Sécurité des mots de passe : le partage confidentiel ou SAPM

Certaines DSI tentent de faire disparaître les mots de passe de leurs utilisateurs au profit de formes d'authentification plus sûres ou plus modernes (biométrie, badge RFID etc.). Néanmoins, elles restent confrontées à la gestion d'un large parc de comptes partagés qui ne sauraient fonctionner autrement qu'avec ces illustres sésames. Ironie de ces comptes des Mille et Une Nuits, ce sont bien souvent eux qui ouvrent les portes de la production, dans le cœur sensible du Système d'Information. L'arrivée du Shared Account Password Management va-t-elle simplifier les choses ?

De Jules César à Bruce Schneier

L'histoire du mot de passe est presque aussi ancienne que celle de l'art militaire. Il y a plus de deux mille ans, les légions romaines en faisaient déjà un usage intensif et disposaient même d'une fonction dédiée à sa gestion. Dans chaque camp Romain, un *tessarius* (sorte de sergent de l'époque) était ainsi chargé de distribuer aux patrouilles et aux gardes, le code qui permettrait à ces derniers de contrôler l'identité des légionnaires rentrant dans le camp.

Plus proche de nous, il s'agit du premier et du plus illustre des paradigmes de sécurité informatique. De son compte mail personnel à son poste de travail professionnel, tout un chacun connaît et utilise aujourd'hui au moins un secret contrôlant l'accès à un service informatique. Bien entendu, à l'heure du passeport biométrique, le mot de passe revêt une certaine allure de grand-père. Toutefois, force est de constater qu'il reste encore aujourd'hui pour le grand public la forme d'authentification la plus répandue.

En entreprise, l'utilisateur informatique est également loin d'en avoir fini avec lui. Rares sont en effet les entreprises à fournir à l'ensemble de leurs salariés un mode d'authentification sans mot de passe. Au point souvent d'en écœurer certains utilisateurs, submergés par le nombre de codes confidentiels à retenir, et qui ne trouvent d'autres remèdes qu'un appel régulier au helpdesk ou l'espérance d'une solution de Single Sign-On.

Par ailleurs, même les entreprises les plus en avance en matière de SSO, d'authentification forte ou de biométrie, ne sont pas totalement débarrassées de toute problématique liée aux mots de passe. En effet, dans le Système d'Information, un village d'irréductibles résiste encore et toujours - et probablement pour très longtemps encore - aux vagues de renforcement du contrôle d'accès.

Ce village, c'est celui des comptes techniques partagés : logins *root* des serveurs Unix, administrateurs locaux des machines Windows, *sysadmin* des bases de données Oracle, comptes *admin* des routeurs Cisco etc. Contrairement à ceux des utilisateurs usuels - qui par essence sont nominatifs -, ces comptes ont la particularité de ne pouvoir être liés à aucune personne physique spécifique. Plusieurs administrateurs (mais parfois aussi quelques stagiaires !) en partagent ainsi la connaissance. Alors, comment protéger les mots de passe reliés à ces comptes ?

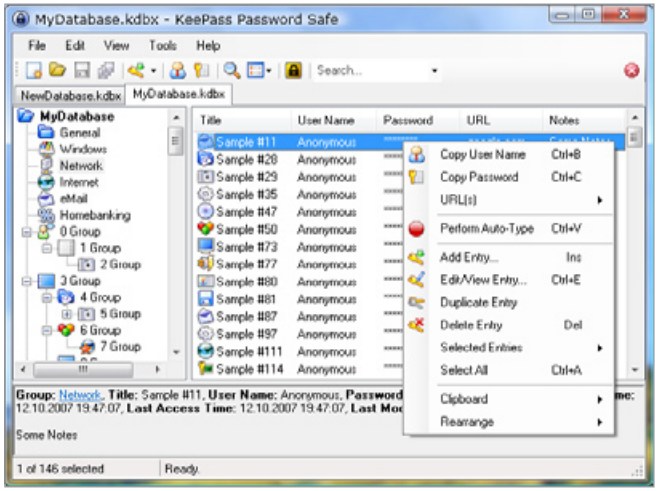

Figure 1 : KeePass, un coffre de mots de passe Open Source

D'aucuns prétendent que les informaticiens adorent la récursivité. En la matière, et au regard des premières initiatives mises en œuvre pour répondre à cette problématique, on serait effectivement tenté de leur donner raison. En effet, quoi de plus naturel pour protéger des mots de passe... que d'utiliser un mot de passe ? C'est l'option jusqu'ici retenue par beaucoup, au travers de logiciels libres tels que KeePass ou Password Safe de Bruce Schneier, star de la sécurité informatique outre-Atlantique. Ces logiciels permettent de créer des coffres, chiffrés par des algorithmes de cryptographie tels qu'AES ou Twofish, et renfermant les mots de passe à protéger. Pourquoi parler de récursivité ? Et bien parce que l'ouverture du coffre s'effectue par la fourniture d'un mot de passe, non nominatif et global au coffre.

Les limites des coffres partagés

Si l'option des coffres à la Keepass ou Password Safe s'avère séduisante pour une utilisation domestique, elle atteint rapidement ses limites dans un véritable environnement de production. Difficile en effet d'imaginer 10 administrateurs Unix, 15 administrateurs Oracle et 12 exploitants Réseau (soit 37 personnes) partager un unique mot de passe leur permettant d'accéder à l'ensemble des ressources serveurs du Système d'Information.

La réponse la plus naturelle à cette problématique de partage revient à scinder ce coffre unique en autant de coffres qu'il y a d'équipes d'administrateurs et d'exploitants, soit dans l'exemple précédent un coffre pour l'équipe Unix, un autre pour l'équipe Oracle et enfin un dernier pour l'équipe Réseau. Le problème de

cette réponse est que les architectures informatiques modernes sont loin de ressembler aux blocs monolithiques des années 1980. De nos jours une application n'est généralement plus portée par un serveur unique, mais bien par un ensemble de briques interconnectées. Ainsi, un administrateur Unix configurant un serveur Tomcat dans cet environnement devra vraisemblablement renseigner un login/mot de passe Oracle pour paramétrer la connexion de son serveur d'applications à la base de données applicative. De même, l'équipe Réseau pourra vouloir installer une sonde sur un serveur Unix, nécessitant ainsi la connaissance d'un compte technique pour cet environnement, etc.

Bref, la stratégie du « diviser pour régner », chère à l'antique Sénat romain, atteint parfois ses limites dans le XXI^{ème} siècle informatique.

L'avènement des solutions centralisées

Cette problématique de gestion et de partage des comptes techniques, dite *SAPM* pour *Shared Account Password Management*, n'est évidemment pas nouvelle, mais elle devient de plus en plus visible (et sensible !) à mesure que les Systèmes d'Information gagnent en complexité. Face à cette nécessaire rationalisation, de nouvelles solutions éditeurs ont vu le jour. Elles partagent un certain nombre de caractéristiques, dont celle de s'attaquer à la multiplication des coffres par une approche centralisée :

- L'architecture classique d'une solution de SAPM « moderne » est en effet celle d'une application Web, proposant après une phase d'authentification nominative (par login / mot de passe personnel, certificat, One Time Password etc.), l'accès à des comptes partagés et stockés dans une unique base de données. À l'instar des coffres à la KeePass ou Password Safe, cette base est chiffrée, même si du fait de la centralisation il devient beaucoup plus complexe de récupérer le container des mots de passe.

- Le coffre centralisé est également accessible par API. Dans un tel mode, l'appelant présente un certificat préalablement émis par le serveur centralisé afin de valider son identité auprès de lui. Il devient alors possible d'éliminer tout mot de passe en clair dans des scripts de démarrage ou de sauvegarde. Grâce à son certificat personnel, le script appelant récupère ainsi dans la base le mot de passe dont il a besoin et uniquement lorsqu'il en a besoin.

- Au-delà de l'authentification nominative, les logiciels de SAPM proposent un contrôle d'accès basé sur des règles individuelles ou suivant les préceptes du modèle RBAC (Role Based Access Control), bien connu des consultants en gestion des identités et des accès. Une équipe d'administrateurs Oracle peut alors partager en lecture seule ou bien en lecture / écriture tout ou partie de ses mots de passe avec une équipe d'administrateurs Unix. Certaines solutions intègrent également un moteur de workflow de demandes d'accès temporaires ou de mots de passe à usage unique.

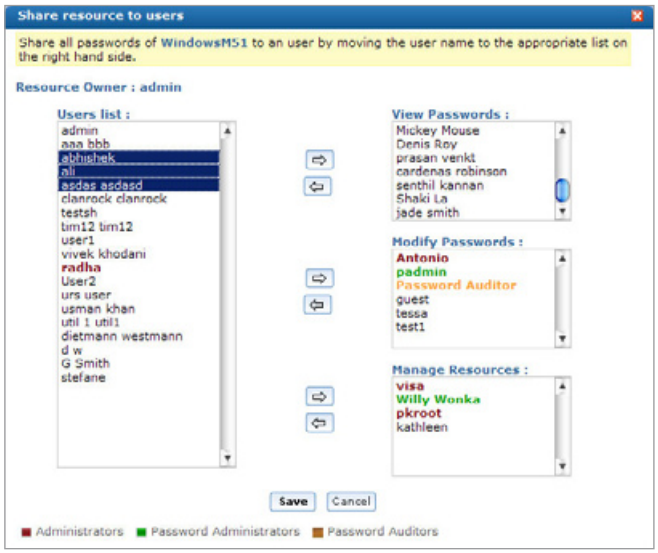

Figure 2 : Partage des mots de passe dans Manageengine Password Manager Pro

- Les comptes techniques peuvent être classés et catégorisés et sujets à des contraintes spécifiques, notamment en termes de force des mots de passe, par exemple : 8 caractères minimum dont 2 spéciaux pour les comptes de préproduction, 6 caractères libres pour les comptes de développement, changement obligatoire tous les 3 mois pour les comptes de production, etc.

- Les solutions de SAPM se veulent aussi être des points d'entrée pour l'administration des comptes techniques sur les serveurs. Aussi, lorsqu'elles sont dotées des connecteurs adéquats, elles permettent à un administrateur de réinitialiser un mot de passe à distance, c'est à dire directement dans l'interface SAPM, sans avoir à réaliser cette opération sur le système cible. Ces opérations peuvent également être automatisées et corrélées aux politiques de mots de passe. Une telle solution peut par exemple être paramétrée pour modifier automatiquement et régulièrement les mots de passe des comptes administrateurs locaux des postes de travail Windows de l'entreprise.

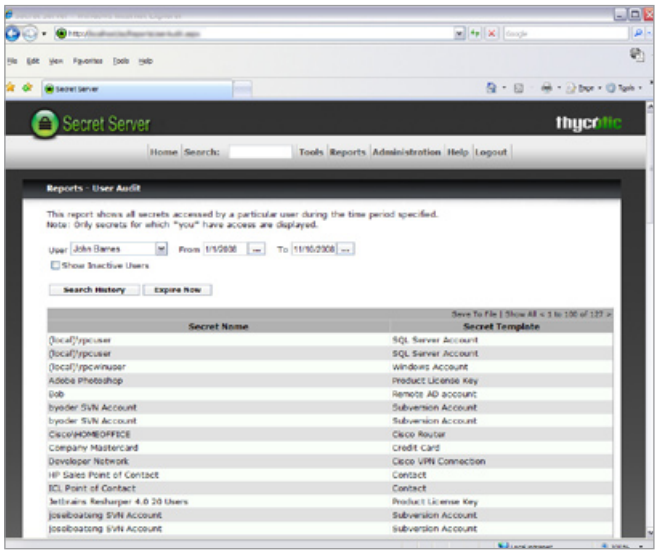

Figure 3 : Piste d'audit dans Thycotic Secret Server

- En termes de traçabilité tout accès sur un mot de passe du coffre est immédiatement inscrit dans une piste d'audit. Il devient alors possible, dans un cadre de sécurité a posteriori, de connaître les derniers mots de passe récupérés ou modifiés par un individu donné, ou bien les dernières personnes ayant consulté un certain mot de passe.

- Enfin, ces solutions sont le plus souvent dotées de fonctionnalités de reporting, permettant à des auditeurs, responsables de la sécurité ou de la production d'obtenir un véritable tableau de bord pour la gouvernance de ces accès privilégiés : nombre de comptes techniques Oracle, Unix, Windows, etc. dans le SI, comptes techniques de production ne respectant pas la politique de sécurité, synthèse des accès possibles pour tel ou tel administrateur réseau, etc.

Encore un marché de niche

Deux grands types de solutions sont disponibles sur le marché du SAPM : les produits logiciels et les boîtiers matériels. On peut ainsi citer *Manageengine Password Manager Pro (AdventNet)* ou *Secret Server (Thycotic)* pour ce qui relève du pur logiciel ou encore *PowerKeeper (Symark)* pour le matériel. À noter que certaines solutions telles *Entreprise Password Vault (Cyber-Ark)* ou *CS Password Manager (Cloakware)* sont elles, disponibles dans les deux formats. Dans tous les cas, la plage de prix est relativement large, allant de quelques centaines à plusieurs milliers d'euros en fonction du produit choisi, de ses options ou connecteurs, du nombre d'entrées ou d'utilisateurs.

Quoi qu'il en soit, il est remarquable de constater que les très gros éditeurs n'ont pas encore investi la place. Le marché du SAPM prenant une forte ampleur (le Gartner Group prédit que 50 % des grandes entreprises seront équipés d'une telle solution d'ici à la fin 2010), il y a néanmoins fort à parier qu'il sera bientôt le théâtre d'acquisitions et d'intégrations au sein des suites d'IAM (Identity & Access Management) de quelques géants de l'informatique.

Réussir son déploiement

À l'instar de nombreuses autres thématiques, la réussite d'un projet de SAPM ne saurait toutefois être réduite à l'achat d'un produit. Le déploiement d'une telle solution doit avant tout être précédé d'une cartographie des composants existants et des comptes techniques partagés. Une fois ce travail effectué, il convient d'identifier qui est maître de la donnée (ex : qui gère ce serveur Unix, qui change le mot de passe *root* et selon quelle fréquence ?), qui en est l'utilisateur (ex : l'équipe Oracle peut être amenée à utiliser ce compte lors de ses installations), et quelles sont les contraintes qui pèsent sur elle (ex : la demande d'accès au compte d'administration doit être validée par le responsable de l'équipe Support). En sa qualité de manager et d'orchestrateur de la sécurité, le RSSI (responsable de la Sécurité du SI) se trouve souvent être sur cette thématique tout à la fois commanditaire, premier sponsor, mais également premier acteur au sein d'un projet qui n'est finalement rien d'autre qu'une démarche de gouvernance sur des données ultra-sensibles : les mots de passe partagés. ■

Bruno Vincent,
cofondateur

ITekia est un cabinet de conseil indépendant, spécialiste de l'Architecture, du Pilotage et de la Sécurité des Systèmes d'Information. ITekia conseille et accompagne les grands comptes et les PME, dans leurs projets de rationalisation, d'innovation et de refonte de leurs Systèmes d'Information.