ManageEngine
PAM360

Sécuriser les comptes de services Windows grâce à des contrôles d'accès efficaces

Les comptes de service sont des comptes de domaine privilégiés, utilisés par des applications ou des services critiques pour interagir avec leurs systèmes d'exploitation et pour exécuter des fichiers batch, des tâches planifiées et des applications hébergées dans des bases de données, des systèmes de fichiers et des périphériques. Ces comptes sont contrôlés par des utilisateurs "non humains", tels que des systèmes, des scripts, des applications, et sont généralement dotés de privilèges élevés pour les applications critiques, les bases de données, les services web, les API, etc.

Catégories de comptes de service

Type de compte	Description
Partagé	Comptes utilisés par deux utilisateurs ou plus sur un système. Les informations d'identification du compte sont partagées entre les utilisateurs.
Système	Également connu sous le nom de "superutilisateur" ou de comptes privilégiés. Ces comptes administratifs sont utilisés pour permettre les communications et les processus au sein du système d'exploitation (par exemple, root sous UNIX).
Non-interactif	Comptes utilisés pour exécuter des processus et des services système, tels que l'exécution de scripts automatisés, de fichiers batch et de tâches planifiées. Les utilisateurs finaux ne peuvent pas se connecter à ces comptes.

Note: Il pourrait y avoir d'autres sous-classifications de comptes qui pourraient entrer dans les catégories de comptes d'exploitation et de services.

Risques de sécurité liés aux comptes de service

La mauvaise gestion des comptes de service peut présenter des risques importants pour la sécurité des entreprises, et ce pour plusieurs raisons.

Trop complexe pour une gestion manuelle

Les comptes de service, bien que simples à configurer et à utiliser, sont étroitement interconnectés et partagés avec plusieurs applications et services. En outre, ils sont référencés dans de multiples instances à travers plusieurs actifs et applications, ce qui rend la gestion de ces comptes si complexe que le moindre oubli dans la chaîne de dépendances pourrait provoquer des défaillances en cascade.

Porte dérobée vers des informations privilégiées

Les comptes de service sont, le plus souvent, liés à des applications critiques et peuvent donc nécessiter un accès privilégié aux serveurs, aux bases de données et à d'autres actifs. Avec un seul compte compromis, les attaquants peuvent prendre le contrôle complet des actifs privilégiés, des terminaux et des informations sensibles partagées.

Cible facile et de grande valeur pour les attaquants

Étant donné que les comptes de service sont principalement utilisés par des entités non humaines pour effectuer des opérations, les contrôles de sécurité tels que l'authentification à deux facteurs (TFA) ne peuvent pas être appliqués, car ils nécessitent une interaction humaine à des fins d'authentification. Pour compliquer les choses, les mots de passe des comptes de service sont définis pour rester permanents, car une rotation fréquente des mots de passe de ces comptes peut entraîner des blocages et des perturbations imprévus. Par conséquent, les comptes de service deviennent une cible facile et lucrative pour les attaquants.

Cycle de vie de la gestion des comptes de service : Pour commencer

Au fur et à mesure que les organisations se développent, la gestion manuelle des comptes de service devient difficile et laborieuse en raison du nombre d'applications et de services auxquels ils accèdent. En raison de l'omniprésence et de la prolifération des comptes de service, et du risque toujours plus élevé qu'ils constituent une cible facile, il est important de surveiller, d'administrer et d'auditer activement l'utilisation de ces comptes. Pour que les organisations puissent identifier et contrecarrer d'éventuelles exploitations de comptes de service, elles devront mettre en œuvre un plan d'action qui trouve un juste équilibre entre les opérations et la sécurité.

Si les outils de gouvernance et d'administration des identités (IGA) aident à gérer les identifiants des des comptes individuels privilégiés, ils ne permettent pas de gérer les comptes de service qui sont liés à des entités non humaines. Voici quelques bonnes pratiques pour vous aider à gérer et à protéger efficacement vos comptes de service contre les attaques. protéger vos comptes de service contre les attaques.

1. Découvrez les comptes de service de votre organisation.

Vous ne pouvez pas protéger vos comptes de service si vous ne les avez pas encore identifiés. La première étape de la sécurisation des comptes de service consiste à les découvrir sur le réseau et dans les applications, et à identifier les activités qui y sont liées. Cela aidera les administrateurs informatiques à découvrir et à renforcer les failles de sécurité qui permettent d'accéder aux données privilégiées par une porte dérobée.

2. Dresser un inventaire des informations d'identification et des dépendances des comptes de service.

Pour établir la responsabilité et le contrôle des comptes de service, Les administrateurs informatiques doivent dresser un inventaire des applications, utilisateurs et services associés qui dépendent des comptes de service. des applications, des utilisateurs et des services associés qui dépendent des comptes de service respectifs. comptes de service respectifs. Les organisations doivent suivre les étapes suivantes étapes suivantes pour établir un inventaire des comptes de service :

- Établir un flux de travail clair pour la création de comptes de service, l'intégration et le suivi de l'utilisation.
- Analyser régulièrement l'environnement applicatif pour découvrir les nouveaux comptes de service, ainsi que les services, les applications et les autres comptes de service auxquels ils sont connectés.
- Veiller à ce que les informations d'identification des comptes de service fassent l'objet d'une rotation et d'une mise à jour régulières, conformément aux politiques standard en matière de mots de passe.
- Examiner l'état des comptes de service : actifs, inactifs et supprimés. S'assurer que les comptes de service expirés sont supprimés du réseau.

3. Accès sécurisé aux comptes de service.

Pour contrer les risques d'abus des comptes de service, les organisations devraient fortement envisager d'investir dans des solutions de gestion des accès privilégiés (PAM), qui aident à rationaliser la gestion du cycle de vie des comptes de service. Les outils PAM permettent aux administrateurs IT de développer une gouvernance forte sur les comptes de service répartis sur le réseau de l'entreprise en utilisant des automatisations efficaces pour découvrir, sécuriser et surveiller l'accès à ces comptes. Une solution PAM solide fournit un coffre-fort sécurisé pour stocker et faire pivoter les informations d'identification des comptes de service, et permet de partager les mots de passe avec des utilisateurs non administrateurs en fonction d'exigences spécifiques. Cela permet d'éviter l'accès non autorisé non autorisés aux comptes de service et protège ces comptes contre l'utilisation abusive des privilèges.

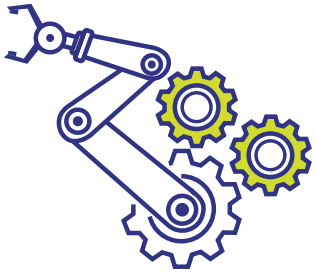
L'intégration des outils PAM avec les outils SIEM et les outils d'analyse informatique permet aux administrateurs IT de surveiller l'activité des utilisateurs avec ces comptes. comptes, d'identifier et de contenir les comportements anormaux, et de de conformité en générant des rapports en temps réel.

4. Mettre en place une gouvernance des comptes de service.

Il est important pour les organisations d'affirmer leur gouvernance sur les comptes de service et les mots de passe en mettant en place des contrôles de sécurité spécifiques basés sur les politiques et les normes existantes. Il s'agit notamment d'attribuer la propriété, les rôles et les responsabilités aux utilisateurs privilégiés, et de déléguer la propriété à l'aide d'un système de partage basé sur les rôles pour les utilisateurs, les propriétaires, les administrateurs et les superadministrateurs (approbateurs). Outre la formation et l'éducation des utilisateurs, les organisations doivent établir un flux de travail bien défini pour les processus de création, de révision et de mappage des comptes de service afin d'obtenir une visibilité complète sur ces comptes.

Le flux de travail du compte de service doit répondre aux questions suivantes questions :

- Qui doit créer les comptes de service et qui doit en approuver l'accès ?
- Qui sera le propriétaire par défaut des comptes de service ?
- À quelle fréquence ces comptes seront-ils examinés ? Le processus d'examen sera-t-il aligné sur la politique interne et/ou les exigences de conformité ?
- Quelle sera la politique en matière de mots de passe pour les comptes de service ?
- Si un compte de service doit être renouvelé, doit-il faire l'objet d'une procédure d'approbation similaire à celle de la création d'un compte ?
- Existe-t-il une disposition permettant de mettre automatiquement hors service les comptes de service expirés/inactifs ?



5. Adopter l'automatisation.

L'établissement d'un flux de travail tangible peut rationaliser la gestion des comptes de service, mais il est presque impossible de gérer l'ensemble du cycle de vie de chaque compte dans un environnement à grande échelle. C'est là que l'automatisation entre en jeu.

Une fois qu'un flux de travail bien défini est mis en place, les organisations peuvent tirer parti d'outils d'automatisation capables de centraliser la gestion des comptes de service. Ces outils permettent aux administrateurs IT d'exercer un contrôle granulaire sur les comptes de service et de gérer le cycle de vie complet des comptes, de la découverte automatique à la création de modèles de flux de travail conformes aux politiques internes, en passant par la fourniture de rapports de conformité permettant d'atteindre les objectifs de sécurité.

L'automatisation de la gestion des comptes de service permet aux administrateurs privilégiés de créer et de réviser les utilisateurs, les groupes et les rôles désignés, ainsi que de sécuriser l'accès aux comptes de service. Certains outils d'automatisation permettent aux administrateurs de provisionner et de déprovisionner automatiquement les comptes de service et leur offrent la possibilité de personnaliser leurs flux de travail en fonction des exigences spécifiques de l'entreprise et du type de demande de compte de service.

Pour prévenir les abus de manière proactive, les outils d'automatisation fournissent des rapports d'état en temps réel pour les comptes de service et aident les administrateurs à déclasser les comptes expirés ou inactifs sans perturber les opérations. En outre, ces outils informent les administrateurs de la création, de l'approbation, du renouvellement et de la suppression des comptes de service.

ManageEngine PAM360

ManageEngine PAM360 est une solution unifiée de gestion des accès privilégiés pour les entreprises. Elle permet aux administrateurs IT et aux utilisateurs privilégiés d'obtenir un contrôle granulaire et complet sur les ressources informatiques critiques, telles que les mots de passe, les signatures numériques et les certificats, les clés de licence, les documents, les images, les comptes de service, etc.

Reconnu par Gartner et Forrester comme l'un des meilleurs fournisseurs de PAM de 2020, ManageEngine PAM360 comprend des intégrations contextuelles avec des solutions SIEM, de ticketing et d'analyse pour aider les équipes informatiques à élaborer des modèles de comportement des utilisateurs afin d'identifier et de mettre fin aux activités anormales, de générer des rapports d'audit et de conformité complets et de prendre des décisions de sécurité basées sur des données.

www.manageengine.fr/pam360

PG Software EUROPE
mail : commercial@pgsoftware.fr
site web : manageengine.fr
téléphone : 0 805 296 540 Service & appel gratuits

ManageEngine
PAM360