Les PME sont en voie de devenir le *ground zero* pour la cybercriminalité

Des solutions complètes de gestion de mots de passe offrent une protection contre les plus grandes menaces.

DOCUMENT TECHNIQUE

TABLE DES MATIÈRES

De nombreuses petites et moyennes entreprises (PME) sont convaincues que les grandes entreprises sont plus à risque en matière de cybersécurité. C'est pourtant de plus en plus évident que les PME sont plus vulnérables que les grandes sociétés. L'insouciance avec laquelle certaines PME abordent la cybersécurité peut avoir des conséquences désastreuses.

Heureusement, il existe de nombreux systèmes de défense contre cette marée montante de cybermenaces, notamment des solutions complètes de gestion des mots de passe. À elles seules, ces solutions peuvent bloquer de nombreuses attaques. En fait, les solutions de gestion de mots de passe sont une solution évidente pour les PME compte tenu des menaces présentes, de leur coût relativement faible et de l'énorme protection contre les attaques qu'elles offrent.

Dans quelle mesure l'utilisation de mots de passe forts est-elle efficace pour contrer les attaques? Le rapport annuel d'enquêtes sur les violations de données de Verizon a révélé une statistique surprenante: près des deux tiers (63 %) des violations de données impliquaient l'exploitation de mots de passe faibles, de mots de passe configurés par défaut ou volés[1]. La plupart – voire la totalité – de ces attaques auraient pu être bloquées par des mots de passe générés par une machine, une fonctionnalité disponible dans toutes les solutions complètes de gestion des mots de passe.

1 Rapport d'enquête sur les violations de données de Verizon, Verizon, 2016

Devolutions Remote Desktop Manager

TechTarget | Custom Media

POURQUOI LES PME SONT DES CIBLES AUSSI IMPORTANTES?

Les PME sont rapidement devenues la cible de prédilection pour les pirates informatiques. C'est un fait qui est de plus en plus connu. Un rapport soutient que non seulement les PME doivent faire beaucoup plus en matière de cybersécurité, mais elles doivent aussi prêter attention « (aux) pratiques relatives aux mots de passe de leurs employés ». Le rapport ajoute que « malgré des preuves claires que l'écrasante majorité des cyberattaques des PME résulte d'une mauvaise gestion des mots de passe, les entreprises font très peu pour améliorer les pratiques de gestion de mots de passe de leurs employés.[2] »

La menace croissante pour les PME est encore plus claire lorsqu'on consulte les résultats de l'État de la cybersécurité dans les petites et moyennes entreprises en 2017 effectué par le Ponemon Institute. Ce rapport renforce d'ailleurs les conclusions similaires de celui de l'année précédente (2016)[3]. Voici les principales constatations du rapport, qui constituent selon nous une bonne raison de lever un drapeau rouge:

- 61 % des PME interrogées ont été victimes d'une cyberattaque, contre 55 % un an plus tôt.
- 54 % ont signalé une violation de données causée par la négligence des employés (c'est-à-dire une mauvaise gestion des mots de passe). Il s'agit d'ailleurs de la principale cause de violation de données selon le rapport.
- 52 % ont signalé une attaque par rançongiciel. Les mots de passe volés ou compromis sont l'un des principaux catalyseurs de ces attaques.
- Le coût total d'une attaque réussie dépasse maintenant 1 M$, des dommages qui peuvent ruiner de nombreuses PME.

LA VISIBILITÉ DES MOTS DE PASSE EST ESSENTIELLE

Un nombre surprenant de responsables informatiques et de responsables non informatiques dans les PME ont peu ou pas de visibilité sur les pratiques d'utilisation des mots de passe de leurs propres employés. Selon un rapport, « mot de passe » figure parmi les 10 principaux mots de passe utilisés l'année dernière. D'autres utilisateurs choisissent des mots de passe simples comme 123456. Une étude qui porte sur près de 13 millions de mots de passe utilisés dans des violations de données a montré que les cinq principaux mots de passe utilisés étaient 123456, 123456789, 12345, 12345678, et qwerty – les lettres consécutives sur la rangée supérieure d'un clavier conventionnel.

D'autres personnes partagent leurs mots de passe avec des collègues et même des tiers sans s'inquiéter. De nombreux utilisateurs écrivent aussi leurs mots de passe sur des morceaux de papier qui trainent sur leur bureau. Les dates d'anniversaire sont également des mots de passe très populaires.

Et trop nombreux sont ceux qui utilisent les mêmes mots de passe ou des dérivés pour accéder à plusieurs systèmes, sites et bases de données. Ils ouvrent ainsi la porte toute grande aux attaques.

Les pirates informatiques sont au fait de ces pratiques communes, ce qui explique pourquoi les PME sont en voie de devenir leur cible de prédilection. Les PME représentent la facilité vers la malfaisance, une proie facile à la portée des prédateurs.

LA MENACE IMMINENTE DE L'INTERNET DES OBJETS

Une autre menace croissante pour la cybersécurité des PME est moins visible, mais pas moins dangereuse. La plupart des chefs d'entreprise pensent que l'Internet des objets (IdO) – ces gadgets connectés à Internet qui dépasseront cette année les 6,4 milliards d'utilisation – est surtout utilisé dans les objets de consommation. Ils sont néanmoins très présents dans les PME (thermostats programmables, téléviseurs intelligents, aspirateurs robotiques et caméras de sécurité en continu, etc.). Ils ont tous une chose en commun : ils arrivent de l'usine avec des mots de passe prédéfinis, très faciles à pirater et très peu de gens prennent la peine de les réinitialiser.

Le piratage de ces appareils peut faire des ravages pour les PME. Par exemple, l'année dernière, des pirates ont pris le contrôle de 100 000 appareils connectés mal sécurisés et ont lancé une attaque de botnet qui a interrompu le service Internet pour des millions de clients[4]. Encore une fois, la mise en place de bonnes pratiques en matière de mots de passe aurait pu éviter ce type d'attaque.

LA VALEUR INESTIMABLE D'UNE SOLUTION DE GESTION DE MOTS DE PASSE

Optez pour une solution complète de gestion de mots de passe qui offre un rempart très solide contre les attaques les plus courantes et les faiblesses de mots de passe généralement exploitées – même si ce n'est pas une recette miracle pour toutes les cybermenaces.

Ces systèmes donnent aux administrateurs TI une visibilité très large sur les pratiques d'utilisation des mots de passe de tous les employés, ainsi que de tous les appareils mobiles qu'ils utilisent. Il faut noter que les administrateurs n'ont jamais connaissance des mots de passe réellement utilisés. Ils peuvent déterminer, cependant, si les utilisateurs respectent les bonnes pratiques : l'utilisation de mots de passe complexes, ne pas utiliser le même mot de passe à plusieurs endroits, etc.

2 Why small and mid-sized businesses are a huge target for cyber attacks CSO from IDG, octobre 2017

3 2016 State of Cyber Security in Small & Medium Size Businesses, *Ponemon Institute*, juin 2016

4 DDoS attack on Dyn came from 100,000 infected devices, *Computerworld*, octobre 2016

Les mots de passe générés par le système sont très complexes. Ils sont composés de lettres, de caractères et de chiffres. Cela les rend difficiles, voire impossibles, à identifier. Ils sont également difficiles à retenir pour les utilisateurs. Ce n'est pas un problème, parce que chaque utilisateur doit se souvenir d'un seul mot de passe qui permet ensuite au système d'appliquer ses mots de passe uniques de manière hautement sécurisée.

Personne chez le fournisseur de solutions de gestion des mots de passe ne peut accéder à ces mots de passe stockés et générés par la machine. Les mots de passe et les autres informations stockés par un client, comme les informations d'identification et autres fichiers sensibles, sont conservés dans un coffre de données hautement sécurisé. Avec ce qu'on appelle les « coffres à connaissance nulle », personne chez le fournisseur ne peut accéder à des mots de passe ni déchiffrer les données dans les coffres.

QUELS ÉLÉMENTS RECHERCHER DANS UNE SOLUTION DE GESTION DE MOTS DE PASSE?

Lorsque vous cherchez la meilleure solution de gestion de mots de passe, assurez-vous qu'elle permet la création, le partage et la gestion sécurisée de dossiers et de fichiers chiffrés entre plusieurs équipes à l'interne, et éventuellement avec des tiers. Une solution avec des politiques et des autorisations configurables peut aussi faciliter l'harmonisation avec vos politiques de sécurité internes.

Un autre avantage est la possibilité de lier la solution de gestion des mots de passe aux politiques et procédures qui affectent les comptes privilégiés et les informations d'identification de compte.

Assurez-vous également que la solution offre une gestion hautement sécurisée et chiffrée des mots de passe et une interface vraiment conviviale, disponible pour une grande variété de systèmes d'exploitation et d'appareils. Aussi, cela facilite les efforts de conformité si la solution dispose de capacités d'audit étendues.

DIRIGEANTS DE PME : NE NÉGLIGEZ PAS LA GESTION DE MOTS DE PASSE

La direction d'une entreprise de plusieurs milliards de dollars peut se permettre de laisser la gestion des mots de passe à d'autres personnes, souvent au chef de l'informatique. Mais les dirigeants d'une PME typique peuvent difficilement se permettre ce luxe. En fait, le mantra des dirigeants d'une PME devrait être « la gestion des mots de passe est bien plus qu'un problème informatique ».

Dans son sondage annuel sur la criminalité économique mondiale, PwC soutient que, trop souvent, les responsables non informatiques rejettent la responsabilité de la cybersécurité en général – dont la gestion des mots de passe est un élément clé de l'informatique. PwC dénonce les entreprises qui agissent de la sorte et ajoute que pratiquement tous les aspects de la cybersécurité, y compris la gestion des mots de passe, « doivent faire partie intégrante de la culture d'entreprise ». Le rapport indique aussi que les responsables non informatiques doivent « intégrer la cybersécurité dans leurs évaluations des risques, puis communiquer le plan de haut en bas et à toute l'organisation. » [5]

En d'autres mots, l'importance de la gestion des mots de passe et de l'application des bonnes pratiques en la matière commence par le haut. Sinon, elle ne sera pas bien comprise au sein de l'organisation.

5 Global Economic Crime Survey, *PwC*, 2016

LE LEADER DE L'INDUSTRIE DANS LES SOLUTIONS DE GESTION DE MOTS DE PASSE

Devolutions est un fournisseur de premier plan et leader reconnu dans la gestion des connexions à distance, des mots de passe et des informations d'identification pour les administrateurs système et les professionnels de l'informatique. Nous proposons un système complet de gestion des mots de passe qui réduit l'accès non autorisé aux actifs numériques tout en contrecarrant les attaques de l'intérieur.

Devolutions prend grand soin d'aider les clients à trouver l'équilibre entre la véritable sécurité et l'accessibilité des utilisateurs aux données critiques de l'entreprise. Nous accomplissons tout ça en sécurisant les mots de passe privilégiés pour les utilisateurs et les administrateurs dans un coffre chiffré et renforcé tout en maintenant une expérience utilisateur intuitive.

Téléchargez une version d'essai gratuite de cette solution essentielle pour les PME ici.