LA SÉCURITÉ DES MOTS DE PASSE DANS LES ENTREPRISES : LES STRATÉGIES DOIVENT CHANGER

SPECOPS SOFTWARE

De nombreuses entreprises utilisent des mots de passe qui suivent désormais des règles dépassées. Une nouvelle stratégie en matière de mots de passe et des filtres de mots de passe sophistiqués peuvent contribuer à la protection contre les incidents de sécurité, avec les pertes, les dommages d'image et, surtout, les sanctions qui en découlent.

À PROPOS DE SPECOPS Specops Software est le leader en de solutions de gestion des mots de passe et d'authentification. Specops protège vos données professionnelles en bloquant les mots de passe faibles et en sécurisant l'authentification des utilisateurs. Chaque jour, des milliers d'organisations utilisent Specops Software pour protéger leurs données professionnelles. Pour plus d'informations, veuillez consulter le site specopssoft.com/fr.

Une protection par mot de passe bien pensée et des mots de passe forts ne sont plus une « bonne chose à avoir », mais une obligation. Après tout, selon l'article 32 du RGPD, une protection adéquate par mot de passe est l'une des mesures organisationnelles qui doivent être mises en œuvre pour protéger les données personnelles. La compagnie aérienne British Airways, par exemple, a dû payer une amende de 183 millions d'euros à la suite d'un vol de données causé par une violation de mot de passe évitable. Les domaines informatiques qui ouvrent l'accès à de nombreux profils d'utilisateurs en cas d'incident de sécurité nécessitent une protection particulière. Dans les environnements Microsoft largement utilisés dans les entreprises, cela concerne l'Active Directory.

Le risque d'être attaqué afin de capturer des mots de passe ou des hachages de mots de passe, puis de les décrypter hors ligne, est élevé. Selon l'étude de la firme de cybersécurité Proofpoint, 91 % des entreprises françaises ont été attaquées numériquement en 2019, et 65% l'ont été à de multiples reprises. Au niveau mondial, 37 % des entreprises interrogées par l'expert en cybersécurité Sophos ont déclaré avoir subi une attaque numérique en 2021. Il ne s'agit plus de savoir si une entreprise va être attaquée mais quand.

Malheureusement, les utilisateurs rendent généralement la tâche trop facile aux voleurs d'identité, qui utilisent divers types d'attaques. Par exemple, les utilisateurs utilisent des mots de passe identiques ou similaires pour leurs comptes privés et professionnels. Ils peuvent également recourir à des modèles de mots de passe similaires avec des éléments tels que la première lettre du nom ou le code postal du lieu de résidence pour différents services, qui peuvent être facilement devinés sans utiliser le hachage. De nombreux administrateurs utilisent même le même mot de passe pour leurs comptes standard et administrateur, alors qu'ils devraient être mieux informés - un comportement qui devrait être formellement sanctionné.

#	MOT DE PASSE	NOMBRE DE CARACTÈRES DIFFÉRENTS	LONGUEUR DU MOT DE PASSE	ENTROPIE	FORCE BRUTE SUPERORDINATEUR	FORCE BRUTE PC + GPU
1	123456	10	6	~ 20 bits	< 1 sec	< 1 sec
2	Ag89!+	95	6	~ 39 bits	< 1 sec	< 1 sec
3	01234567890123456789	10	20	~ 66 bits	8 minutes	43 jours
4	Summer_2018	95	11	~ 72 bits	7 heures	6 ans
6	someruniversusvenus	26	20	~ 94 bits	> 3000 ans	23 Millions d'années
5	P@ssw0rdP@ssw0rd	95	16	~ 105 bits	6 millions d'années	∞
7	Djvdjfvb47643876*!43579439>	95	27	~ 177 bits	∞	∞

De nombreux types de mots de passe supposés sûrs peuvent être brisés en peu de temps (Image : Specops Software).

La sécurité des mots de passe n'a rien à voir avec les caractères spéciaux

Mais quels mots de passe sont forts ? Cela dépend avant tout de la rapidité avec laquelle un hachage de mot de passe, une sorte de chiffre de contrôle, peut être décrypté. La mesure mathématique de ce phénomène est l'entropie, qui quantifie le nombre minimal de bits nécessaires pour représenter l'information contenue dans un message, et donc sa complexité mathématique. Une entropie d'au moins 70 bits est considérée comme sûre pour les utilisateurs simples, et de 90 bits et plus pour les comptes administrateurs.

La longueur du mot de passe est déterminante pour l'entropie. Ce n'est qu'à partir d'une longueur d'au moins 15 caractères que des mots de passe sûrs sont mathématiquement possibles. Les chiffres, les caractères spéciaux ou les lettres majuscules dans le mot de passe augmentent la complexité, mais si le mot de passe est trop court, cela ne sert à rien. Mais même les mots de passe suffisamment complexes sont inadaptés s'ils sont trop courts ou déjà compromis.

La solution de l'avenir : des phrases de passe faciles à mémoriser

La solution la plus judicieuse au dilemme des mots de passe est donc celle des phrases de passe faciles à mémoriser et non compromises. Par principe, elles ne doivent pas être écrites et doivent donc être faciles à mémoriser. En revanche, il faut éviter de modifier trop fréquemment ces mots de passe qui ne sont suffisamment sûrs que grâce au passage du temps. Cependant, si un mot de passe est compromis, il doit être changé immédiatement. En outre, les mots de passe ne doivent pas être tirés de dictionnaires ou d'une liste de mots interdits propre à l'entreprise, trop faciles à deviner.

L'outil Specops Password Auditor analyse l'Active Directory et identifie les vulnérabilités liées aux mots de passe, qui sont affichées en un clin d'œil dans un tableau de bord interactif. (Image : Specops Software)

S’équiper des bons outils est nécessaire

Prendre tout cela en compte est une tâche écrasante pour toute équipe de sécurité informatique. Plus le nombre de comptes et de services est élevé, plus la situation devient confuse. Il est donc conseillé d'utiliser un gestionnaire de mots de passe doté de fonctionnalités et de performances supérieures à la moyenne et capable de faire face à l'évolution des exigences en matière de protection des mots de passe.

Toutefois, si vous souhaitez tester la sécurité de vos propres mots de passe avant de vous décider pour un outil, vous pouvez le faire avec Specops Password Auditor, qui peut être téléchargé gratuitement. L'outil analyse l'Active Directory et identifie les vulnérabilités liées aux mots de passe. Les informations recueillies sont résumées dans un rapport interactif et permettent de savoir si certains comptes utilisent des mots de passe faibles, compromis, expirés ou identiques.

Specops Password Policy : Définir des politiques de mot de passe pour des groupes d'utilisateurs.

Un exemple de logiciel capable de répondre à une grande variété d'exigences en matière de mots de passe est Specops Password Policy pour la protection d'Active Directory. La solution est exécutée parallèlement au filtre Windows sur les serveurs du domaine. L'outil vérifie les mots de passe par rapport à une base de données en ligne de mots de passe déjà compromis, qui compte actuellement plus de 2,5 milliards de mots de passe et qui est mise à jour quotidiennement. En outre, une version hors ligne contenant 760 millions de mots de passe est disponible. Des dictionnaires individuels peuvent également être ajoutés.

Specops Password Policy peut être utilisé pour appliquer des politiques pour des groupes entiers d'utilisateurs. Les dates d'expiration peuvent être définies en fonction de la longueur du mot de passe, de sorte que les employés ayant des mots de passe plus longs doivent les changer moins souvent. Les utilisateurs dont les mots de passe ne sont pas conformes à la politique reçoivent un retour d'information détaillé sur ce qui doit être modifié. De cette façon, les voleurs de mots de passe n'ont pratiquement aucune chance et la conformité est maintenue.