Le zéro mot de passe devient possible

Découvrez pourquoi votre entreprise devrait abandonner les mots de passe et comment elle peut fournir une expérience de connexion transparente à ses employés.

80 % des failles restent attribuables aux mots de passe faibles ou réutilisés, et 76 % des employés rencontrent régulièrement des problèmes de mots de passe. Confronté aux exigences en ressources et aux risques de sécurité associés aux mots de passe, que peut faire le service informatique ?

Pourquoi votre entreprise doit passer au zéro mot de passe.

Éliminer les mots de passe peut sembler impossible, mais le bon mélange de technologies peut supprimer les problèmes liés aux mots de passe. Mais pourquoi votre entreprise songerait-elle à dépasser le mot de passe ? Passer au zéro mot de passe présente plusieurs avantages pour votre organisation :

Sécurité renforcée :

Les risques associés aux mots de passe, notamment ceux qui sont faibles, réutilisés ou mal gérés, sont bien connus. Près de 80 % des piratages impliquent l'exploitation d'identifiants volés. Lorsque vous supprimez les mots de passe de l'équation, vous diminuez considérablement les risques de piratage associés.

Meilleure expérience.

L'employé moyen lutte pour jongler plus de 100 mots de passe, et il n'est donc pas surprenant que 59 % des gens utilisent souvent ou toujours les mêmes mots de passe. Les employés veulent tout simplement des technologies rapides et simples à utiliser. En éliminant les mots de passe, vos employés se connectent plus rapidement à leurs outils de travail, tout en éliminant les pertes de temps associées aux comptes bloqués, réinitialisations et mises à jour fréquentes des mots de passe.

Plus de contrôle.

77 % des employés utilisent une app tierce dans le cloud à l'insu du SI et la plupart (83 %) des professionnels de l'informatique déclarent que les employés stockent des données

de l'entreprise sur des services dans le cloud non approuvés. En résumé, le SI manque de visibilité sur les accès des employés à l'échelle de l'entreprise et de contrôle sur « l'informatique parallèle ». Les technologies qui remplacent ou éliminent les mots de passe donnent au SI la capacité de supervision qui rendent la visibilité et le contrôle possibles.

Réduction des coûts.
En moyenne, les équipes du SI consacrent 4 heures par semaine rien qu'aux problèmes liés à la gestion des mots de passe et reçoivent 96 demandes liées aux mots de passe par mois. Les anciennes technologies gérées et exploitées en interne sont souvent coûteuses à gérer. Les solutions zéro mot de passe éliminent ces surcoûts, réduisent la quantité de main-d'œuvre nécessaire et libèrent des ressources du SI qui peuvent se concentrer sur des tâches à valeur ajoutée.

Comment passer au zéro mot de passe.

Commencez par centraliser les mots de passe.
Si les mots de passe sont un tel problème, c'est en partie parce que les employés doivent se débrouiller pour les gérer eux-mêmes. Commencez par fournir aux employés une solution de gestion des mots de passe en entreprise (GME) qui capture et stocke tous les mots de passe utilisés.

Les employés ne doivent plus mémoriser leurs identifiants (le gestionnaire de mots de passe les saisit à leur place) et le SI obtient de la visibilité sur l'hygiène des mots de passe de chaque connexion et chaque utilisateur.

Les mots de passe ne sont pas encore éliminés, mais les employés ne doivent mémoriser qu'un seul mot de passe maître, ce qui est un grand pas en avant.

Là où c'est possible, remplacez les mots de passe par d'autres protocoles sécurisés.
Ensuite, remplacez les mots de passe par l'authentification unique (SSO). En exploitant le protocole sécurisé SAML 2.0, les employés peuvent se connecter à leurs apps, qu'elles soient dans le cloud, mobiles ou internes, sans jamais stocker un mot de passe ni remplir un formulaire de connexion.

Associer le SSO et la GME permet aux employés de n'avoir qu'un seul mot de passe à mémoriser, et de se connecter à de nombreux services sans avoir à manipuler de mot de passe, tandis que tout identifiant exigé par un formulaire de connexion est automatiquement saisi à leur place.

Éliminez les mots de passe à l'aide d'une authentification plus robuste.
La dernière étape pour atteindre le zéro mot de passe consiste à mettre en œuvre l'authentification multifacteur. Généralement, on considère que l'authentification multifacteur ajoute des étapes de connexion, et il est vrai que l'un des principaux objectifs consiste à ajouter des couches de protection en exigeant des informations (ou « facteurs ») complémentaires pour valider l'identité.

Mais une solution d'authentification moderne peut associer des facteurs biométriques (humains) comme l'analyse des empreintes ou du visage à des facteurs contextuels (invisibles) comme l'ID de l'appareil, la géolocalisation ou l'adresse IP. Ces données peuvent servir à valider plus finement l'identité de l'utilisateur. De plus, elles peuvent remplacer les mots de passe, en évitant d'avoir à saisir un identifiant pour accéder à un portail SSO et GME ou à d'autres services.

Avec une solution d'identité tout-en-un, le zéro mot de passe devient possible.
Une solution d'identité qui associe GME, SSO et AMF est un moyen efficace pour les entreprises de fournir une expérience sans mot de passe aux employés. L'authentification sans mot de passe signifie une meilleure expérience, plus de visibilité et de contrôle pour le SI, une sécurité renforcée à l'échelle de l'organisation et une diminution des coûts informatiques. En résumé, c'est une solution gagnant-gagnant, tant pour les utilisateurs que les administrateurs.

Les entreprises qui souhaitent obtenir un contrôle simple et une visibilité unifiée de tous les points d'entrée, avec un accès intuitif et une expérience d'authentification multifacteur qui fonctionne à tous les niveaux, du cloud aux apps mobiles aux apps internes, peuvent essayer LastPass Identity.

En savoir plus sur l'unification de l'accès et de l'authentification avec LastPass Identity :
www.lastpass.com/products/identity