Devolutions

Pourquoi les mots de passe n'ont-ils pas encore disparu et ce que les entreprises peuvent faire pour l'instant?

SERAIT-IL TEMPS DE SE DÉBARRASSER UNE FOIS POUR TOUTES DES MOTS DE PASSE?

123456. Qwerty. Iloveyou. Non, ce ne sont pas des exercices pour apprentis dactylographes. Ce sont, étonnamment, les mots de passe choisis par de nombreux utilisateurs finaux en 2021.

Oui oui, vous avez bien lu : en 2021. Nous ne parlons pas ici du début de l'Internet, à la fin des années 1980, où les gens déambulaient avec leur très cool Walkman Sony. 2021, l'époque où les violations massives de données font les manchettes quasi quotidiennement et que 81 % d'entre elles sont dues à des mots de passe faibles.

Tout cela soulève une question importante : serait-il temps de se débarrasser une fois pour toutes des mots de passe? Bien que la majorité des professionnels de l'informatique et de la sécurité de l'information (InfoSec) croient que c'est la voie à suivre, un sondage récent a révélé que 85 % d'entre eux pensent que cela ne se produira pas de sitôt. Pourquoi? Bien qu'ils ne soient pas exempts de défauts, les mots de passe sont très polyvalents. Ils peuvent être utilisés sur n'importe quel appareil, à partir de n'importe quel endroit et à tout moment. À l'heure actuelle, dans la plupart des entreprises et dans pratiquement toutes les petites et moyennes entreprises (PME), une infrastructure qui fonctionne sans mot de passe n'existe pas.

Les vieilles manies ont la vie dure. Pour des milliards de personnes dans le monde, choisir et utiliser des mots de passe sont des habitudes qu'ils ont depuis des décennies. Ils connaissent le processus. C'est pourquoi passer soudainement à une réalité sans mot de passe serait non seulement déconcertant, mais désorientant. Dans une interview pour WIRED, Andrew Shikiar, le directeur général de l'Alliance FIDO, a mentionné : « C'est un comportement qu'on a appris. Il s'agit toujours de la création d'un mot de passe dans un premier temps. Le problème, c'est que cela repose sur une fondation vraiment médiocre. Nous devons briser cette dépendance. »

Comment les entreprises sont-elles censées s'y prendre? Surtout lorsque, comme indiqué précédemment, l'infrastructure en place ne peut prendre en charge une expérience utilisateur transparente sans mot de passe? De plus en plus d'experts recommandent aux entreprises d'adopter une approche hybride qui, sans éliminer complètement les vulnérabilités des mots de passe, réduit considérablement les risques. C'est une option plus réaliste pour la plupart des entreprises, car cela ne nécessite pas une refonte complexe et coûteuse de l'infrastructure et prend en charge un mélange de systèmes hérités sur site et de services privés ou publics sur le nuage.

Comment fonctionne une approche hybride?

Dans une approche hybride, les comptes liés au fournisseur d'identité de l'entreprise (ou IdP qui vient de l'anglais Identity Provider) sont utilisés pour s'authentifier auprès d'une solution de gestion des accès privilégiés (PAM). Cela permet aux utilisateurs de se connecter à des comptes d'actifs autonomes non fédérés (par exemple : imprimantes, équipements réseau, appareils spécialisés, etc.).

Avec une approche hybride, les utilisateurs n'ont besoin de connaître qu'un seul mot de passe : celui du fournisseur d'identité (IdP). La solution PAM facilite l'accès à tous les autres comptes. Les solutions PAM les plus avancées permettent également aux utilisateurs de se connecter à des comptes sans divulguer de mots de passe, améliorant encore plus la sécurité. Des contrôles avancés peuvent aussi être mis en place pour limiter l'accès au compte, comme les exigences de demande d'accès et l'utilisation basée sur le temps (c'est-à-dire qu'une fois que les utilisateurs ont la permission d'accéder à un compte, ils doivent le faire dans un délai précis, sinon cette permission expirera).

Le futur des mots de passe

Les mots de passe vont éventuellement être relégués aux oubliettes. Les générations futures ne comprendront probablement pas comment leurs ancêtres se sont appuyés sur une combinaison de mots, de chiffres et de symboles pour accéder à leurs comptes et appareils. Et cette réalité sans mot de passe est peut-être plus proche qu'on le croit : Gartner prédit que dans les mois à venir, 60 % des grandes entreprises mondiales et 90 % des entreprises de taille moyenne mettront en œuvre des méthodes sans mot de passe dans plus de la moitié des cas d'utilisation.

Pour le moment, les mots de passe continueront de jouer un rôle important dans nos environnements de travail. Adopter une approche hybride est un moyen stratégique, pragmatique et rentable pour les entreprises de réduire leur surface d'attaque et, finalement, de réduire les risques de sécurité. Étant donné que le coût moyen d'une violation de données a atteint 4,24 millions de dollars (USD) par incident, trouver des moyens intelligents et durables de réduire le risque n'est pas seulement une bonne pratique, c'est une exigence fondamentale.

Comment Devolutions peut-elle vous aider?

Votre entreprise envisage de mettre en œuvre une approche hybride pour la gestion des mots de passe? Devolutions peut vous aider!

Devolutions Server, notre solution auto-hébergée de gestion des comptes partagés et des mots de passe, offre des composants d'accès privilégié et s'intègre à Microsoft Active Directory et Microsoft Office365 pour authentifier l'identité unique de chaque utilisateur. Devolutions Server utilise également des paramètres de contrôle d'accès basés sur les rôles (RBAC) pour accorder des autorisations en fonction de l'appartenance à un groupe, ce qui améliore la sécurité tout en réduisant la charge administrative.

De plus, Devolutions Server s'intègre harmonieusement avec **Remote Desktop Manager**, qui utilise l'injection d'identifiants pour injecter des mots de passe lorsque les utilisateurs lancent des technologies d'accès à distance, ce qui signifie que les mots de passe ne sont jamais exposés.

Si votre entreprise adhère à (ou souhaite mettre en œuvre) une approche basée sur la Confiance zéro, vous pouvez ajouter **Devolutions Gateway** qui achemine toutes les connexions via un tunnel sécurisé. Cela empêche les mouvements latéraux, tout en éliminant la réutilisation des jetons d'authentification dans l'infrastructure.

Pour en apprendre davantage

- Planifiez une démonstration en direct de Devolutions Server.
- Essayez Devolutions Server gratuitement pendant 30 jours.
- Communiquez avec notre équipe des ventes pour toute question : sales@devolutions.net | +1 844 463.0419