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

Devolutions

UNE SOLUTION PAM EST ESSENTIELLE POUR ASSURER LA SÉCURITÉ DES ORGANISATIONS DE TOUTES TAILLES

La plupart des solutions de gestion des accès privilégiés (PAM) sur le marché sont conçues pour les grandes entreprises. Tout en offrant de nombreuses fonctionnalités et une grande flexibilité, elles ne conviennent pas aux PME en raison de leur complexité et de leur coût. N'empêche qu'une solution PAM est essentielle pour assurer la sécurité des organisations de toutes tailles et que les fonctionnalités des solutions PAM destinées aux grandes entreprises sont également pertinentes pour les PME. Ainsi, lorsque vous cherchez la solution PAM adaptée à votre entreprise, assurez-vous qu'elle inclut les fonctionnalités indispensables pour sécuriser les comptes et les sessions privilégiés.

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

1. Facilité d'implantation et de gestion

Active Directory (AD) est la solution de gestion d'identités la plus utilisée à ce jour et tous les produits PAM s'y intègrent. Microsoft dispose de 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 au moins un serveur exécutant MIM. Cette solution est considérablement complexe. Il devient difficile de l'implanter et elle entraîne des coûts de gestion et d'administration supplémentaires.

Lorsque vous êtes à la recherche d'une solution PAM, assurez-vous qu'elle ne nécessite aucune modification de votre infrastructure Active Directory existante et qu'elle s'intègre à Azure Active Directory si vous utilisez Office 365. Vous devriez avoir l'option de séparer les composants sur plusieurs serveurs afin d'améliorer la performance, dans le cas d'une implantation à plus grande échelle. Une implantation simple pilotée par un assistant est toujours préférable, de même qu'une console de gestion graphique intuitive. Enfin, comme le temps, c'est de l'argent, assurez-vous que la sauvegarde et la restauration de la solution PAM choisie soient simples. Au cas où les choses ne se passeraient pas comme prévu.

2. Coffre de mots de passe sécurisé

Les mots de passe sont une solution imparfaite, mais qu'on aime ou non, ils constituent toujours le moyen par défaut pour sécuriser l'accès aux ressources informatiques. Au fil des ans, les utilisateurs ont trouvé des moyens de faciliter la gestion des mots de passe, notamment en les écrivant sur des Post-It et en les collant sur les écrans d'ordinateur ou en utilisant le même mot de passe pour plusieurs sites. Aucune de ces méthodes n'est recommandée.

Le fait de conserver des mots de passe à plusieurs endroits, comme dans des feuilles de calcul Excel, des fichiers texte et des sessions de Bureau à distance, rend leur intégration plus difficile dans une solution PAM et rend les comptes plus vulnérables à l'exposition, puisque les fichiers ne sont pas conçus pour gérer les mots de passe.

Toutefois, qu'il s'agisse d'un utilisateur final qui a besoin de stocker ses informations d'identité en toute sécurité ou d'une entreprise qui souhaite sécuriser les mots de passe permettant d'accéder aux ressources informatiques, un coffre sécurisé donne à chacun l'assurance que les mots de passe sont en sécurité et qu'ils peuvent être récupérés si nécessaire. Recherchez une solution PAM dotée d'un coffre centralisé sécurisé pouvant être partagé et accessible de n'importe où.

3. Journalisation et rapports

Avoir un bon aperçu de votre infrastructure informatique vous permet de réagir aux problèmes et de les prévenir. Une solution PAM ne fait pas exception à la règle, et c'est pourquoi il est important de comprendre comment les comptes et sessions privilégiés sont utilisés dans votre organisation. Toute solution PAM devrait pouvoir enregistrer par qui, quand et où les identifiants sont utilisés.

La journalisation n'est utile que si vous pouvez extraire les informations dont vous avez besoin, quand vous en avez besoin. Une solution PAM doit non seulement enregistrer toutes les activités liées aux mots de passe, y compris les tentatives de connexion et l'historique, mais elle doit également inclure des rapports prêts à l'emploi qui vous permettent de visualiser rapidement les informations. Quel que soit le système qui enregistre beaucoup de données, il est important de pouvoir filtrer le bruit à l'aide de fonctions de recherche avancées. Vous devriez également rechercher la possibilité de personnaliser les rapports et d'exporter les données dans différents formats.

4. Authentification à 2 facteurs intégrée

Que vous utilisiez un gestionnaire de mots de passe, un coffre de mots de passe sécurisé et/ou que vous suiviez les bonnes pratiques en matière de sécurité des mots de passe, si les informations d'identification sont compromises, elles peuvent être utilisées pour obtenir un accès non autorisé. L'authentification à deux facteurs ajoute un niveau de protection supplémentaire qui oblige les utilisateurs à avoir quelque chose en leur possession, en plus de connaître leur mot de passe. L'un des moyens les plus répandus d'authentification à deux facteurs consiste à utiliser une application comme Google Authenticator qui fournit un code à saisir, en plus du mot de passe, avant que l'accès à une ressource ne soit accordé.

Comme les mots de passe peuvent être compromis de plusieurs façons et qu'il est impossible d'assurer une protection à 100 %, l'authentification à deux facteurs est un outil essentiel pour assurer la sécurité des comptes et sessions privilégiés. Vous devez donc rechercher des outils d'authentification à deux facteurs offrant diverses options d'authentification, comme Devolutions Authenticator, 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 injecte également les mots de passe 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 de mots de passe n'est pas obligatoire : il y a génération automatique d'un nouveau mot

de passe chaque fois que des identifiants sont réservés, car le mot de passe ne peut pas être réutilisé par l'utilisateur. Néanmoins, la rotation du mot de passe est généralement incluse même lorsqu'il y a injection des identifiants.

L'injection des identifiants empêche également les utilisateurs d'accéder aux ressources en dehors d'un flux de travail fourni par la solution PAM, ce qui réduit potentiellement le risque d'abus de données d'identification. Les utilisateurs sont souvent le maillon le plus faible de la chaîne de sécurité. Par conséquent, recherchez un produit PAM offrant l'injection des identifiants.

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

Le contrôle des accès basé sur les rôles (RBAC) simplifie la gestion en fournissant une série de rôles pouvant être attribués aux utilisateurs, leur donnant accès uniquement aux informations d'identité privilégiées qu'ils sont autorisés à utiliser. Un RBAC permet aux organisations de séparer facilement les tâches et d'appliquer d'autres contrôles afin de s'assurer que les informations d'identité ne soient pas fournies accidentellement à des utilisateurs non autorisés. En effet, définir les rôles, puis configurer des autorisations d'accès précises aux sessions est le moyen le plus simple et le plus sûr de protéger les informations d'identification privilégiées et d'empêcher l'exposition accidentelle aux mauvaises personnes.

Comme la plupart des entreprises utilisent déjà Active Directory (AD), recherchez une solution PAM dotée d'un RBAC qui s'intègre à AD pour mapper les utilisateurs et les groupes existants. La gestion des autorisations d'accès, des utilisateurs et des groupes peut rapidement devenir compliquée, même dans les petites entreprises. Un RBAC peut ainsi simplifier le processus et faciliter la gestion d'une solution PAM, tout en vous permettant de savoir que l'accès aux informations d'identification privilégiées est toujours contrôlé.

GESTION DES ACCÈS PRIVILÉGIÉS DE DEVOLUTIONS

La solution de gestion des accès privilégiés (PAM) de Devolutions, Devolutions Password Server, offre toutes les fonctionnalités ci-dessus et bien plus encore. Conçue spécifiquement pour répondre aux besoins des PME, elle inclut des fonctionnalités qui apportent un niveau de protection généralement réservé aux grandes entreprises, tout en restant simple à implanter et à gérer. Les PME peuvent réduire les risques liés aux menaces internes et aux atteintes à la sécurité des données qui résultent souvent d'une utilisation abusive ou du fait que des informations d'identification ont été compromises. Utilisez aussi la solution PAM de Devolutions pour répondre aux exigences de rapports et de conformité.

Les autres produits de Devolutions s'intègrent à la solution PAM pour fournir une solution complète aux PME, y compris Remote Desktop Manager, qui aide les utilisateurs et les services informatiques à gérer l'accès aux connexions à distance nécessitant l'utilisation d'identifiants privilégiés.