, les pirates ciblent des vulnérabilités connues (et non corrigées) pour voler ces mots de passe et établir un accès à distance. Ils peuvent alors modifier les fichiers binaires du système et même élever les comptes standards en comptes privilégiés pour se déplacer à travers le réseau.

6. Comptes système

Les comptes système sont utilisés par les services et les applications (au lieu des utilisateurs humains) pour lancer des processus et exécuter des tâches planifiées. La bonne nouvelle est que les comptes système n'ont généralement pas la possibilité de se connecter aux systèmes. La mauvaise nouvelle est qu'ils ont souvent des mots de passe qui ne changent jamais, parce que les entreprises les oublient complètement ou ne connaissent même pas leur existence. Ainsi, les comptes système sont fréquemment ciblés par des pirates, qui lancent des fichiers binaires avec des privilèges élevés pour mener leurs attaques.

7. Comptes de services (domaine)

Les comptes de services permettent à diverses applications et systèmes de communiquer et d'accéder à différentes ressources, d'exécuter des rapports, etc. Ils sont généralement utilisés pour mettre à jour les correctifs de sécurité, les sauvegardes et le déploiement de logiciels. Le problème est que la modification du mot de passe sur un compte de services le déconnecte ensuite des applications et du système, jusqu'à ce qu'il soit synchronisé dans l'environnement. En conséquence, de nombreuses organisations modifient rarement, voire jamais, le mot de passe, ce qui est précisément ce sur quoi les pirates comptent.

Conclusion

Les PME doivent sécuriser et surveiller TOUS leurs comptes privilégiés. Ne pas le faire peut entraîner des violations de données coûteuses, des dommages persistants à la réputation et, dans certains cas, une fermeture définitive.

En effet, 6 PME sur 10 mettent la clé dans la porte dans les six mois suivant une cyberattaque.

Chez Devolutions, nous avons pour mission d'aider les PME à protéger leurs données, leurs clients et leur réputation. Nous avons travaillé en étroite collaboration avec deux cabinets d'analystes bien connus, et un **nouveau composant PAM est désormais intégré à la dernière version de Devolutions Password Server! Découvrez comment l'activer ici**.

Cette plateforme vise à « démocratiser » la gestion des comptes privilégiés en la rendant abordable et accessible aux PME partout dans le monde. Elle répond à toutes les exigences fondamentales, tout en reflétant notre engagement en matière de performance, de convivialité, de sécurité et de soutien. Restez à l'affût des mises à jour qui seront publiées dans les semaines et les mois à venir!