Une solution pour gérer les accès privilégiés

Les menaces actuelles exigent un cadre sécurisé pour la gestion des accès à distance.

DOCUMENT TECHNIQUE

TABLE DES MATIÈRES

Si vous êtes un spécialiste de l'informatique ou de la sécurité dans une petite organisation, le scénario suivant vous sera probablement familier.

Scénario : un besoin émerge d'accéder à certains serveurs et appareils virtuels distants, chacun avec un mot de passe unique. Ces appareils et les domaines qui y sont stockés sont accessibles par différents utilisateurs privilégiés. L'administrateur système connaît certains des mots de passe et certains des utilisateurs, mais pas tous. Les courriels sont envoyés, les appels téléphoniques sont passés, les feuilles de calcul Excel et même les Post-it sont analysés. Finalement, l'expert TI accède aux serveurs distants, mais il a perdu un temps fou. Et peut-être plus important encore, cette situation ne pourrait pas se produire si on applique les pratiques de sécurité de niveau militaire qu'exige l'environnement actuel où on fait face à des menaces dangereuses.

C'est le scénario typique qui se produit si souvent dans les petites et moyennes entreprises qui ne disposent pas d'une solution de gestion des accès privilégiés (de l'anglais Privileged Access Management ou PAM) efficace et conviviale. Et, comme nous le montrerons, un certain nombre de facteurs entrent en ligne de compte, ce qui rend d'autant plus important pour les PME de disposer d'une telle solution de gestion d'accès privilégiés.

Devolutions Remote Desktop Manager TechTarget Custom Media

De l'autre côté du spectre, la plupart des grandes entreprises disposent de solutions PAM depuis un bon bout de temps déjà, soit un produit local, soit une des nombreuses solutions achetées auprès des principaux fournisseurs PAM. Ces solutions PAM complètes, toutefois, demandent des moyens financiers et une expertise technique dont la plupart des PME ne bénéficient pas. Elles apportent aussi leur lot de problèmes. Elles sont souvent complexes et peu conviviales.

Les besoins en matière de solutions PAM sont parfois différents d'une organisation à l'autre, notamment selon leur taille. Ce que les entreprises partagent, toutefois, c'est ce qui les motive à se tourner vers une solution PAM et les risques de sécurité liés à l'absence d'une solution opérationnelle.

QUELS SONT LES PROBLÈMES RÉSOLUS PAR LES SOLUTIONS PAM?

Les pirates informatiques et les outils dont ils disposent sont de plus en plus sophistiqués, ce qui leur permet de pénétrer plus facilement dans les réseaux et de voler les mots de passe des comptes administrateur des domaines. Ceux-ci peuvent être les clés du royaume et la voie vers la destruction des données, le vol de données et, en général, un monde de malheur pour l'organisation attaquée.

En termes simples, l'objectif des solutions PAM est de faire la vie dure aux pirates informatiques en leur bloquant l'accès aux comptes des utilisateurs privilégiés. Les solutions PAM renforcent davantage la surveillance en améliorant la visibilité globale du réseau pour les administrateurs système. Elles offrent aussi des contrôles plus précis. Ces solutions permettent de savoir en temps réel qui sont les utilisateurs privilégiés et ce qu'ils font dans l'ensemble du parc informatique à distance.

Les meilleures solutions PAM automatisent également le processus de génération des mots de passe aléatoires, puis leur gestion dans un coffre hautement sécurisé. Il est aussi possible de stocker d'autres informations d'identification pour divers comptes et d'applications.

UNE NÉCESSITÉ ET NON UN LUXE

De ce point de vue, les solutions PAM sont un élément essentiel des environnements sécurisés d'utilisateurs et de serveurs distants. Elles permettent aux organisations, y compris aux PME, de surveiller et de gérer efficacement les comptes et les accès privilégiés, ce qui non seulement renforce la protection des actifs critiques, mais aide également les entreprises à répondre aux exigences de conformité.

L'intérêt croissant pour les solutions PAM, en particulier parmi les PME qui les jugeaient auparavant inutiles ou trop coûteuses, est dû à ces facteurs :

- L'augmentation marquée de la sophistication, de la fréquence et du pouvoir destructeur des cyberattaques sur les organisations de toutes tailles, y compris les PME ciblées par le harponnage et les attaques de rançongiciels.
- La conviction des pirates que de nombreuses PME n'ont pas protégé de manière adéquate l'accès privilégié aux comptes et aux serveurs à distance.
- Le renforcement des réglementations et des règles de conformité qui imposent de meilleures pistes d'audit et la preuve que des efforts ont été déployés en matière de sécurité des données.
- Le nombre croissant de tiers, comme les sous-traitants et les fournisseurs de services d'infonuagiques, qui se voient accorder des accès privilégiés.

GÉRER LES MOTS DE PASSE, C'EST ESSENTIEL

Par définition, l'accès à distance implique l'utilisation et le partage de mots de passe. C'est dans ce domaine que de nombreuses PME sont loin de prendre des mesures pourtant simples pour combler les lacunes en matière de sécurité.

Une étude importante a révélé que 63 % des failles de sécurité confirmées concernaient des mots de passe faibles, par défaut ou volés1. Une autre étude récente a déterminé que 20 % des utilisateurs professionnels utilisent des mots de passe très faibles ou partagent régulièrement des mots de passe, ce qui les rend relativement faciles à pirater2. L'étude a également révélé que les PME ayant un pourcentage de mots de passe compromis supérieur à la moyenne avaient également un pourcentage de mots de passe partagés supérieur à la moyenne.

La solution? Un système complet de gestion des mots de passe. Les meilleurs outils génèrent des mots de passe complexes et aléatoires et disposent d'un coffre sécurisé qui stocke tous les mots de passe et informations d'identification. Les utilisateurs n'ont pas besoin de se souvenir de ces mots de passe. Et les administrateurs système qui utilisent des mots de passe partagés pour l'accès à distance ne voient jamais les mots de passe réels, parce qu'ils passent par la solution de gestion des mots de passe.

Ainsi, ces systèmes de gestion des mots de passe accomplissent la double tâche de synchroniser les différents mots de passe nécessaires à l'accès à distance sans entraver la productivité globale, le tout de manière hautement sécurisée. En fin de compte, les PME qui adoptent pour la première fois des gestionnaires de mots de passe constatent souvent que les appels au service d'assistance informatique sont réduits presque immédiatement, parce que les utilisateurs n'appellent plus pour dire qu'ils ont oublié leurs mots de passe.

1 "2016 Data Breach Investigations Report" *Verizon*, 2016

2 "35% of LinkedIn Users' Passwords Are Weak Enough to Hack" *TechRepublic*, le 13 mars 2017

PAM AU SECOURS DES ENTREPRISES

Les grandes entreprises utilisent les solutions PAM depuis plusieurs années déjà. En général, ces solutions sont complexes, coûteuses et souvent peu conviviales. Cependant, plusieurs fabricants s'associent désormais à des fournisseurs de solution PAM qui ciblent les PME pour offrir des solutions plus conviviales.

Lorsqu'elles envisagent de telles intégrations, les entreprises doivent d'abord vérifier que ces solutions prennent en charge une large liste de technologies, notamment les réseaux privés virtuels (RPV), les gestionnaires d'informations d'identification, les protocoles Secure Shell (SSH), l'informatique en réseau virtuel, le protocole Bureau à distance et tous les gestionnaires de mots de passe personnels.

MIEUX GÉRER, EN TOUTE SÉCURITÉ

L'équipe informatique de Siemens Building Technologies (SBT) à West Sacramento, en Californie, était constamment confrontée à des problèmes liés à la gestion des connexions à distance pour les 30 serveurs pris en charge par l'équipe. Elle n'avait aucun moyen d'organiser et de gérer en toute sécurité les connexions partagées aux sites des clients, et le partage des informations d'identification avec les serveurs des clients était mal fait, difficile et donc coûteux.

Fatigué d'avoir à gérer les défaillances de leur gestionnaire de connexion à distance, le programmeur principal sur place a téléchargé un **essai gratuit** d'une autre solution PAM, ce qui a rapidement conduit à l'achat d'une licence pour cette autre solution.

Aujourd'hui, l'équipe informatique de SBT peut gérer en toute sécurité les connexions et les informations d'identification d'une manière facile à protéger, à mettre à jour et à partager.[3] Les membres de l'équipe n'envoient plus de connexions par courriels ou SMS et ne stockent plus les informations dans un emplacement du réseau.

SE SORTIR DU CHAOS

Pendant ce temps, en Slovénie, des ingénieurs et l'équipe informatique d'EM-Soft Sistemi stockaient localement des informations d'identification sur un ordinateur désigné. Cela signifiait qu'il fallait placer toutes les informations d'identification ailleurs au cas où l'ordinateur tomberait en panne ou devrait être remplacé. Ils ne pouvaient pas non plus accéder aux informations d'identification en dehors de leur bureau. Ils utilisaient un mélange confus d'outils pour différents appareils et types de connexion.

Après avoir essayé différents outils PAM (essais qui n'ont pas été un succès), l'équipe a opté pour une solution de gestion des connexions à distance qui stocke en toute sécurité les informations d'identification des différents utilisateurs dans un coffre centralisé[4]. Le service informatique contrôle désormais tous les pare-feux et les services à partir d'une console unique. Ils utilisent désormais une seule application conviviale pour tous les types de connexions.

DES BÉNÉFICES COMMUNS

Ce que ces différentes entreprises et **beaucoup d'autres** ont en commun, ce sont les excellents résultats obtenus grâce aux solutions PAM de Devolutions, dont le produit phare, **Remote Desktop Manager**, est aujourd'hui utilisé par plus de 300 000 utilisateurs dans 130 pays. Les solutions Devolutions se démarquent grâce à un coffre hautement sécurisé pour le stockage des mots de passe et des identifiants.

En plus, les outils PAM de Devolutions sont conçus pour fonctionner avec le plus grand nombre de RPV, de tunnels SSH et de gestionnaires de mots de passe personnels. Véritable couteau suisse pour les professionnels de la sécurité et de l'informatique dans les PME comme dans les grandes entreprises, les solutions PAM de Devolutions permettent de résoudre les principaux problèmes liés à la sécurité des accès privilégiés.

Pour savoir comment les solutions de gestion des connexions à distance peuvent aider les administrateurs système à faire leur travail plus efficacement, lisez le Top cinq des fonctionnalités à rechercher dans une solution de gestion des connexions à distance.

3 "Siemens Uses Remote Desktop Manager to Synk Up Its New Connections Automatically In a Shared Database" *The Devolutions Blog*, le 10 janvier 2017.

4 "EM-Soft Sistemi Chose Remote Desktop Manager as Their Centralized Repository Solution to Store Their Credentials" *The Devolutions Blog*, le 26 octobre 2016.