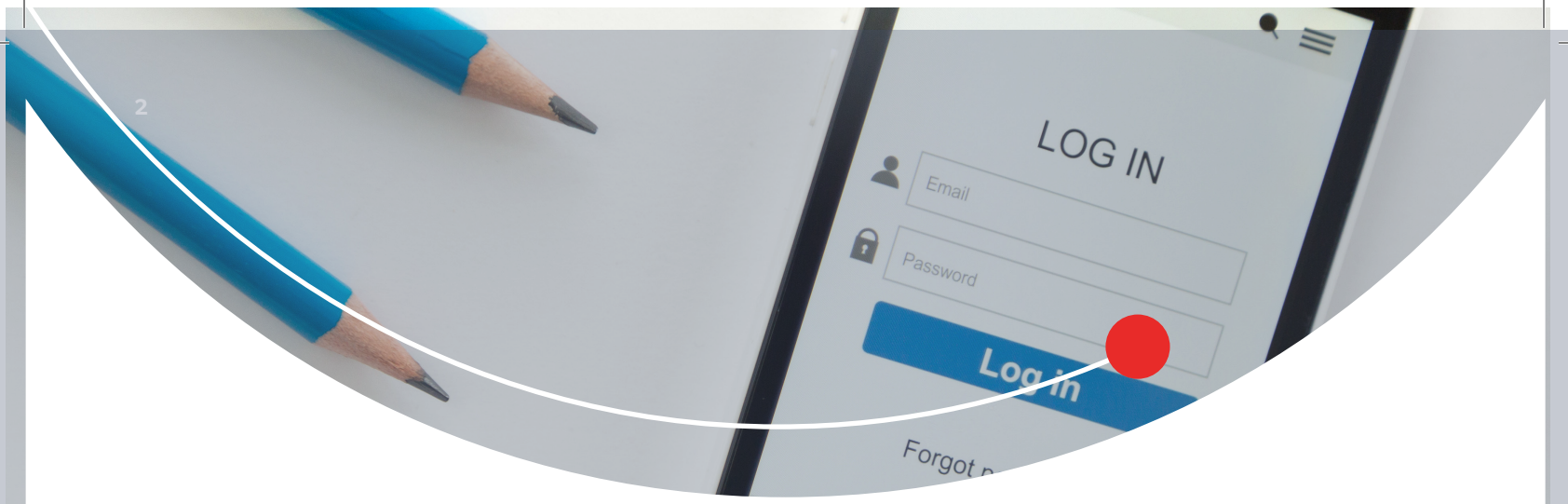
LastPass •••|
by LogMeIn

GUIDE DE L'AUTHENTIFICATION MULTIFACTEUR

Pourquoi les mots de passe ne suffisent pas à assurer la sécurité de votre entreprise



LES MOTS DE PASSE SEULS NE SUFFISENT PAS.

Les mots de passe ont été créés pour restreindre l'accès à des informations sensibles, mais ils constituent désormais un risque pour votre entreprise. L'utilisateur moyen doit gérer bien plus de 100 identifiants[1], ce qui est devenu un cauchemar logistique.

Les employés sont connus pour leurs mauvaises habitudes en matière de mots de passe, de la réutilisation endémique aux mots de passe faciles à deviner. Ils veulent seulement que les choses soient simples, donc tout ce qui les ralentit est un obstacle malvenu.

La transition vers un monde du travail centré sur le nuage et les outils personnels fait également grimper la complexité. L'augmentation du nombre d'apps, d'appareils et d'utilisateurs entraîne un environnement hybride difficile à sécuriser pour le SI.

Et les règles strictes en matière de mots de passe, comme les changements fréquents, ne semblent pas avoir beaucoup d'effet.

80 % DES FUITES DE DONNÉES CONNUES SONT DUES AUX IDENTIFIANTS FAIBLES, RÉUTILISÉS OU VOLÉS[2].

FAITES-VOUS CONFIANCE AUX MOTS DE PASSE POUR PROTÉGER VOTRE ENTREPRISE ?

59 % DES INDIVIDUS
utilisent généralement ou toujours le même mot de passe[3].

47 % DES INDIVIDUS
disent qu'ils utilisent les mêmes mots de passe au travail et à la maison[4].

42 % DES INDIVIDUS
conservent leurs mots de passe dans un fichier non protégé[5].

61 % DES DIRIGEANTS INFORMATIQUES
ne comptent que sur la formation des employés pour l'application de mots de passe forts[6].

MÊME LES MOTS DE PASSE FORTS NE SUFFISENT PAS, LES ATTAQUES ÉTANT PLUS SOPHISTIQUÉES ET PERSISTANTES QUE JAMAIS.

Qu'il s'agisse d'hameçonnage ou de rançongiciels, de failles de type « zero-day », d'attaques de type « man-in-the-middle », d'enregistreurs de frappe ou de piratage de mots de passe, les cyberattaques utilisent des outils plus rapides et exploitent les faiblesses connues pour contourner les mots de passe les plus robustes. Chaque app, appareil et identifiant est une porte d'entrée à votre entreprise qui doit être mieux gardée.

LES ATTAQUES PAR RANÇONGICIEL ONT AUGMENTÉ DE 350 % EN 2017[7].

6 MOIS
POUR DÉTECTER UNE FUITE EN MOYENNE[8].

43 %
DES CYBERATTAQUES CIBLENT LES PME/PMI[9].

PLUS DE 90 %
DES CYBERINCIDENTS PEUVENT ÊTRE ÉVITÉS AVEC LES BONS OUTILS[10].

AJOUTEZ DES COUCHES DE SÉCURITÉ AVEC L'AUTHENTIFICATION MULTIFACTEUR.

Il est évident que les mots de passe ne suffisent plus à assurer la sécurité de votre entreprise. Les associer à des technologies et facteurs d'authentification supplémentaires est essentiel. L'authentification multifacteur (AMF) a été développée pour ajouter des étapes de vérification au processus de connexion. En créant des étapes de vérification supplémentaires, vous pouvez mieux valider l'identité de quelqu'un, tout en compliquant considérablement la tâche de ceux qui essaieraient de contourner vos défenses.

L'AUTHENTIFICATION MULTIFACTEUR PROTÈGE LES COMPTES AVEC :

1 Quelque chose que vous savez
Un « facteur de connaissance » comme un mot de passe.

2 Quelque chose que vous avez
Un « facteur de possession » comme un téléphone ou une clé de sécurité.

3 Quelque chose que vous êtes
Un « facteur d'inhérence » comme la biométrie.

En cas de vol d'un mot de passe, le pirate ne pourra pas accéder au compte sans tous les facteurs exigés.

QUE FAUT-IL PROTÉGER PAR AMF ?

Les meilleures options d'AMF améliorent considérablement votre posture de sécurité, sans ralentir les employés. De nombreux points d'accès à votre entreprise doivent être protégés par AMF, dont les suivants :

1. Comptes du SI et privilégiés
2. Télétravailleurs et sous-traitants
3. Apps dans le nuage
4. Bases de données
5. Réseaux
6. Authentification unique
7. Gestionnaires de mots de passe
8. Apps mobiles

Pour résumer, chaque utilisateur, app, identifiant et appareil est un point d'entrée à votre entreprise qui doit être sécurisé par AMF.

A2F OU AMF : QUELLES SONT LES DIFFÉRENCES ET LAQUELLE CHOISIR ?

Lorsque vous cherchez à renforcer la sécurité, l'authentification à deux facteurs (A2F) et l'AMF ont l'air identiques. Ce n'est pas le cas. L'authentification à deux facteurs est un bon point de départ, mais une approche unique ne fonctionne pas lorsque les utilisateurs ont des comportements, des appareils personnels, des niveaux d'accès et des attributs distincts. L'AMF est l'option la plus robuste, car la possibilité d'exploiter des facteurs supplémentaires et de les adapter à différentes situations pour valider l'identité se traduit par une expérience d'authentification plus fluide et une diminution considérable des piratages réussis.

De nombreuses entreprises commencent ici.

VÉRIFICATION EN DEUX ÉTAPES (V2E)

Un code à usage unique est envoyé par e-mail, SMS ou appel téléphonique à un ordinateur ou appareil mobile.

Votre entreprise utilise G Suite ? Vous avez donc certainement activé la V2E qui exige un code pour accéder à Google Apps. Lorsque les deux facteurs sont des « choses que vous savez », il ne s'agit pas à proprement parler d'A2F.

Certaines entreprises arrivent jusqu'ici.

AUTHENTIFICATION À DEUX FACTEURS (2FA)

Associe deux facteurs distincts : votre mot de passe (connaissance) et un code généré par une app sur un smartphone (possession) ou une lecture d'empreinte digitale (inhérence).

Bien plus sûr que la V2E grâce à la combinaison de deux facteurs distincts. Les solutions récentes sont économiques et évolutives, mais sont souvent dénuées de commandes d'administration granulaires et d'intégrations, et elles ne sont pas adaptées à un large éventail de cas d'utilisation et de situations.

Les entreprises les plus sécurisées arrivent ici.

AUTHENTIFICATION MULTIFACTEUR (AMF)

Passez de deux à trois facteurs ou plus, comme un mot de passe (connaissance), une notification push vers un appareil de confiance (possession) et une lecture d'empreinte (inhérence), ou exploitez des facteurs masqués et contextuels.

Les meilleures solutions d'AMF proposent une authentification adaptative qui exploite une combinaison de facteurs bio-métriques et contextuels. Une solution tout-en-un renforce la sécurité d'ensemble tout en fluidifiant l'expérience de connexion.

VOTRE AMF ACTUELLE A-T-ELLE UN TRAIN DE RETARD ?

De nombreuses entreprises ont mis en œuvre l'A2F (ou commencé à le faire) il y a plusieurs années, mais n'ont pas suivi les dernières avancées en matière d'authentification. La situation a beaucoup évolué, comme la manière dont l'AMF exploite les appareils comme les smartphones, l'expérience utilisateur ou encore les commandes d'administration.

FONCTIONNALITÉS CLÉS DES MEILLEURES SOLUTIONS D'AMF D'AUJOURD'HUI :

Règles exhaustives pour gérer les utilisateurs au niveau individuel, des groupes ou de l'organisation

Authentification adaptative qui exploite les facteurs biométriques et contextuels

Conception sécurisée avec chiffrement des données biométriques au niveau de l'appareil

Déploiement et gestion centralisés via un portail d'administration

La possibilité de combiner les options d'authentification, comme l'A2F traditionnelle, et l'authentification biométrique et adaptative

Prise en charge des apps dans le nuage, des apps anciennes et internes, des apps mobiles, des formulaires de connexion, etc.

L'AUTHENTIFICATION MULTIFACTEUR SE PRÉSENTE SOUS PLUSIEURS FORMES.

L'AMF a plus de dix ans, et il existe plus d'options que jamais. L'essor des smartphones personnels et les avancées des technologies mobiles (comme les caméras et les capteurs spécialisés) ont eu un impact particulièrement important sur les options d'AMF.

VOICI DES TYPES D'AMF LES PLUS COURANTS, DU MOINS AU PLUS RECOMMANDÉ :

- SMS et codes vocaux
- Jetons matériels
- Jetons logiciels
- Notifications push
- Facteurs biométriques
- Facteurs adaptatifs

Option d'AMF	Fonctionnement	Avantages	Inconvénients
SMS et codes vocaux	• L'utilisateur reçoit un code temporaire par SMS, appel téléphonique ou e-mail	• Familier et facile à mettre en œuvre	• Pas une vraie AMF, sauf si elle est associée à un autre facteur, puisque le code et le mot de passe sont tous deux des facteurs de connaissance • Déconseillé par NIST en raison de vulnérabilités[11]
Jetons matériels	• L'utilisateur saisit un code généré et affiché sur l'appareil • Ou l'utilisateur touche l'appareil pour envoyer un code à usage unique	• Difficile à voler • Nombreuses options : cartes à puce, jetons Bluetooth, porte-clés OTP, clés USB de type YubiKey ou RSA SecurID	• Les appareils coûtent $50+ • Faciles à perdre ou oublier • Généralement plus fastidieux à utiliser
Jetons logiciels	• L'utilisateur saisit un code à usage unique généré par une app exécutée sur ordinateur ou smartphone • Ex. : Google Authenticator et Microsoft Authenticator	• Ne peuvent pas être perdus ou volés • Économiques • Mises à jour automatiques • Faciles à fournir aux utilisateurs dans le monde entier	• Fonctionnalité limitée. Ne peuvent pas être associés à d'autres facteurs pour renforcer la sécurité • Contrôle administratif limité

Option d'AMF	Fonctionnement	Avantages	Inconvénients
Notifications push	• Les demandes d'accès sont transmises par notification hors bande vers un appareil mobile de confiance • L'utilisateur touche « Accepter » ou « Refuser »	• Simple et rapide pour les utilisateurs • Le code ne peut pas être intercepté • Les demandes sont transmises en temps réel • Un code ou facteur biométrique peut sécuriser l'appareil • Installation en libre-service • Mises à jour automatiques	• De nombreuses apps populaires n'offrent pas de supervision et de contrôle administratif exhaustif à base de règles • Les entreprises doivent trouver un fournisseur qui s'intègre aux technologies existantes et donne aux administrateurs le contrôle et la visibilité nécessaires
Facteurs biométriques	• Les ordinateurs et smartphones sont désormais équipés de capteurs plus sensibles et intelligents • L'identité de l'utilisateur peut être validée par empreinte digitale, iris, reconnaissance faciale et même par rythme cardiaque	• Les dernières solutions sont économiques • Les consommateurs ont l'habitude de la validation des empreintes digitales • Moyen simple et sûr d'authentifier les utilisateurs	• Coût historiquement prohibitif pour de nombreuses entreprises • Les anciennes solutions souffraient d'une expérience utilisateur compliquée • Les entreprises doivent s'assurer que les données biométriques sont protégées et ne sont pas transmises ou stockées sur un serveur central
Facteurs adaptatifs	• Adapte les décisions d'authentification à une situation de connexion donnée • Géolocalisation, ID d'appareil, adresse IP et d'autres caractéristiques servent à bâtir un profil d'utilisateur • Sélectionne une combinaison de facteurs en fonction du profil de risque et des habitudes de l'utilisateur	• Expérience de connexion naturelle et transparente • Sécurité renforcée par l'utilisation de plusieurs facteurs • Meilleure visibilité et plus de contrôle pour les administrateurs grâce aux règles souples et granulaires • Évolutif et économique en exploitant le matériel existant (smartphones)	• Certaines solutions fonctionnent en silo. Les meilleures s'intègrent aux technologies existantes et gèrent tous les cas d'utilisation • Les entreprises doivent privilégier les méthodes d'authentification mixtes, qui permettent d'appliquer plusieurs options d'AMF au niveau des utilisateurs ou des groupes • Les entreprises doivent examiner la manière dont les données biométriques sont protégées

Les meilleures plates-formes d'authentification offrent la possibilité de choisir plusieurs méthodes d'AMF, ce qui vous permet d'investir dans une solution complète tout en l'adaptant aux cas d'utilisation particuliers de votre entreprise.

ADMINISTRATEURS ET UTILISATEURS : LA SÉCURITÉ SANS SACRIFIER LA CONVIVIALITÉ.

Pour qu'une solution d'AMF soit adoptée avec succès dans votre entreprise, vous devez répondre aux besoins des administrateurs informatiques comme des utilisateurs finaux. Lésiner sur les fonctionnalités ou la convivialité pour les uns ou les autres suscitera résistance et insatisfaction.

LES ADMINISTRATEURS ONT BESOIN DES ÉLÉMENTS SUIVANTS :

- Des règles qui permettent d'exercer un contrôle dans toute l'organisation, au niveau des utilisateurs et des groupes
- Une configuration prête à l'emploi capable de se brancher sur l'infrastructure existante (comme Microsoft Active Directory)
- La prise en compte de tous les cas d'utilisation de l'entreprise
- La compatibilité avec les solutions d'authentification unique, de gestion des mots de passe et de gestion des accès
- Une diversité de méthodes d'AMF, biométriques, par notification push ou encore adaptatives, qui peuvent être fournies au niveau individuel ou des groupes

LES UTILISATEURS FINAUX ONT BESOIN DES ÉLÉMENTS SUIVANTS :

- Une installation en un minimum d'étapes
- Peu ou pas de formation
- Une expérience de connexion fluide qui devient vite transparente
- La confidentialité de leurs données biométriques

71 % DES EMPLOYÉS SONT PRÊTS À ESSAYER DE NOUVELLES TECHNOLOGIES LORSQU'ELLES PROMETTENT UNE MEILLEURE EFFICACITÉ SANS PERTURBE LEURS HABITUDES[12].

POURQUOI VOUS NE POUVEZ PAS IGNORER LA NÉCESSITÉ DE L'AMF.

Avec ses avantages de sécurité supplémentaires, l'AMF est vivement recommandée pour les entreprises de toutes tailles. Sélectionner la bonne solution d'AMF est l'une des façons les plus économiques et efficaces de renforcer votre posture de sécurité d'ensemble et de protéger votre entreprise des cyberattaques.

Lorsqu'une solution est simple à utiliser et qu'elle élimine (au lieu de créer) des obstacles pour les utilisateurs, les employés l'adoptent volontiers et votre entreprise s'en trouve mieux protégée. Les meilleures solutions offrent aux administrateurs différentes méthodes d'AMF, pour que vous puissiez déployer une seule solution et adapter son fonctionnement en fonction de l'évolution de vos besoins.

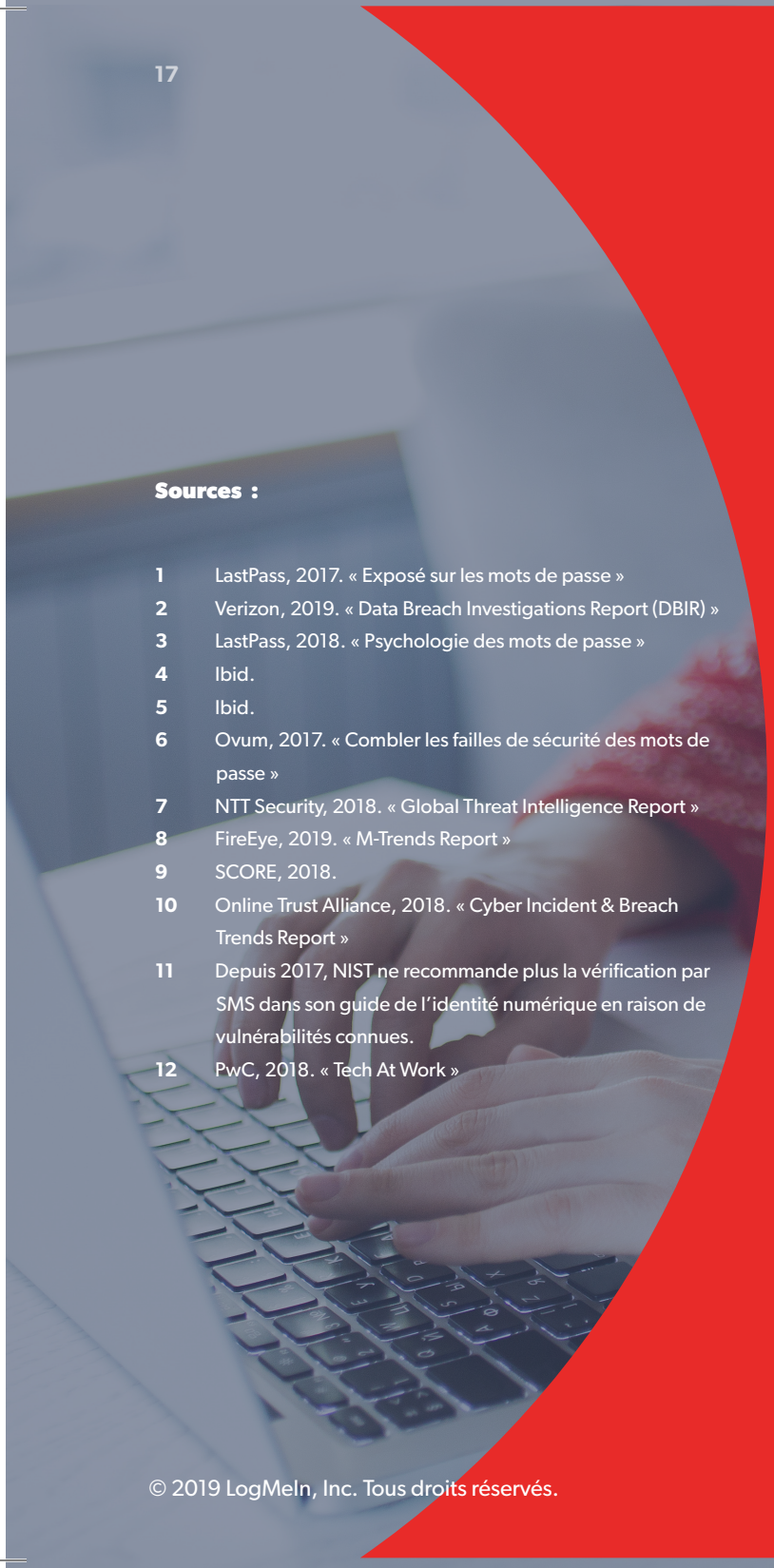
La solution d'AMF idéale offre des commandes souples, évolue avec la croissance de l'entreprise, est prête à l'emploi et dotée d'une expérience utilisateur appréciée des employés. Mais il ne suffit pas d'avoir une stratégie d'authentification multifacteur isolée. Votre entreprise a besoin d'une solution intégrée qui prend en charge vos applications existantes, avec des règles et des rapports qui permettent d'effectuer un suivi des utilisateurs de l'authentification jusqu'aux accès, pour plus de contrôle et de visibilité.

DÉCOUVREZ COMMENT LASTPASS REND L'AUTHENTIFICATION AUSSI SÛRE QUE FLUIDE.

LastPass MFA protège votre entreprise avec une technologie de pointe actuelle tout en simplifiant l'expérience de connexion des employés. LastPass MFA va au-delà de l'authentification à deux facteurs standard pour s'assurer que les bons utilisateurs ont accès aux bonnes données au moment adéquat, sans complexité supplémentaire.

Conçu sur un modèle unique de sécurité, LastPass MFA garantit la confidentialité et la protection des données biométriques tout en tirant parti de nombreux autres facteurs pour identifier et authentifier les utilisateurs. Créez des règles au niveau de l'utilisateur ou des groupes, avec la souplesse nécessaire pour gérer l'authentification d'une manière adaptée aux besoins de votre entreprise.

LastPass MFA est une solution d'AMF tout-en-un moderne qui offre une expérience multifacteur intuitive, qui est simple à déployer pour les administrateurs et simple à adopter pour les employés.



Sources :

1 LastPass, 2017. « Exposé sur les mots de passe »
2 Verizon, 2019. « Data Breach Investigations Report (DBIR) »
3 LastPass, 2018. « Psychologie des mots de passe »
4 Ibid.
5 Ibid.
6 Ovum, 2017. « Combler les failles de sécurité des mots de passe »
7 NTT Security, 2018. « Global Threat Intelligence Report »
8 FireEye, 2019. « M-Trends Report »
9 SCORE, 2018.
10 Online Trust Alliance, 2018. « Cyber Incident & Breach Trends Report »
11 Depuis 2017, NIST ne recommande plus la vérification par SMS dans son guide de l'identité numérique en raison de vulnérabilités connues.
12 PwC, 2018. « Tech At Work »

LastPass •••|
by LogMeIn

EN SAVOIR PLUS SUR
WWW.LASTPASS.COM/PRODUCTS/MULTIFACTOR-AUTHENTICATION

05.27.19/PDF/ LMI0638C