Un futur sans mot de passe est-il possible ?

En effet, si de nombreuses équipes de sécurité recommandent aux utilisateurs professionnels de créer des mots de passe individuels, complexes et forts pour chacun de leurs comptes, beaucoup ne suivent pas ce conseil. Par conséquent, de nombreux mots de passe sont soit trop faibles, soit fréquemment réutilisés pour se connecter à plusieurs outils ou plateformes.

Une fois compromis ou volés, les identifiants peuvent être vendus en ligne, et les attaquants comptent sur le fait que la plupart des utilisateurs réutilisent les mêmes mots de passe ; ce qui est plus inquiétant, c'est donc l'impact à long terme de chaque attaque.
Actuellement, les cybercriminels peuvent accéder à des millions de mots de passe volés, divulgués sur des sites publics, afin de compromettre des informations précieuses sur d'autres sites.

Renforcer la sécurité grâce à l'authentification

Les authentifications à deux facteurs (2FA) et à facteurs multiples (MFA) ont été créées pour pallier les limites de sécurité associées aux mots de passe.
Grâce à ces deux méthodes, l'identité d'une personne est authentifiée à la fois par un élément qu'elle connaît (le mot de passe) et par un élément qu'elle possède ; comme une application sur son téléphone ou une forme d'authentification biométrique, comme l'empreinte du pouce. Si un mot de passe est compromis, les cybercriminels auront alors besoin d'un autre facteur pour pouvoir l'utiliser.

Bien que ces méthodes renforcent la sécurité, certains administrateurs et responsables des opérations craignent toujours que ces mesures supplémentaires ne nuisent à la productivité.
Cela est particulièrement vrai aujourd'hui dans le monde des développeurs et des architectes cloud, qui misent sur la vitesse et la flexibilité.

Le problème est que l'accès dont ces personnes disposent est bien trop critique pour qu'il soit laissé dans une situation de vulnérabilité : les développeurs et les architectes figurent parmi les utilisateurs les plus privilégiés au sein d'une organisation ; ils ont accès à des secrets et contrôlent totalement leur environnement, d'où la nécessité d'une authentification supplémentaire.

Cependant, les authentifications 2FA et MFA ne sont pas parfaites. Le stockage et la rotation des identifiants dans un coffre-fort numérique ou un gestionnaire d'informations d'identification constituent une autre stratégie à mettre en place. Elle empêche la réutilisation des mots de passe et résout par conséquent le problème lié aux « personnes ».

En outre, les organisations sont désormais amenées à devoir protéger des informations d'identification sans mot de passe, notamment pour les clés SSH ou les clés API du cloud et les secrets DevOps qui permettent d'accéder à différents systèmes et applications. La mise en coffre-fort et la rotation de ces identifiants empêchent leur réutilisation, tout en supprimant les difficultés liées à leur gestion manuelle.

Authentifier sans mot de passe

L'expression « sans mot de passe » ne signifie pas que ces derniers cessent d'exister ; cela signifie simplement que les utilisateurs finaux et les comptes d'application ne sont pas en contact direct avec les identifiants nécessaires pour accéder aux systèmes critiques. L'objectif est alors d'améliorer la sécurité et de simplifier l'accès aux ressources pour les utilisateurs.
Avec cette authentification, ces derniers n'ont pas besoin de mémoriser ou de saisir des mots de passe pour se connecter aux applications.

Au contraire, l'accès est fourni en fonction des autorisations de l'utilisateur ou d'un élément qui ne peut être pas obtenu par une personne non légitime, comme une identification biométrique. Si un mot de passe n'est jamais révélé à l'utilisateur, il ne peut alors jamais être volé.

Grâce à cette approche, les équipes IT et de sécurité peuvent avoir la certitude que l'accès des utilisateurs est sécurisé et que les mots de passe ne sont pas réutilisés ou partagés.
Les cybercriminels ne sont donc pas en mesure de procéder au phishing des mots de passe ou des accès utilisateurs. Les données d'authentification ne sont jamais stockées dans le système comme le serait un mot de passe. Ainsi, toute personne ayant accès au système ne peut pas récupérer les données d'authentification, ce qui confère aux solutions sans mot de passe un avantage clé en matière de sécurité. Il en résulte une expérience positive pour les utilisateurs et une sécurité renforcée.

Gérer les accès à privilèges

Reste à protéger un accès sans mot de passe au compte racine d'une machine nouvellement acquise ou un compte de service exécutant des services essentiels à la mission.
Ces formes d'accès à privilèges représentent le plus grand risque pour les organisations et nécessitent des contrôles de sécurité encore plus rigoureux que ceux que peut fournir un outil ordinaire sans mot de passe.

L'accès aux systèmes qui contiennent les actifs les plus privilégiés d'une organisation, doit être protégé par une solution complète de gestion des accès à privilèges (PAM).
Ces outils peuvent recourir à un coffre-fort et isoler les identifiants afin que les utilisateurs ne les connaissent jamais – ce qui les rend, de fait, sans mot de passe – mais elles offrent également des couches de sécurité supplémentaires comme la surveillance des sessions, les enregistrements et la détection des menaces fondée sur l'analyse.

Finalement, les organisations doivent protéger leurs comptes de service, leurs administrateurs et leurs identités non humaines avec des solutions plus robustes et spécialisées. Toutefois, qu'il s'agisse de sécuriser l'accès à des informations critiques ou d'authentifier des utilisateurs individuels, les règles de base restent les mêmes.

D'une part, l'utilisateur ne doit pas connaître le mot de passe et il doit bénéficier d'une expérience simplifiée et rationalisée. D'autre part, les secrets doivent être protégés, faire l'objet d'une rotation adéquate et leur accès doit être sécurisé et surveillé.
Cette approche nous rapprochera ainsi d'un monde sans mot de passe, un monde plus sûr.