Petri IT Knowledgebase Resource
Une propriété de BWW Media Group

Petri
IT Knowledgebase

Top 6 des fonctionnalités que les PME devraient rechercher dans une solution de gestion d'accès privilégiés

Commandité par

Devolutions

Top 6 des fonctionnalités que les PME devraient rechercher dans une solution de gestion d’accès privilégiés

Actuellement, la plupart des solutions de gestion des accès privilégiés (de l'anglais Privileged Access Management ou PAM) sur le marché sont conçues pour les grandes entreprises. Bien qu'elles offrent de nombreuses fonctionnalités et beaucoup de flexibilité, elles ne sont pas adaptées aux PME en raison de leur complexité et de leur coût. Une solution PAM est néanmoins essentielle pour sécuriser les organisations de toutes tailles. Et les fonctionnalités populaires de niveau entreprise sont aussi pertinentes pour les PME. Donc, lorsque vous cherchez la bonne solution PAM pour votre entreprise, assurez-vous qu'elle offre les fonctionnalités essentielles pour sécuriser les comptes privilégiés.

Dans ce document technique, Devolutions examine 6 fonctionnalités que les PME devraient rechercher dans une solution PAM.

1. Facilité de déploiement et de gestion

Active Directory (AD) est la solution de gestion d'identités la plus largement utilisée aujourd'hui et tous les produits PAM s'y intègrent. Microsoft a sa propre solution PAM basée sur Windows Server 2016 et Microsoft Identity Manager (MIM). Son déploiement nécessite l'ajout d'une forêt AD à votre infrastructure existante et d'au moins un serveur exécutant MIM. C'est donc assez complexe à déployer et ça génère beaucoup de mouvements, ce qui augmente les coûts de gestion et d'administration.

Lorsque vous cherchez une solution PAM, assurez-vous qu'elle ne nécessite pas de faire des modifications à votre infrastructure Active Directory existante et qu'elle s'intègre à Azure AD (si vous utilisez Office 365). Il devrait être possible de séparer les composants sur plusieurs serveurs pour améliorer les performances dans le cas de déploiements plus importants. Un déploiement simple, piloté par un assistant, est préférable, ainsi qu'une console de gestion graphique dont l'utilisation est intuitive. Finalement, le temps c'est de l'argent. Alors, au cas où les choses tourneraient mal, assurez-vous que la sauvegarde et la restauration de la solution PAM choisie soient faciles.

2. Coffre de mots de passe sécurisé

Les mots de passe sont une solution imparfaite, mais qu'on le veuille ou non, ils restent le moyen par défaut de sécuriser l'accès aux ressources informatiques. Au fil des ans, les gens ont trouvé des moyens de rendre les mots de passe plus faciles à gérer, notamment en les écrivant sur des Post-it et en les collant sur des écrans ou en utilisant le même mot de passe sur plusieurs sites web. Aucune de ces méthodes n'est recommandée.

Garder les mots de passe dans plusieurs endroits, comme les fichiers Excel, les fichiers texte et les sessions de Bureau à distance, rend plus difficile leur intégration dans une solution PAM. Cela laisse aussi les comptes plus vulnérables, parce que ces documents ne sont pas conçus pour gérer des mots de passe.

Qu'il s'agisse d'un utilisateur final qui a besoin de stocker ses identifiants en toute sécurité ou d'une organisation qui veut sécuriser les mots de passe pour autoriser l'accès aux ressources informatiques, un coffre sécurisé donne à chacun la certitude que les mots de passe sont en lieu sûr et qu'ils peuvent être récupérés si nécessaire. Vous devriez donc chercher une solution PAM qui possède un coffre de mots de passe centralisé et sécurisé, qui peut être partagé et accessible de n'importe où.

3. Journalisation et rapports

Une bonne connaissance de votre infrastructure informatique vous permet de répondre aux problèmes et de les prévenir. Un outil PAM ne fait pas exception, et il est important de comprendre comment les comptes privilégiés sont utilisés dans votre organisation. La solution PAM que vous choisirez devrait pouvoir enregistrer quand et où les comptes privilégiés sont utilisés, par qui et comment.

Mais des journaux ne sont utiles que si vous pouvez extraire les informations dont vous avez besoin, quand vous en avez besoin. Non seulement une solution PAM doit enregistrer toutes les activités liées aux mots de passe, y compris les tentatives de connexion et l'historique, mais elle doit aussi inclure des rapports prêts à l'emploi

qui permettent de consulter rapidement les informations. Et comme avec tout système qui enregistre des tonnes de données, il est important de pouvoir filtrer le tout en utilisant des fonctionnalités de recherche avancées. La possibilité de personnaliser les rapports et d'exporter les données dans différents formats est aussi quelque chose à ne pas négliger.

4. Authentification à deux facteurs intégrée

Que vous utilisiez un gestionnaire de mots de passe, un coffre sécurisé et/ou que vous suiviez les meilleures pratiques en matière de sécurité des mots de passe, si les informations d'identification sont compromises, elles peuvent être utilisées par une personne malveillante pour obtenir un accès non autorisé. L'authentification à deux facteurs ajoute un niveau de protection qui exige des utilisateurs qu'ils aient quelque chose en leur possession en plus de connaître leur mot de passe. Par exemple, vous pouvez utiliser une application d'authentification, comme Google Authenticator, qui fournit un code que les utilisateurs doivent fournir en plus de leur mot de passe avant que l'accès ne leur soit accordé à une ressource. Cette façon de faire est la plus populaire actuellement.

Comme il existe de nombreuses façons de compromettre les mots de passe et qu'il est impossible d'assurer une protection à 100 %, l'authentification à deux facteurs est un outil essentiel pour sécuriser les comptes privilégiés. Vous devriez chercher une prise en charge de l'authentification à deux facteurs avec une variété d'options d'authentification différentes, comme Google Authenticator, SMS, courriel, RADIUS et Yubikey.

5. Injection des identifiants

Une bonne solution PAM ne se contente pas de stocker les mots de passe et d'en contrôler l'accès. Elle sert aussi d'intermédiaire entre le serveur de mots de passe et le logiciel client afin que les utilisateurs n'aient jamais besoin de connaître le mot de passe réel d'un compte privilégié. Cela signifie que la rotation des mots de passe n'est pas nécessaire : un nouveau mot de passe est généré automatiquement chaque fois qu'un identifiant est utilisé. Autrement dit, le mot de passe ne peut pas être réutilisé par l'utilisateur. Néanmoins, la rotation du mot de passe est généralement incluse même dans ce cas.

L'injection des identifiants empêche également les utilisateurs d'accéder à des ressources en dehors de ce qui est autorisé par la solution PAM, ce qui réduit potentiellement le risque d'abus. Les utilisateurs sont souvent le maillon le plus faible de la chaîne de sécurité, alors cherchez un produit PAM qui offre l'injection des identifiants.

6. Système de contrôle d'accès basé sur les rôles

Le contrôle d'accès basé sur les rôles simplifie la gestion en fournissant une série de « rôles » qui peuvent être attribués aux utilisateurs, leur donnant accès uniquement aux informations d'identification privilégiées qu'ils sont autorisés à utiliser. Ce contrôle basé sur les rôles permet aux entreprises de séparer facilement

les tâches et de mettre en place d'autres contrôles pour s'assurer que les informations d'identification ne sont pas accidentellement fournies à des utilisateurs non autorisés. Le moyen le plus simple et le plus sécuritaire de protéger les informations d'identification privilégiées (et d'éviter que des personnes non autorisées y aient accès par accident), c'est de bien définir les rôles, puis de configurer les autorisations d'accès de façon granulaire.

Comme la plupart des entreprises utilisent déjà Active Directory, vous devriez chercher une solution PAM qui dispose d'un contrôle des accès basé sur les rôles et qui s'intègre à AD pour que vous puissiez utiliser vos utilisateurs et vos groupes existants. La gestion des autorisations, des utilisateurs et des groupes peut se compliquer rapidement, même dans les petites entreprises. Un accès basé sur les rôles peut donc aider à rationaliser le processus et faciliter la gestion continue d'une solution PAM, tout en vous permettant de savoir que l'accès aux informations d'identification privilégiées est toujours correctement contrôlé.

Devolutions et la gestion des accès privilégiés

La solution PAM de Devolutions offre toutes les fonctionnalités ci-dessus et plus encore. Elle est spécifiquement conçue pour répondre aux besoins des PME. Elle vient avec des fonctionnalités de niveau entreprise pour apporter une protection habituellement réservée aux grandes organisations, tout en étant simple à déployer et à gérer. Les PME peuvent ainsi réduire les risques liés aux menaces internes et aux violations de données qui proviennent souvent d'informations d'identification compromises ou mal utilisées. De plus, la solution PAM de Devolutions permet de répondre aux exigences en matière de vérification et de conformité.

Les autres produits Devolutions s'intègrent à la solution PAM pour fournir une solution complète aux PME. Nous parlons par exemple de Remote Desktop Manager (RDM), qui aide les utilisateurs et l'équipe des TI à gérer l'accès aux connexions à distance qui nécessitent l'utilisation d'informations d'identification privilégiées.