ÉVALUATION

# Évaluation des risques : sécurité de la solution MFA (Multi-Factor Authentication)

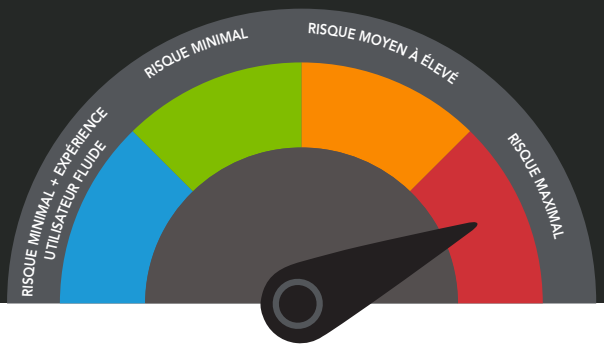
*Comprendre l'échelle de risque des solutions d'authentification actuelles*

80 % de toutes les violations liées au piratage impliquent le vol des informations d'identification des utilisateurs ou des mots de passe peu sécurisés[1] et plus de 613 millions de mots de passe ont été exposés par le biais de violations de données[2]. Ajouter une solution MFA (Multi-Factor Authentication) comme couche de sécurité supplémentaire lors de la connexion peut réduire considérablement les risques, mais la plupart des solutions MFA traditionnelles peuvent encore être compromises relativement facilement.

**Quel est le niveau de sécurité de l'authentification dans votre entreprise ? Comprenez les risques des modèles d'authentification actuels :**

# Risque maximal

Authentification par nom d'utilisateur et mot de passe




Les entreprises qui s'appuient uniquement sur la force des informations d'identification pour une authentification sécurisée sont hautement vulnérables aux attaques. Les noms d'utilisateur et mots de passe n'ont jamais été aussi peu sécurisés. Les informations de connexion sont volées, piratées et récoltées par des acteurs très motivés, avant d'être rapidement monétisées en étant utilisées ou vendues sur le Dark Web.

Les acteurs malveillants contournent le barrage des noms d'utilisateur et mots de passe des manières suivantes :

- **Credential stuffing**
- **Hameçonnage**
- **Pulvérisation de mot de passe**
- **Attaques en force**
- **Violation de données antérieure/réutilisation des mots de passe**
- **Réinitialisation du mot de passe**
- **Enregistrement des frappes**
- **Découverte locale**

Et le fait que les utilisateurs aient tendance à réutiliser des mots de passe sur plusieurs sites menace davantage la sécurité de l'entreprise. Le niveau de sécurité de votre société est égal à celui du compte personnel le moins sécurisé de vos utilisateurs. Les vulnérabilités inhérentes aux mots de passe, y compris les plus complexes, générés par des algorithmes, prouvent la nécessité de MFA. En fin de compte, il n'est jamais conseillé de se contenter d'un seul niveau de sécurité (dans ce cas, l'authentification à facteur unique). La sécurité de pointe comprend toujours plusieurs couches de défense.

# Risque moyen à élevé

MFA (Multi-factor authentication) standard


Ajouter la fonctionnalité MFA à votre système de sécurité de l'authentification améliore immédiatement la sécurité de l'entreprise. La solution MFA, comprenant l'authentification à deux facteurs (2FA), repose sur un minimum de deux facteurs d'authentification distincts pour vérifier l'identité d'un utilisateur. Le premier facteur est généralement un mot de passe. Le deuxième (et potentiellement le troisième) facteur peut être une information que vous connaissez, comme un code PIN ou une question de sécurité, un élément que vous avez, comme un terminal, un code/mot de passe à usage unique ou un jeton matériel/logiciel, ou encore, une donnée physique qui vous appartient, y compris une donnée biométrique comme une empreinte digitale ou une identification par reconnaissance faciale, ou bien des signaux contextuels comme votre emplacement.

Bien que la MFA traditionnelle réduit considérablement les risques par rapport à l'authentification à facteur unique par nom d'utilisateur/mot de passe, elle reste vulnérable à plusieurs méthodes de contournement de la sécurité d'authentification :

- **Hameçonnage**
- **Utilisation de proxys transparents (attaques de type MITM (man-in-the-middle))**
- **Interception de code d'authentification par e-mail ou SMS**
- **Credential stuffing**
- **Attaques de réplication**
- **Échange de carte SIM**
- **Ingénierie sociale**
- **Vulnérabilités dans les pages en ligne traitant des opérations de MFA**

Il existe de nombreux exemples bien documentés de contournement d'authentification multifactorielle par des acteurs malveillants. En 2020, une telle violation de grande envergure a été réalisée à l'aide d'une combinaison d'ingénierie sociale et d'hameçonnage pour contourner une solution MFA. Elle aurait pu être évitée en utilisant des clés de sécurité physiques.

# Risque minimal

MFA FIDO2 via une clé de sécurité physique


La norme FIDO2 est la méthode d'authentification basée sur les normes la plus forte du secteur et résout les vulnérabilités de sécurité des MFA traditionnelles, éliminant ainsi les risques d'attaques d'hameçonnage, de réplication et MITM. La norme FIDO2 associe la spécification Web Authentication du World Wide Web Consortium et le protocole client-authentifiant (Client to Authenticator Protocol) correspondant de la FIDO Alliance. Ce modèle d'authentification ouvre la voie à l'avenir de la MFA : l'authentification via des identifiants de connexion cryptographiques qui ne quittent jamais le terminal de l'utilisateur et ne sont jamais stockés sur un serveur. FIDO2 prend également en charge l'évolution éventuelle vers une authentification sans mot de passe.

L'inconvénient est que la seule façon d'activer la MFA FIDO2 est d'acheter des clés de sécurité physiques pour tous les utilisateurs, afin qu'ils les utilisent comme facteur d'authentification.

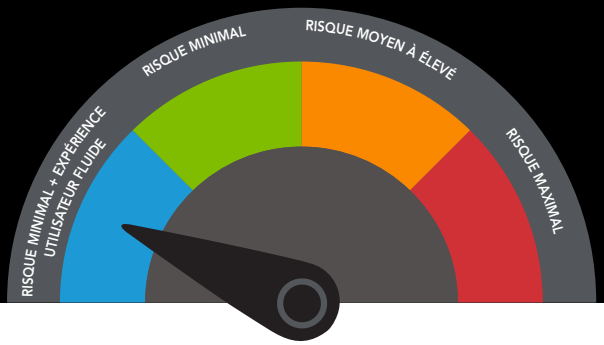
Bien que FIDO2 soit la norme la plus sécurisée, la mise en œuvre via des clés de sécurité matérielles peut présenter de nombreux défis :

- **Coût d'achat et de maintenance des clés pour chaque utilisateur**
- **Complexité de la distribution et de la gestion des clés**
- **Remplacement des clés matérielles perdues**
- **Impossibilité de mettre à jour ou de corriger les clés matérielles**
- **Répartition inégale : seuls certains employés ont accès aux clés**

L'achat, la configuration, la distribution et la gestion de clés matérielles physiques pour tous les employés sont des étapes coûteuses et chronophages. En outre, le fait d'exiger des utilisateurs qu'ils branchent une clé physique sur leur terminal à chaque connexion diminue la productivité en rendant l'expérience utilisateur fastidieuse.

# Risque minimal + Expérience utilisateur fluide

MFA nouvelle génération en bordure de l'Internet




MFA d'Akamai est une solution FIDO2 nouvelle génération dotée d'un facteur d'authentification anti-hameçonnage, sécurisé par le chiffrement. Le service utilise une application pour smartphone à la place d'une clé de sécurité physique, éliminant ainsi les problèmes qui empêchent fréquemment les entreprises de mettre en œuvre la technologie de MFA FIDO2. La solution peut être déployée rapidement et facilement à l'aide d'un smartphone existant, offrant le plus haut niveau de sécurité d'authentification avec une expérience utilisateur fluide. MFA d'Akamai élimine le risque d'hameçonnage et prend en charge l'évolution éventuelle vers une authentification sans mot de passe.

Pour en savoir plus sur MFA d'Akamai et commencer une période d'essai gratuite de 60 jours, cliquez ici : **akamai.com/mfa**.

## Sources :


1. https://www.infosecurity-magazine.com/blogs/pwned-passwords-business-risk/
2. https://haveibeenpwned.com/Passwords


Akamai sécurise et diffuse des expériences digitales pour les plus grandes entreprises du monde entier. L'Intelligent Edge Platform d'Akamai englobe tout, de l'entreprise au cloud, afin d'offrir rapidité, agilité et sécurité à ses clients et à leurs entreprises. Les plus grandes marques mondiales comptent sur Akamai pour les aider à concrétiser leur avantage concurrentiel à travers des solutions agiles qui augmentent la puissance de leurs architectures multiclouds. Akamai place les décisions, les applications et les expériences au plus près des utilisateurs, et au plus loin des attaques et des menaces. Les solutions de sécurité en bordure de l'Internet, de performances Web et sur mobile, d'accès professionnel et de diffusion vidéo du portefeuille d'Akamai s'appuient également sur un service client exceptionnel, des analyses et une surveillance 24 h/24 et 7 j/7, 365 jours par an. Pour savoir pourquoi les plus grandes marques internationales font confiance à Akamai, visitez www.akamai.com, blogs.akamai.com ou @Akamai sur Twitter. Vous trouverez nos coordonnées dans le monde entier à l'adresse www.akamai.com/locations. Publication : 03/21.