Le SSO pour renforcer la sécurité des identités

La crise sanitaire, le recours massif au télétravail et l'augmentation constante des attaques ont contraint de nombreuses entreprises à faire évoluer leur approche de la sécurité ces derniers mois.

En effet, les modèles traditionnels, basés sur les pare-feux et les VPN, n'ont pas été conçus pour protéger les environnements IT hautement distribués ; c'est-à-dire avec beaucoup d'employés travaillant de chez eux. Or, lorsque les organisations adoptent une infrastructure cloud hybride et se tournent vers un nombre croissant d'applications SaaS, l'identité devient le seul périmètre de sécurité pour les télétravailleurs.

Avec cette nouvelle normalité, une cybersécurité efficace repose sur la capacité à gérer et à authentifier de manière sûre les identités, ainsi qu'à contrôler l'accès de chaque personne, application et machine ; qu'elle se trouve à l'intérieur ou à l'extérieur du périmètre du réseau. Désormais, l'ensemble des identités peuvent devenir à privilèges – autrement dit avec des droits d'accès élevés – sous certaines conditions, en fonction des systèmes, des environnements, des applications ou des données auxquels elles accèdent, ou des types d'opérations qu'elles effectuent.

Le problème des mots de passe…

Dans ce contexte, il n'est pas surprenant que les cybercriminels ciblent avant tout les identifiants à privilèges – du fait de leur niveau d'accès aux données et infrastructures les plus critiques d'une organisation. Selon le rapport Verizon DBIR 2020, plus de 80 % des violations de données liées au piratage informatique impliquent l'utilisation d'identifiants perdus ou volés, ou « la force brute » qui consiste à essayer différentes combinaisons d'identifiants jusqu'à ce qu'un fonctionne.

En compromettant des identifiants à privilèges, les attaquants peuvent accéder à des ressources internes, obtenir des données confidentielles et perturber l'activité. Pourtant, de nombreuses entreprises continuent à recourir à des mots de passe pour sécuriser les accès à privilèges des utilisateurs. Cette approche est problématique à de nombreux égards.

Microsoft Services fait l'objet de plus de 300 millions de tentatives de connexion frauduleuses chaque jour, et pourtant, 53 % des utilisateurs n'ont pas modifié leur mot de passe au cours des 12 derniers mois. Et même changé, il est fort probable que le nouveau mot de passe soit faible ou utilisé pour plusieurs comptes, ce qui le rend vulnérable.

Bien entendu, de nombreuses organisations ont pris des mesures pour sécuriser les identités, telles que l'obligation d'utiliser des mots de passe uniques et forts, et de les changer fréquemment. Toutefois, ces contrôles peuvent en réalité causer plus de mal que de bien, en incitant les utilisateurs finaux à adopter des pratiques risquées en matière de mots de passe, comme les écrire sur papier, et en imposant une charge inutile aux équipes IT responsables de la gestion manuelle des accès.

La mémorisation, l'oubli, la saisie et la réinitialisation des mots de passe représentent donc une

difficulté significative et une perte de productivité ; en particulier à l'ère du travail à distance, où les employés et les fournisseurs tiers dépendent fortement des applications pour collaborer et accéder aux ressources de l'entreprise.

Les employés perdent ainsi environ 12,6 minutes par semaine à saisir et à réinitialiser ses mots de passe. D'après une étude de PwC, environ 30 % de tous les appels au support IT sont liés à des mots de passe, ce qui détourne de précieuses ressources IT de missions à caractère plus stratégique.

… peut être résolu avec le SSO

L'authentification par signature unique (SSO) résout ce problème endémique des mots de passe et réduit la surface d'attaque. Les entreprises sont ainsi à même d'appliquer systématiquement des politiques de mots de passe plus strictes et de réduire le risque de mauvaises pratiques en éliminant complètement le recours aux mots de passe individuels.
Grâce au SSO, les organisations peuvent utiliser une seule identité sécurisée pour l'ensemble des applications, des terminaux et des ressources.

En outre, l'expérience de l'utilisateur final est améliorée : il peut accéder en un seul clic aux applications dans le cloud et sur site. Sans compter que pour aider les employés à maintenir leur productivité et à évoluer au rythme de l'entreprise, certaines solutions SSO ne nécessitent des contrôles de sécurité supplémentaires que pour les demandes d'accès à privilèges à haut risque.

Pour les équipes IT, le SSO a l'avantage de rompre les silos et de simplifier la gestion des utilisateurs et des comptes, grâce à une intégration homogène des répertoires ; et de bénéficier d'une visibilité complète de l'activité des utilisateurs en matière d'accès, ce qui permet de satisfaire aux exigences de conformité relatives à l'accès, de faciliter la production de rapports et d'améliorer la sécurité globale.

Les organisations peuvent tirer de nombreux autres avantages à long terme en mettant en œuvre des solutions SSO. Par exemple, avec des outils en libre-service correctement configurés, les entreprises seront en mesure de réduire considérablement leurs coûts IT en diminuant le nombre de tickets et d'appels au service d'assistance liés aux mots de passe. En outre, le SSO permet d'éliminer tout risque de comptes restant actifs lorsque les employés changent de rôle ou quittent l'entreprise.

Certaines solutions SSO peuvent même étendre les capacités de sécurité au-delà des mots de passe, pour intégrer l'authentification à plusieurs facteurs (MFA) et les méthodes d'authentification sans mot de passe.