LastPass ••• | by LogMeIn

10 mesures
pour augmenter la sécurité et la productivité dans le cadre du travail à distance

Le travail à distance présente de nombreuses opportunités pour les entreprises, mais comporte aussi les défis suivants :

- Sécuriser l'ensemble de l'entreprise
- Garantir l'accès des employés aux ressources dont ils ont besoin pour être productifs

#1 Déployez l'authentification unique

L' authentification unique permet au service informatique de gérer l'accès à partir d'une vue unique, avec la flexibilité d'attribuer ou révoquer les accès si nécessaire.

90 % **des entreprises disent que la gestion de l'accès utilisateur est très importante dans le cadre de la sécurité générale de l'organisation.[1]**

#2 Ajoutez l'authentification multifacteur

L'authentification multifacteur ajoute une couche supplémentaire d'authentification pour une sécurité renforcée et des facteurs biométriques pour offrir une expérience de connexion transparente.

59 % **des entreprises classent le renforcement de l'authentification utilisateur comme un des points clés à améliorer dans le cadre de la gestion des identités et des accès (IAM).[1]**

#3 Utilisez des facteurs contextuels

Les stratégies contextuelles permettent d'appliquer des modalités d'authentification adaptées au processus de connexion pour une flexibilité et un contrôle renforcés.

60 % **des organisations estiment que la sécurité organisationnelle renforcée résulte de l'authentification multifacteur.[1]**

#4 Activez votre VPN en permanence

Les mots de passe forts et l'authentification multifacteur sur le VPN renforcent la sécurité pour garantir l'identité des employés avant toute tentative d'accès.

80 % **des fuites de données ont pour seule origine des mots de passe faibles, réutilisés ou piratés.[2]**

#5 Protégez votre poste de travail

L'authentification multifacteur au niveau du poste de travail garantit que seuls les employés légitimes peuvent s'authentifier même si le poste de travail est piraté.

30 % des fuites de données touchent les postes de travail des employés.[2]

#6 Partagez en toute sécurité

La fonctionnalité de partage de mots de passe permet le partage d'identifiants entre employés et garantit leur accès aux ressources nécessaires pour exécuter leur travail.

185 fichiers partagés sont utilisés en moyenne dans les entreprises.[3]

#7 Limitez les mots de passe

L'authentification sans mot de passe permet d'éliminer le mot de passe de l'expérience de connexion, et d'instaurer une manière plus transparente et sécurisée de travailler.

95 % **des professionnels de la sécurité informatique estiment que leur entreprise ferait bien de donner plus d'importance aux comportements visant à renforcer les mots de passe.[1]**

#8 Prenez des mesures à l'égard du Shadow IT

Un gestionnaire de mots de passe offre aux employés une localisation sécurisée pour gérer tous leurs identifiants, connus ou non par le service informatique.

77 % **des employés utilisent une app tierce dans le cloud à l'insu du service informatique.[4]**

#9 Déjouez les pratiques de fishing

La gestion des mots de passe permet de réduire les risques de fishing en évitant le remplissage automatique de mots de passe sur les sites suspects.

En moyenne, 26,5 % des destinataires d'un e-mail malveillant ont cliqué sur un lien dans le message.[5]

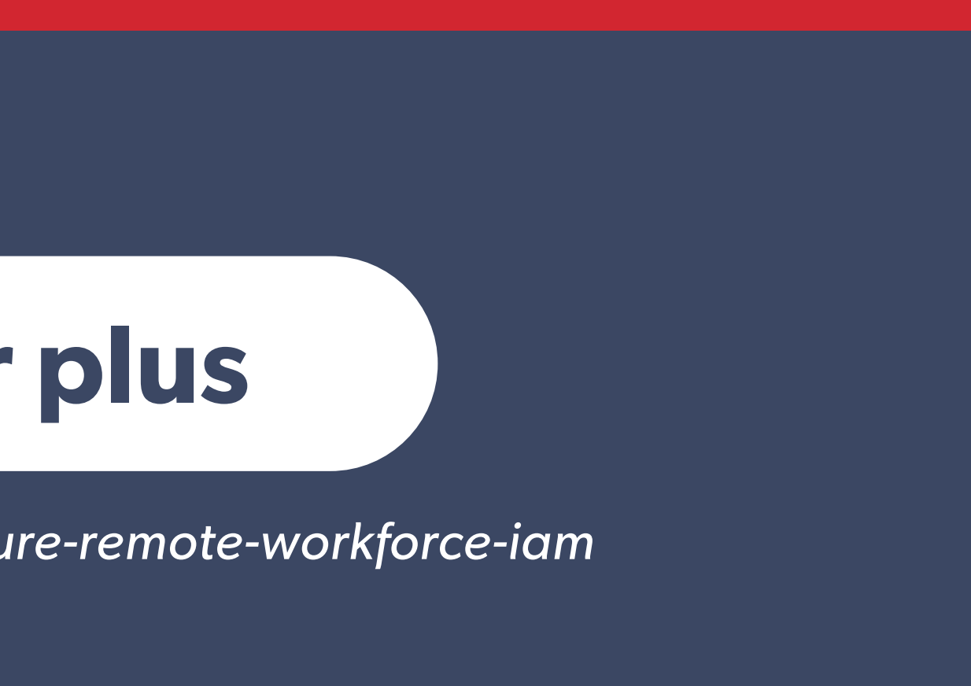
#10 Affichez une vue globale

À travers des rapports détaillés, surveillez l'activité grâce à des informations qui vous permettent de modifier les accès et l'authentification en fonction des besoins.

53 % **des entreprises considèrent la surveillance de l'activité utilisateur comme une priorité de leurs fonctionnalités IAM.[1]**

Le travail à distance, simplifié et sécurisé avec l'IAM

Le travail à distance n'a pas à être un problème si la stratégie IAM est bien adaptée.



Découvrez comment LastPass Identity peut sécuriser et dynamiser votre main-d'œuvre à distance pour renforcer sa productivité et assurer la sécurité de votre entreprise.

En savoir plus

www.lastpass.com/solutions/secure-remote-workforce-iam

Sources :

[1] Le guide de l'identité moderne
[2] 2019 Verizon Data Breach Investigations Report
[3] LastPass State of the Password Report 2019
[4] NTT Com, "Shadow IT Survey", 2016.
[5] IBM State of the Phish Research 2019

03.31.2020/PDF/LMI1356