Ressource de Petri IT Knowledgebase
Une propriété de BWW Media Group

Petri IT Knowledgebase

Commandité par

Devolutions

Tour d'horizon sur la gestion des accès privilégiés pour les PME

TABLE DES MATIÈRES

Dans ce document technique, Devolutions explore les problèmes uniques auxquels sont confrontées les PME en matière de sécurisation des accès privilégiés.

Les professionnels de l'informatique se connectent à des systèmes distants pour effectuer des tâches de gestion et ont souvent besoin de droits d'accès de niveau administratif. Si certaines applications permettent la délégation afin que les tâches puissent être effectuées sans compte privilégié, de nombreuses opérations nécessitent des droits administratifs. La délégation augmente également les coûts de gestion, puisqu'elle oblige les entreprises à déterminer si les applications prennent en charge la délégation, à identifier les rôles du personnel, les tâches à accomplir et les droits requis pour les réaliser. Et cela devient alors un processus continu, parce que les applications, les systèmes et les rôles changent.

Il arrive donc souvent que les employés en TI se fassent donner des droits administratifs pour d'importants systèmes seulement pour accélérer l'accès. Dans le pire des cas, il peut s'agir d'un accès à un compte administratif partagé. Cela se produit souvent dans Active Directory de Windows Server, où le mot de passe de l'administrateur de domaine est largement connu. Mais si le compte est utilisé de manière abusive, tombe entre de mauvaises mains ou est compromis d'une autre façon, il peut en résulter une violation de données dont il peut être difficile de s'en remettre. Dans le cas d'Active Directory (AD), c'est particulièrement risqué, AD étant le logiciel de gestion d'identités qui contrôle l'accès aux autres systèmes de l'entreprise.

Le fait d'attribuer aux employés des comptes d'utilisateurs nommés avec des privilèges administratifs n'est pas beaucoup mieux, parce que les mots de passe sont facilement compromis. Les connexions non sécurisées à des systèmes distants ou la saisie de mots de passe sur des appareils infectés par des logiciels malveillants sont deux façons couramment utilisées par les pirates pour obtenir des mots de passe. Ces derniers utilisent des techniques automatisées pour étendre arbitrairement leurs filets virtuels à grande échelle avec un minimum d'effort. Par conséquent, même si vous ne pensez pas que votre entreprise est une cible, vous n'êtes pas nécessairement à l'abri de ce genre de problème.

Les droits administratifs augmentent les risques

La prolifération des comptes administratifs utilisés dans une entreprise signifie que les mots de passe sont souvent stockés dans des bases de données, des feuilles de calcul, des scripts et d'autres types de documents.

Et ils peuvent donc être facilement compromis. Il est important d'utiliser un gestionnaire de mots de passe ou un autre coffre sécurisé pour s'assurer que les mots de passe soient stockés en toute sécurité, qu'ils peuvent être récupérés en cas de besoin et qu'ils ne sont pas partagés entre différents comptes administratifs. Sans gestionnaire de mots de passe, les utilisateurs ont tendance à répéter le même mot de passe pour accéder à plusieurs applications, sites Web, logiciels ou autres, ce qui augmente les dommages que les pirates peuvent infliger à l'entreprise en cas d'attaque. Les utilisateurs ont aussi tendance à créer des mots de passe faibles, parce qu'il est difficile de se souvenir de mots de passe longs et complexes si on n'utilise pas de gestionnaire de mots de passe.

Windows Server offre la possibilité d'utiliser des permissions granulaires. Il permet aux organisations d'attribuer aux utilisateurs des droits pour exécuter des tâches spécifiques, sans pour autant les ajouter aux administrateurs ou à d'autres groupes privilégiés. Cependant, cela peut conduire à l'attribution de droits de « type administrateur » qui, s'ils ne sont pas soigneusement contrôlés, peuvent entraîner une violation de données. Les organisations doivent également identifier les droits nécessaires à l'exécution des tâches. Windows PowerShell et Linux peuvent être configurés pour limiter les utilisateurs à des commandes spécifiques avec des privilèges élevés, mais cela nécessite l'utilisation d'outils de gestion modernes qui ne sont pas toujours accessibles aux PME.

Gérer l'accès à distance en toute sécurité

Il y a ici plusieurs problèmes qui doivent être résolus. Lorsque le personnel TI ou des fournisseurs tiers accèdent à des systèmes distants, ils ont besoin non seulement des détails de la connexion – comme l'adresse IP, le nom DNS, le protocole et d'autres propriétés – mais aussi d'informations d'identification privilégiées pour s'authentifier sur le périphérique distant.

Authentification multifacteur et mots de passe

En utilisant uniquement un gestionnaire de mots de passe, les organisations peuvent s'assurer que des mots de passe forts sont en place pour les comptes administratifs plus sensibles. Par contre, les utilisateurs doivent encore saisir des mots de passe pour se connecter. Cela peut conduire à une exposition des mots de passe si les connexions ne sont pas sécurisées ou si les dispositifs sources sont compromis.

Et les mots de passe doivent faire l'objet d'une rotation pour s'assurer que les utilisateurs ne peuvent pas accéder aux systèmes distants après avoir effectué les modifications nécessaires.

L'authentification à deux facteurs (A2F) devrait être activée pour les comptes administratifs, question d'avoir une couche de sécurité supplémentaire. Au lieu de simplement connaître un mot de passe, les utilisateurs doivent fournir une vérification supplémentaire par le biais d'un élément qu'ils possèdent, comme une application d'authentification sur leur cellulaire. Lorsque l'authentification à deux facteurs est activée, un mot de passe compromis ne suffit pas pour se connecter.

Outils classiques de gestion d'accès à distance

Les outils de gestion offrent rarement aux organisations un moyen de surveiller les modifications apportées, ce qui peut entraîner des changements de configuration non autorisés qui ne peuvent être retracés. Les systèmes doivent être sécurisés et gérés de manière à ce que seules les modifications autorisées soient permises et qu'il existe un journal de toutes les actions effectuées. La plupart des pannes de systèmes sont le résultat de changements autorisés.

Les serveurs soumis à des politiques strictes de contrôle des changements sont plus faciles à entretenir et à supporter, parce qu'il existe une configuration connue qui peut être facilement analysée et rétablie au besoin.

Microsoft Remote Desktop (RDP) est l'outil de gestion à distance le plus courant dans les PME, parce qu'il est facile à installer et à configurer. Il permet d'accéder à un environnement de bureau et aux outils de gestion de l'ancienne interface graphique que les administrateurs système connaissent bien. Bien que RDP soit pratique, il est susceptible d'être compromis s'il n'est pas configuré correctement, en particulier lorsqu'il est exposé sur Internet.

Les attaques par force brute et par pulvérisation de mots de passe peuvent donner aux pirates un point d'entrée dans votre réseau. Les « attaques de l'homme du milieu » (mieux connues sous leur appellation en anglais *man-in-the-middle attack*), au cours desquelles les utilisateurs se connectent à un dispositif imposteur au lieu du véritable serveur, peuvent entraîner une compromission des informations d'identification et des données si le RDP n'est pas configuré correctement.

Gestion des accès privilégiés

Les solutions de gestion des accès privilégiés (PAM) permettre de résoudre les problèmes décrits ci-dessus en sécurisant les informations d'identification administratives sans diminuer la productivité des utilisateurs.

Les solutions PAM permettent aux organisations de stocker et de gérer des informations d'identification sensibles dans une base de données centralisée. Au lieu de s'appuyer sur des processus manuels ou, pire encore, sur des comptes administratifs partagés, elles fournissent un coffre sécurisé et un flux de travail pour gérer l'accès aux informations d'identification privilégiées.

Les utilisateurs demandent l'accès aux mots de passe, qui peut être approuvé ou refusé. Tout comme les systèmes de gestion des documents comme SharePoint qui permettent de vérifier l'entrée et la sortie des documents, la solution PAM vous permet de vérifier l'entrée et la sortie des mots de passe afin d'éviter qu'ils soient utilisés par plusieurs utilisateurs simultanément. Il est important de savoir qui utilise un compte, où, quand et ce qui est fait avec. La solution PAM enregistre toutes ces informations. Ainsi, en cas d'incident, c'est facile d'obtenir les preuves d'un changement de configuration en générant un rapport.

Idéalement, les modifications devraient être effectuées à l'aide d'une interface système moderne ou d'outils d'interface graphique comme le Centre d'administration Windows pour que les modifications puissent être enregistrées. En pratique, toutefois, les administrateurs effectuent généralement des tâches avec des outils qui ne consignent pas les modifications. Une bonne solution PAM vous aide résoudre ce problème grâce à une fonctionnalité d'enregistrement des sessions qui permet de capturer exactement les actions effectuées.

Devolutions Password Server

Les solutions PAM sont généralement conçues pour les grandes entreprises et la plupart des produits sont trop complexes à configurer et à gérer pour les PME. Et ça, c'est sans compter le prix prohibitif de ce genre de solutions. Par exemple, la solution PAM de Microsoft nécessite deux forêts Active Directory supplémentaires et Microsoft Identity Manager (MIM). Cela fait beaucoup de choses à gérer et de produits sous licence.

Devolutions Password Server (DPS) est conçu pour les PME. Déployable sur site, il dispose d'un coffre sécurisé de mots de passe qui peut être partagé, et des fonctionnalités intégrées de gestion des sessions privilégiées pour sécuriser les comptes et les accès administratifs. Le courtage de comptes DPS permet aux utilisateurs et à l'équipe TI de lancer des connexions à distance à des serveurs, des sites Web et des applications sans jamais avoir besoin de connaître le mot de passe du compte utilisé. La rotation des mots de passe n'est donc pas nécessaire, puisque les mots de passe ne sont jamais connus des utilisateurs. Néanmoins, DPS inclut la rotation des mots de passe pour ceux qui préfèrent émettre un mot de passe différent chaque fois qu'un accès est demandé.

DPS est géré via une interface Web contrôlée selon le principe d'accès basé sur les rôles. Les utilisateurs se connectent aux serveurs et applications distants à l'aide de Devolutions Launcher. Cet outil fonctionne avec Windows, macOS, Linux, Android et iOS. Il fournit un accès rapide et sécurisé aux services distants tandis que le courtage de comptes DPS injecte des informations d'identification sans aucune interaction avec l'utilisateur.

Installer Devolutions Password Server

Devolutions Password Server (DPS) est installé et configuré à l'aide d'une console. Il fonctionne sur toutes les versions actuellement prises en charge de Windows et Windows Server. DPS nécessite Internet Information Services (IIS) 7.0 ou plus récent et Microsoft SQL Server 2008 ou plus récent. Les PME qui ne souhaitent pas acquérir de licence SQL Server peuvent utiliser l'édition Express gratuite.

Même si DPS est conçu pour les PME, il prend en charge plusieurs topologies de déploiement différentes pour une flexibilité maximale. DPS et SQL Server peuvent être installés sur le même appareil pour les petits déploiements. Sinon, DPS peut se connecter à un cluster de basculement SQL Server mis en miroir. DPS peut également être configuré pour l'équilibrage de charges et installé dans le nuage.

Mots de passe, authentification à deux facteurs, chiffrement et intégration

Les connexions et les informations d'identification sont stockées dans un ou plusieurs coffres centralisés protégés par un cryptage AES 256 bits. Les informations d'identification peuvent être vérifiées par des opérateurs DPS autorisés, de sorte que les utilisateurs n'ont accès aux informations d'identification sensibles que lorsqu'ils en ont reçu l'autorisation.

L'extension de navigateur Devolutions Web Login permet un accès rapide aux sites Web et peut être utilisée pour générer des mots de passe forts. Les organisations qui disposent de Devolutions Remote Desktop Manager peuvent intégrer DPS avec des gestionnaires de mots de passe tiers comme 1Password et LastPass.

DPS prend en charge l'importation et la synchronisation des utilisateurs et des groupes d'Active Directory. Et si AD est synchronisé avec Azure AD, les utilisateurs d'Office 365 peuvent également être importés dans DPS. L'authentification à deux facteurs est intégrée pour un niveau de protection supplémentaire. Des rapports complets et détaillés permettent aux organisations de savoir quels utilisateurs accèdent aux comptes, ce qu'ils font, quand et où ils se connectent. Aussi, il est possible de configurer des alertes par courriel lorsqu'un compte privilégié est utilisé ou modifié.

Remote Desktop Manager

Devolutions Remote Desktop Manager (RDM) est un ensemble complet d'outils qui permet à l'équipe informatique de gérer et de partager les connexions aux systèmes distants. RDM stocke les mots de passe de manière sécurisée et effectue le courtage de comptes afin que les experts TI puissent se connecter à des périphériques distants sans exposer d'informations d'identification privilégiées. Il s'intègre à DPS et Wayk pour fournir une solution d'accès à distance complète.

RDM aide les experts TI à se connecter de manière sécuritaire et efficace aux systèmes distants. Il peut stocker les connexions et les informations d'identification pour Microsoft Remote Desktop (RDP), VNC, Hyper-V, Telnet, Citrix, VMWare, Web, VPN, SSH, FTP et de nombreux autres protocoles courants qui sont directement intégrés au produit ou disponibles via des modules complémentaires. Les informations d'identification du compte peuvent être stockées directement dans la session de l'utilisateur, dans un coffre privé de mots de passe ou dans une base de données partagée. Les fonctionnalités de RDM comprennent un accès mobile à l'aide des applications Android ou iOS, un accès hors ligne sécurisé et des consoles de ligne de commandes intégrées.

Si les comptes d'utilisateurs nommés sont généralement considérés comme une bonne pratique parce qu'ils permettent aux organisations de savoir qui accède aux systèmes, RDM peut simplifier la gestion grâce au partage du mot de passe administratif. Par exemple, au lieu de configurer des comptes nommés pour chaque utilisateur, RDM vous permet d'utiliser un compte administratif pour tous les utilisateurs.

RDM enregistre les personnes qui accèdent à un système à l'aide d'un compte administratif partagé et signale d'autres informations importantes, comme le moment et l'endroit où les connexions sont établies, qui pourraient être requises dans le cadre d'un audit.

RDM stocke les connexions dans des sources de données privées ou partagées, comme Devolutions Password Server, SQL Server, Dropbox, etc. Les connexions peuvent être partagées sur Internet, un intranet ou un nuage privé. L'édition Enterprise de RDM permet aux utilisateurs de partager en toute sécurité des connexions à partir d'un répertoire centralisé. Les organisations peuvent contrôler l'accès aux comptes privilégiés à l'aide du contrôle d'accès basé sur les rôles (RBAC).

Prochaines étapes

Devolutions Password Server est une solution PAM conçue pour répondre aux besoins des PME. Les failles de sécurité peuvent être particulièrement coûteuses pour les PME, parce qu'elles ne sont pas toujours en mesure d'absorber l'impact d'une attaque sérieuse. La gestion de l'accès aux comptes privilégiés est essentielle pour garantir l'intégrité et la sécurité du système. Pour une solution complète, DPS s'intègre avec d'autres outils de Devolutions qui aident les TI à gérer les connexions à distance.

Pour plus d'informations sur Devolutions Password Server et Remote Desktop Manager, visitez le https://devolutions.net/fr.