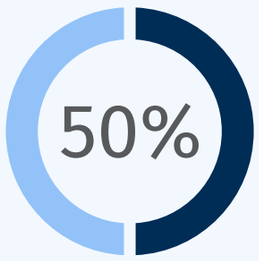
Authentification multifacteur : Une sécurité forte, simple et flexible

Protection essentielle pour les petites et moyennes entreprises

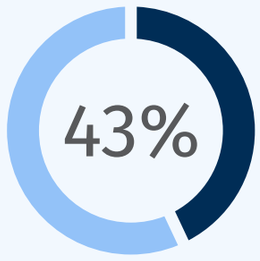
Le coût élevé d’une sécurité faible

Chaque jour, les cyberattaques sont de plus en plus élaborées. Les cybercriminels tirent parti de méthodes et de normes de sécurité faibles et obsolètes pour accéder aux comptes et aux données sensibles de façon alarmante.

Compte tenu de l’augmentation considérable du nombre de cyberattaques, un renforcement des mesures de sécurité est non seulement recommandé, mais essentiel, en particulier pour les PME, qui en subissent plus que jamais les effets sur leurs finances, leur réputation et leurs activités.

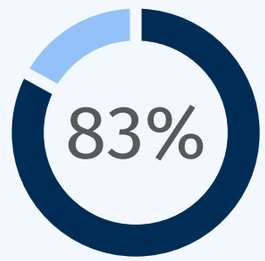


Augmentation des cyberattaques au cours de l’année écoulée[1]



Par de cyberattaques visant de petites entreprises

Nombre d’heures d’indisponibilité après une violation de sécurité type



Part de PME non préparées financièrement à se remettre d’une attaque[2]

Ces statistiques sont effrayantes, mais il existe une solution : **80 à 90 %**[3] des cyberattaques peuvent être évitées grâce à l’authentification multifacteur (MFA).

[1]https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=5cdc68866b61

[2]https://cybersecurity-magazine.com/10-small-business-cyber-security-statistics-that-you-should-know-and-how-to-improve-them/

[3]https://www.infosecurity-magazine.com/news/tech-execs-mfa-prevent-90-of

Comprendre l'authentification multifacteur (MFA)

Au lieu d'utiliser un facteur d'authentification unique, les solutions d'authentification multifacteur consistent à vérifier une identité au moyen de deux méthodes différentes au moins, notamment :

CE QUE VOUS AVEZ
- Smart Card
- Clé de sécurité
- Badge d'accès
- Jeton OTP
- Téléphone portable

CE QUE VOUS SAVEZ
- Code PIN
- Mot de passe
- Questions de sécurité

CE QUE VOUS ÊTES
- Empreinte digitale
- Reconnaissance faciale
- Reconnaissance vocale

Les entreprises peuvent combiner les méthodes d'authentification de leur choix dans n'importe quel ordre.

Carte + mot de passe + empreinte digitale

Téléphone portable + code PIN + question de sécurité

Clé de sécurité compatible FIDO + PIN

Ces couches d'authentification fonctionnent ensemble pour réduire le niveau de risque. Même quand un facteur d'authentification est compromis, un autre est requis de l'utilisateur pour accorder l'accès – les données et les actifs protégés restent ainsi sécurisés.

Plus rapide avec FIDO

Le système FIDO (Fast IDentity Online) remplace les connexions reposant uniquement sur la saisie d'un mot de passe par des expériences d'authentification fiables et simples sur tous les sites Internet et applications. Il s'appuie sur des normes gratuites et ouvertes pour plus de sécurité et de commodité, à la fois pour les utilisateurs et les organisations. Plus d'informations sur fidoalliance.org/how-fido-works

HID

MFA : sécuriser les éléments essentiels pour vous

L'authentification multifacteur (MFA) peut et doit être utilisée partout où l'accès à des ressources sensibles doit être protégé contre les cyberattaques et les erreurs humaines. Les PME y ont recours pour sécuriser certains éléments, notamment :

- **Bases de données et applications –** Accès sécurisé aux bases de données, logiciels de comptabilité et de gestion des RH, ainsi qu'aux applications en ligne, dans le cloud et sur site à l'aide de Smart Cards, de clés de sécurité, de jetons OTP ou de systèmes d'authentification mobiles
- **Ordinateurs et appareils des employés –** Protégez les appareils à domicile et dans les bureaux distants en ajoutant une deuxième couche d'authentification avec une clé de sécurité ou une Smart Card, en plus du mot de passe traditionnel
- **Appareils multi-utilisateurs –** Favorisez une connexion rapide et sécurisée des employés aux ordinateurs et périphériques partagés dans les environnements tels que les commerces de détail, les usines, les établissements de santé, etc.
- **Réseaux et serveurs –** Les réseaux VPN et serveurs sécurisés facilitent l'accès des employés aux ressources de travail nécessaires en tout lieu — y compris depuis un réseau public

MFA : une référence, dont l'adoption est à la traîne

Compte tenu de l'importance des risques et de l'existence de solutions simples, on pourrait penser que la majorité des PME tirent parti de l'authentification multifacteur (MFA). Or, une étude récente du Cyber Readiness Institute (CRI)[4] révèle que seules 46 % d'entre elles ont mis en œuvre un telle politique, pour les raisons suivantes :

1. ELLES NE SAVENT PAS QUE CES SOLUTIONS EXISTENT

55 % des PME ne sont pas protégées, simplement par ignorance de l'authentification multifacteur et de ses avantages.

2. ELLES NE COMPRENNENT PAS CES SOLUTIONS

30 % des propriétaires d'entreprises ont déclaré ne pas avoir recours à la MFA par méconnaissance du mode de fonctionnement de ces solutions. En réalité, il existe de nombreux types de MFA différents, allant d'options plug-and-play simples et faciles à déployer à des modules intégrés plus complexes. En outre, les entreprises ont le choix entre divers formats (cartes, clés et applications mobiles) et méthodes (FIDO, PKI, OTP, notifications push ou biométrie).

3. ELLES PENSENT QU'ELLES NE SONT PAS PRATIQUES

20 % des PME estiment que la MFA n'est pas pratique. En réalité, nous sommes tous beaucoup plus familiarisées avec ces solutions que nous ne le pensons. Toute personne qui a déjà saisi un code PIN et inséré une carte bancaire dans un distributeur de billets a déjà utilisé la MFA. Au total, le processus ne dure que quelques secondes et peut permettre d'éviter des cyberattaques coûteuses, pouvant potentiellement ruiner la réputation d'une entreprise, voire l'obliger à mettre la clé sous la porte.

[4]https://cyberreadinessinstitute.org/resource/global-small-business-multi-factor-authentication-mfa-study/

La MFA comme solution pour les PME : avantages

L'authentification multifacteur (MFA) peut être la pièce maîtresse d'un programme de cybersécurité solide pour les entreprises de toutes tailles, en particulière pour les PME, dont les défis et les situations sont uniques. Sa mise en œuvre permet aux entreprises de bénéficier d'une sécurité et d'une commodité accrues à plusieurs égards.

FINIS LES MOTS DE PASSE

En moyenne, une personne doit conserver plus de 100 mots de passe[5] dans le cadre de sa vie privée et professionnelle. Par facilité, de nombreux utilisateurs utilisent des mots de passe faciles à mémoriser ou identiques pour plusieurs applications – de la connexion au réseau professionnel à leurs comptes bancaires personnels. Malheureusement, cela facilite également la tâche des personnes qui tentent de voler des données. De plus, les mots de passe oubliés doivent être réinitialisés, ce qui mobilise du temps et des ressources.

Grâce à la MFA, vous pouvez vous défaire de la dépendance aux mots de passe et protéger vos données tout en améliorant l'expérience utilisateur.

FAVORISER UN TRAVAIL À DISTANCE PLUS SÉCURISÉ

Les collaborateurs travaillent en tout lieu et à toute heure. Plus que jamais, les employés utilisent des appareils personnels et professionnels pour accéder à des réseaux et applications, parfois via des connexions Internet peu sécurisées. Même l'équipe de cybersécurité la plus efficace ne peut pas contrôler tous les lieux depuis lesquels les utilisateurs se connectent. Le mieux est donc d'instaurer des mesures de sécurité renforcées qui fonctionnent partout.

CONTRECARRER LES CYBERCRIMINELS

L'authentification multifacteur complique la tâche des cybercriminels potentiels qui cherchent à dérober des données de l'entreprise en accédant aux logiciels et aux équipements critiques, notamment les périphériques réseau. Elle ferme tous les points d'entrée fragiles d'un système non sécurisé et permet d'éviter 99,9 % des compromissions de comptes selon Microsoft[6].

[5]https://tech.co/password-managers/how-many-passwords-average-person

[6]https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

Trouver la solution optimale et le fournisseur idéal

Décider d'utiliser la MFA est facile, le choix de la solution et du fournisseur appropriés peut sembler plus difficile. La MFA n'est pas une solution universelle et le processus de sélection implique la prise en compte de nombreuses variables. Assurez-vous de conclure un partenariat avec un fournisseur qui répond à tous vos besoins, notamment :

- **Facilité d'utilisation —** Votre solution MFA doit non seulement comprendre une sélection de méthodes d'authentification, y compris sans mot de passe et résistantes au phishing basées sur FIDO ou PKI, mais également être facile à adopter et à utiliser. Cette mesure de protection est destinée à assurer pour votre sécurité et votre confort d'utilisation — pas à vous compliquer la tâche.
- **Méthodes et formats multiples —** Ne soyez pas liés à un petit ensemble de méthodes d'authentification (p. ex. OTP et notifications push) ou de formats (cartes ou téléphones portables). Optez pour un fournisseur offrant un vaste choix dans les deux domaines ainsi que différentes options selon les utilisateurs et les besoins de sécurité.
- **Déploiement et gestion simples —** Le déploiement de certaines solutions peut prendre plusieurs mois. Or, votre sécurité ne peut pas attendre. D'autres solutions nécessitent une formation approfondie, l'installation d'un nouveau serveur ou encore une adaptation du code des applications existantes. Optez pour une solution potentiellement opérationnelle en quelques jours et non en quelques mois.
- **Solution complète —** Assurez-vous que votre nouvelle configuration de sécurité couvre l'ensemble de vos actifs, des PC aux téléphones en passant par les applications intégrées et les réseaux.
- **Conformité —** Dans les secteurs réglementés en particulier, la conformité est un aspect essentiel. Optez pour une solution et un fournisseur capables de satisfaire aux exigences et réglementations en constante évolution du secteur, notamment en matière de protection des données (RGPD et CCPA notamment).
- **Adaptabilité –** Vos besoins en matière de sécurité sont amenés à évoluer avec le temps. Par ailleurs, certains utilisateurs ou domaines de votre entreprise peuvent avoir besoin d'un niveau de sécurité supérieur à d'autres. Assurez-vous que votre fournisseur vous offre cette flexibilité.

Authentification avancée : critères déterminants pour le choix d'un fournisseur

Pour en savoir plus sur le choix du fournisseur approprié, consultez le livre blanc de HID intitulé Advanced Authentication Buyers Guide.

Conciliez sécurité et facilité d'utilisation grâce à la solution MFA forte de HID

En qualité de leader mondial de la fourniture d'identités fiables, HID propose une gamme étendue et solide de solutions MFA comprenant des Smart Cards et des clés de sécurité Crescendo® reposant sur FIDO et PKI ainsi que des logiciels MFA comme DigitalPersona®.

La solution primée DigitalPersona aide les établissements de santé, les entreprises industrielles, les commerces, les centres d'appels, les autorités et d'autres organisations à sécuriser les connexions aux ordinateurs de bureau, sites Internet, VPN, réseaux et applications dans le cloud et sur site. Cette solution d'authentification multifacteur facile à déployer et à gérer permet de se conformer aux normes, impératifs et règles de sécurité en constante évolution et prend en charge le plus large éventail de méthodes d'authentification et de formats qui soit (biométrie, appareils mobiles, badges d'accès, Smart Cards et clés de sécurité…).

En plus de sécuriser l'accès aux données sensibles, aux applications et aux e-mails, les Smart Cards HID Crescendo très sûres peuvent aussi servir de badge d'identification visuelle des employés pour assurer un accès sécurisé aux bâtiments, aidant ainsi les propriétaires d'entreprises à faire coïncider accès physique et logique et à protéger à la fois les installations et les données avec un seul système d'authentification.

Prêt à faire passer votre sécurité à un niveau supérieur ? Contactez-nous dès aujourd'hui pour demander un essai et découvrir comment la MFA peut être mise en place dans votre entreprise.

hidglobal.com

Amérique du Nord : +1 512 776 9000
Numéro gratuit : 1 800 237 7769
Europe, Moyen-Orient, Afrique : +353 91 506 900
Asie Pacifique: +852 3160 9800
Amérique latine : +52 (55) 9171-1108

Pour plus de numéros de téléphone internationaux, cliquez ici

2022-11-15-iams-multi-factor-auth-smb-eb-fr
PLT-07034

Part of ASSA ABLOY