Projet Sécurité des Réseaux :

Gestion des Comptes à Privilèges

Effectué par :

William Staël KAYO

Elie BOU SABA

Sous la direction de : M. Albert DIPANDA

Table des matières

INTRODUCTION :

Chaque système, service, application et périphérique d'une entreprise possède des comptes administrateurs puissants. Ces comptes "admin" ont un pouvoir énorme. Ils peuvent apporter des modifications substantielles à ces systèmes, accéder à la propriété intellectuelle ou avoir accès à des informations secrètes de l'entreprise. Il n'est pas surprenant que ces comptes soient des cibles prisées des cyber-attaquants. Le contrôle d'accès à ces comptes puissants est donc un besoin fondamental pour une entreprise. Lorsque ces comptes ne sont pas gérés, tous les systèmes informatiques et de cybersécurité dont dépend l'entreprise sont en danger.

De ce fait, pour résoudre le problème de contrôle d'accès à ces comptes puissants, nous faisons appel au PAM (Privileged Access Management) – la gestion des accès privilégiés.

Avant d'aborder la gestion des accès privilégiés en tant que discipline de sécurité, son importance et son fonctionnement, revenons aux bases. Tout d'abord, nous définirons ce que signifie l'accès privilégié, puis nous en apprendrons davantage sur la gestion sécurisée des accès privilégiés.

I. Définitions :

La gestion des accès privilégiés (PAM) [1] fait référence à un ensemble de principes de gestion de la sécurité informatique qui aident les entreprises à isoler et à gérer les accès privilégiés, à contrôler qui peut recevoir quel niveau d'accès administratif à quels terminaux, et à surveiller ce que les utilisateurs autorisés font avec cet accès.

Un accès privilégié, au sens large, est un type d'accès au système informatique qui accorde des droits spéciaux au titulaire de l'accès. Les utilisateurs ayant un accès privilégié peuvent exécuter des actions qu'un utilisateur standard ne peut pas faire. Les actions généralement qualifiées d'opérations privilégiées comprennent la capacité de modifier les paramètres du serveur, d'accéder aux systèmes de données de l'entreprise, d'installer un nouveau programme, d'exécuter des services critiques, d'ajouter des profils d'utilisateurs, de mener des activités de maintenance ou de modifier la configuration du réseau. Les équipes informatiques des entreprises d'aujourd'hui s'appuient largement sur les comptes d'utilisateurs critiques, appelés "comptes privilégiés", pour déléguer aux utilisateurs un accès privilégié aux différents systèmes d'information du réseau.

Si les comptes privilégiés restent le premier choix pour le provisionnement des accès privilégiés dans le scénario informatique actuel, d'autres options rarement utilisées incluent l'authentification biométrique et les cartes à puce. Dans certains cas, les organisations sécurisent complètement un serveur physique, une station de travail, un dispositif de centre de données ou tout système contenant des informations sensibles, et interdisent l'accès direct à la machine. Dans de telles circonstances, l'accès physique direct à la machine signifie que l'utilisateur dispose d'un accès privilégié.

Les utilisateurs privilégiés sont des utilisateurs autorisés à accéder à une partie ou à la totalité du réseau d'infrastructure informatique par la possession d'un ou de plusieurs comptes privilégiés ou par tout autre mode sont appelés "utilisateurs privilégiés". Parmi les utilisateurs privilégiés les plus connus, on trouve des travailleurs informatiques tels que des administrateurs système, des architectes et administrateurs réseau, des administrateurs de bases de données, des administrateurs d'applications métier, des ingénieurs DevOps et d'autres responsables informatiques.

II. Importance de la gestion des accès privilégiés

Les privilèges non contrôlés constituent une menace silencieuse pour les entreprises d'aujourd'hui. En effet, le rapport de 2019 de Thales sur les menaces liées aux données a classé l'accès privilégié parmi les cinq premiers facteurs de sa liste des " plus grandes menaces pour la sécurité des données ". Un rapport 2019 de Verizon [1] indique que la mauvaise utilisation des accès privilégiés est à l'origine de la plupart des incidents de sécurité et des violations de données dans tous les secteurs. Les analystes estiment même que 60 à 80 % de toutes les atteintes à la sécurité impliquent désormais la compromission des mots de passe des utilisateurs et des comptes à privilèges.

En outre, il s'agit également de l'un des vecteurs d'attaque les plus difficiles à découvrir ; certaines brèches résultant d'une mauvaise utilisation des privilèges peuvent en fait rester non découvertes pendant des mois ou plus.

Même dans les environnements informatiques les plus sophistiqués, les comptes à privilèges sont trop souvent gérés par l'utilisation de mots de passe communs à plusieurs systèmes, le partage non autorisé des informations d'identification et les mots de passe par défaut qui ne sont jamais modifiés, ce qui en fait des cibles de choix pour les attaques.

Ces pratiques peuvent facilement compromettre la sécurité, car pour la plupart des attaquants, la prise de contrôle des comptes d'utilisateurs de bas niveau n'est qu'une première étape. Leur véritable objectif est de s'emparer des comptes privilégiés afin d'augmenter leur accès aux applications, aux données et aux fonctions administratives clés. Après avoir obtenu l'accès aux informations d'identification des comptes privilégiés, les pirates peuvent facilement dissimuler leurs activités sous l'apparence d'un utilisateur administratif légitime. Un compte d'utilisateur privilégié entre de mauvaises mains est donc une arme mortelle qui peut facilement faire tomber une entreprise. Une politique PAM complète permettra de limiter cette vulnérabilité.

III. Fonctionnement de la gestion des accès privilégiés

Tout d'abord, PAM permet aux organisations de prévenir et de répondre aux menaces externes et internes. Elle réduit la surface d'attaque cybernétique en **établissant un accès avec le moins de privilèges possible pour les personnes, les processus et les applications**. Cela diminue les voies et les entrées qu'un attaquant peut utiliser pour prendre pied et limite l'étendue des dégâts en cas de violation.

[1] Importante entreprise de télécommunications américaine

Ensuite, **une centralisation de l'accès administratif** qui permet de réduire la complexité opérationnelle. Comme nous l'avons vu, accorder un large accès aux comptes privilégiés peut entraîner des failles de sécurité et des perturbations majeures. PAM adopte une approche plus globale pour améliorer le flux de travail. Sans PAM, les administrateurs peuvent suivre un protocole différent pour chaque système, souvent sur plusieurs réseaux. Avec un cadre efficace de gestion des accès privilégiés en place, les administrateurs gèrent les comptes critiques à partir d'un emplacement central. De plus, les utilisateurs accèdent aux systèmes dont ils ont besoin sans avoir à se souvenir de plusieurs mots de passe grâce à **l'intégration de l'authentification unique**. Il en résulte une meilleure productivité et une réduction des frustrations.

Enfin, **une surveillance des activités privilégiées** qui améliore la visibilité sur l'ensemble du réseau. Avec la gestion des sessions privilégiées, le super-utilisateur[2] peut facilement identifier et répondre aux problèmes en temps réel. Les administrateurs peuvent observer l'activité de chaque utilisateur privilégié du début à la fin.

La gestion des privilèges sécurise les accès distants vers le cloud car les comptes privilégiés étant de plus en plus nombreux dans certaines entreprises, elles ont besoin d'une solution plus granulaire qu'un VPN pour sécuriser l'accès aux environnements cloud.

IV. Les solutions PAM sur le marché international

Dans un article d'Expert Insight[3][2] pourtant sur le PAM, ils énumèrent les dix meilleures solutions de gestion des accès à privilèges conçues pour sécuriser les systèmes critiques d'une organisation. Pour effectuer ce classement, ils ont examiné des fonctionnalités telles que la gestion des mots de passe et l'authentification multifactorielle, la sécurité basée sur les rôles, les notifications en temps réel et les rapports robustes. On retrouve aussi dans l'article, quelques informations générales sur les différents fournisseurs et les principales caractéristiques de chaque solution qu'ils proposent, ainsi que le type de client auquel elles conviennent le mieux.

Le top des solutions de gestion des accès privilégiés (PAM) comprend donc : ARCON | BeyondTrust | Centrify | CyberArk | Foxpass | Hitachi ID Systems | JumpCloud | One Identity | Thycotic | WALLIX.

La France est représentée par WALLIX qui est un fournisseur spécialisé dans les solutions de gestion des accès et des identités pour protéger l'infrastructure informatique, les applications et les données des entreprises.

[2] Également appelé administrateur, ce compte accorde des privilèges presque illimités sur un système
[3] Site de recherche et de comparaison des solutions de cybersécurité des entreprises

CONCLUSION :

La gestion des accès privilégiés est le processus qui consiste à confier à certains utilisateurs l'accès privilégié le moins nécessaire que leur travail justifie, en partageant avec eux de manière sécurisée des comptes privilégiés spécifiques. Elle implique également une surveillance continue des utilisateurs privilégiés afin de s'assurer qu'ils n'abusent pas de leurs droits d'accès. Cela nécessite un examen régulier des privilèges attribués et la révocation des droits excessifs chaque fois que le rôle d'un utilisateur dans l'organisation change. Vue son importance, on peut donc conclure que le **PAM n'est pas un achat facultatif**.

Un système de gestion des privilèges sécurise donc efficacement un réseau et améliore la visibilité tout en réduisant la complexité opérationnelle.

BIBLIOGRAPHIE :

[1] CbyerArk. https://www.cyberark.com/fr/what-is/privileged-access-management/ . Consulté le 15 Octobre 2021

[2] Expert Insights. https://expertinsights.com/insights/the-top-10-privileged-access-management-pam-solutions/ . Consulté le 21 Octobre 2021