okta

GUIDE DE DÉPLOIEMENT DE L'AUTHENTIFICATION MULTIFACTEUR

Okta France
Paris

paris@okta.com
01 85 64 08 80

Introduction

La sécurité des mots de passe s'est fragilisée ces dernières années. En réaction, l'authentification multifacteur (MFA) gagne en popularité, car il s'agit d'une méthode efficace pour renforcer la fiabilité de l'authentification au niveau des applications web et mobiles, professionnelles et grand public.

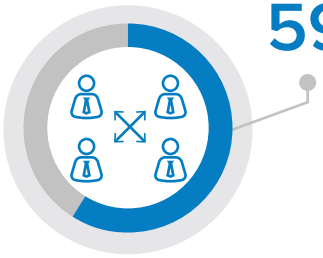
Pour que l'authentification s'opère, il faut généralement valider l'un des trois types de facteurs suivants : un élément que vous connaissez (par ex. un mot de passe), que vous possédez (par ex. une carte d'identité) ou qui vous caractérise (par ex. une empreinte digitale). L'authentification multifacteur (MFA, Multi-Factor Authentication) utilise au minimum deux types de facteurs. Souvent, les solutions web et mobiles associent un mot de passe et un jeton à durée limitée détenu par l'utilisateur, mais globalement les modalités d'implémentation de l'authentification MFA sont très variées.

Ce guide explique pourquoi l'utilisation d'une solution d'authentification multifacteur (MFA) est un choix logique et présente les bonnes pratiques de déploiement dans ce domaine. Il propose également les résultats d'une enquête réalisée en partenariat avec IDG, qui montre les priorités de vos pairs et le rôle de la gestion des identités et des accès (IAM) dans les systèmes de sécurité et d'authentification forte. Il détaille ensuite les éléments à prendre en compte avant de déployer une solution MFA, notamment les politiques et les besoins en matière d'accès. Enfin, ce guide fournit des conseils pratiques à ceux qui développent une solution d'authentification multifacteur pour leurs applications, sur la base de notre expérience et en collaboration avec des ingénieurs et des équipes produits.

Utiliser l'IAM et le MFA à l'âge d'or des cyberattaques

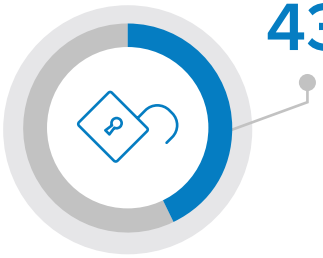
Les menaces se multiplient : malwares, piratage, phishing, social engineering... Ces tactiques se soldent souvent par le piratage de comptes et le vol d'identifiants.

Principaux problèmes de sécurité liés à l'identité



59%

Extension de la base utilisateurs à des personnes externes à l'entreprise

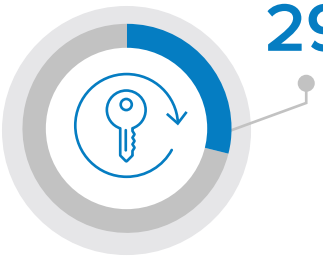


43%

Contrôles d'authentification peu pratiques, ignorés ou contournés

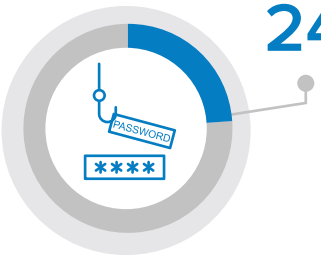
33%

Absence de politiques IAM



29%

Réutilisation des mêmes mots de passe

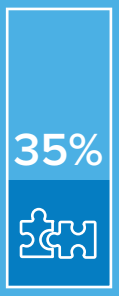


24%

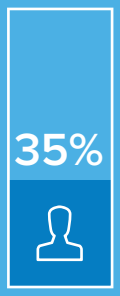
Vol d'identifiants

Les grands défis de la gestion des identités et des accès

Gestion des identités et des accès dans plusieurs environnements applicatifs



Intégration avec les solutions de sécurité en place (50 % dans les grandes entreprises)



Collecte d'informations et rapports sur les modèles d'accès des utilisateurs

Anticiper l'avenir - Priorité de l'IAM et évaluation des fonctionnalités IAM actuelles :

92 % Gestion des identités et des accès dans plusieurs environnements applicatifs → **77 %** des managers

30 %
indiquent une bonne ou meilleure capacité à détecter l'utilisation illégitime d'identifiants

45 %
intègrent les données IAM dans leur SOC (Security Operations Center)

Faire face aux problèmes de sécurité : principaux avantages potentiels des solutions IAM

Authentification dans tous les services et applications, permettant d'élargir la base utilisateurs en toute sécurité	**53 %**
Automatisation du provisioning/ déprovisioning	**45 %**
Amélioration de l'expérience utilisateur avec des contrôles utilisateurs moins contraignants	**43 %**
Adoption de contrôles d'accès plus stricts	**43 %**

Consultez le site d'Okta pour en savoir plus sur l'IAM et le MFA

* Enquête IDG

7 éléments à prendre en compte avant d'adopter l'authentification multifacteur (MFA)

Les mots de passe sont complexes à mettre en œuvre. Leurs critères de création de plus en plus stricts sont censés les rendre plus sûrs, mais dans bien des cas, ils produisent l'effet inverse. Les mots de passe qui respectent toutes les exigences de sécurité sont difficiles à mémoriser, et souvent réutilisés d'un site à l'autre. Les utilisateurs les griffonnent sur des Post-it. Ils emploient des noms d'animaux de compagnie, des dates de naissance ou des numéros de téléphone familiers, tous faciles à deviner. Bref, en matière de protection de données, nous sommes loin de la panacée. Heureusement, certaines entreprises commencent à prendre conscience du danger, mais aussi à adhérer au principe selon lequel les accès doivent être dissuasifs pour les pirates et simples pour les utilisateurs autorisés. La meilleure solution consiste à opter pour l'authentification multifacteur, ou MFA (Multi-Factor Authentication).

L'authentification MFA est un excellent moyen de protéger les applications et services de vos utilisateurs finaux contre tout accès non autorisé. Voici quelques points à prendre en considération si vous envisagez de l'adopter.

1. Sensibiliser les utilisateurs

Vous déployez l'authentification multifacteur pour réduire les risques que présentent les accès reposant sur un simple mot de passe, mais certains utilisateurs pourraient trouver cette nouvelle méthode fastidieuse et craindre que ce changement leur fasse perdre un temps précieux.

Veillez donc à ce que tous les collaborateurs, du management aux utilisateurs finaux, comprennent bien les raisons de cette transition vers l'authentification multifacteur. Il est important d'obtenir l'adhésion de toute l'entreprise afin que chacun contribue activement à sa sécurité. Menez des actions de sensibilisation auprès des utilisateurs pour les aider à cerner les avantages de cette étape supplémentaire.

2. Définir les politiques MFA

Afin de ne pas alourdir le coût d'un déploiement MFA, il est recommandé de concilier sécurité et ergonomie. Vos politiques MFA doivent donc décrire quand et comment appliquer un facteur supplémentaire.

Bien que cela puisse sembler paradoxal, il est parfois judicieux d'appliquer l'authentification renforcée avec parcimonie plutôt qu'à tout-va. Pour être efficaces, les politiques axées sur les risques ne doivent déclencher une authentification renforcée qu'en cas de nécessité.

On peut par exemple imaginer une politique qui exige un deuxième facteur uniquement en cas de connexion à un service en dehors du réseau de l'entreprise (sur la base d'une série d'adresses IP) ou en dehors du pays (sur la base de données de géolocalisation). De même, il est envisageable d'appliquer une politique plus stricte à un groupe d'utilisateurs ayant accès à des données sensibles. L'authentification MFA vous permet d'exiger un deuxième facteur pour accéder aux ressources sensibles, mais pas pour consulter le calendrier des événements de l'entreprise. L'idée est de rendre cette vérification supplémentaire la plus transparente possible afin de garantir une expérience utilisateur satisfaisante, sans compromettre la sécurité.

3. S'adapter aux différentes demandes d'accès

Il arrive qu'un utilisateur dispose d'un accès à Internet mais que sa couverture mobile soit faible, voire inexistante. C'est parfois le cas à bord d'un avion proposant le Wi-Fi, dans une habitation en zone rurale, ou tout simplement au sous-sol d'un grand bâtiment en béton. Dans ces situations où les services vocaux et SMS ne sont pas disponibles, Okta Verify avec envoi de notifications push ou génération de mots de passe à usage unique (OTP) constitue une alternative intéressante, le chiffrement des communications s'opérant sur la connexion Internet du téléphone.

Les dispositifs physiques qui génèrent des mots de passe à usage unique à durée limitée (TOTP) ou basés sur des événements ne nécessitent aucun canal de communication. Ils sont aussi plus difficiles à pirater ou à copier. Mais au-delà du coût de déploiement, ces terminaux constituent une contrainte supplémentaire pour les utilisateurs, qui peuvent les oublier chez eux ou même les perdre.

Cette solution n'est donc pas forcément judicieuse pour les sous-traitants à court terme et les entreprises à forte rotation d'effectifs.

En ce qui concerne les facteurs MFA, un grand nombre de possibilités s'offrent à vous pour couvrir une multitude de scénarios. Optez pour une configuration adaptée à votre entreprise, tout en sachant que, s'il n'existe pas de solution standard (il y en a rarement), l'application de plusieurs politiques et facteurs est le meilleur moyen de gérer toutes les situations.

4. Peser le pour et le contre de l'envoi de mots de passe à usage unique par SMS

Les SMS sont très pratiques et, avec la multiplication des téléphones mobiles et tablettes, ils sont devenus un moyen de communication courant, notamment pour l'envoi de mots de passe à usage unique. S'ils sont généralement considérés comme suffisamment sécurisés dans ce cas de figure, c'est en partie dû au fait que l'infrastructure sous-jacente est à la fois propriétaire et opaque.

Des études montrent cependant que la sécurité des SMS est fait défaut, et pas seulement dans le cas des vulnérabilités documentées. En y ayant recours, vous faites confiance aux bonnes pratiques de sécurité des opérateurs de télécommunications, mais le risque de compromissions par usurpation d'identité ou social engineering subsiste. Bien souvent, il n'est pas très compliqué pour un pirate de transférer votre numéro sur un terminal qu'il contrôle, et d'accéder ainsi à vos SMS et mots de passe à usage unique.

Si la CNIL déconseille d'utiliser les SMS pour ces raisons précises, il vous incombe néanmoins d'évaluer votre exposition aux risques en fonction de vos utilisateurs, de vos cas d'usage et des données à protéger. Après tout, l'authentification multifacteur par SMS n'est pas parfaite, mais elle vaut mieux que son absence totale.

5. Étudier attentivement les exigences de conformité

La plupart des normes de conformité IT telles que PCI DSS, SOX et HIPAA exigent des contrôles d'authentification stricts, ce qui peut justifier un déploiement MFA. Cela peut paraître évident, mais si vous voulez vous conformer à ces normes, vous devez en cerner toutes les exigences afin de pouvoir adapter votre configuration et vos politiques en conséquence.

Par exemple, les normes PCI et HIPAA nécessitent une authentification forte, avec application d'au moins deux des trois facteurs suivants : un facteur de connaissance, un facteur de possession et un facteur de biométrie. La norme SOX est moins centrée sur la technologie, mais en cas d'audit, vous devez prouver que les données financières et comptables de votre entreprise sont sécurisées.

La conformité IT nécessite de mettre en œuvre les normes pertinentes, mais aussi de prouver que leurs principes sont respectés. Documentez vos configurations et implémentations afin de pouvoir démontrer rapidement et avec assurance que toutes les conditions sont remplies.

Vous vous en féliciterez plus tard, et votre entreprise vous en sera reconnaissante.

6. Prévoir les mesures à prendre en cas de perte d'un terminal

Dans le cadre d'un déploiement MFA classique, le deuxième facteur d'authentification est un « facteur de possession » (le premier étant un « facteur de connaissance » et le troisième un « facteur de biométrie »). Dans le cas d'un SMS, d'un message vocal ou d'une application d'authentification comme Okta Verify ou Google Authenticator, l'utilisateur se sert de son téléphone. Et dans le cas d'un jeton physique de type YubiKey ou RSA, il est en possession du dispositif en question. Or, tout ce qui est en sa possession peut être égaré.

Votre support IT doit donc être assorti d'une procédure de gestion des terminaux perdus. Pensez à inclure les appareils utilisés pour le MFA, et veillez à ce que la perte d'un équipement entraîne :

- **l'expiration des sessions en cours et un demande de réauthentification de l'utilisateur ;**
- **la dissociation de l'équipement du compte utilisateur et des droits d'accès correspondants ;**
- **la suppression à distance des informations de l'entreprise sur les terminaux mobiles, si nécessaire.**

Il est également important d'auditer les activités du compte utilisateur avant la perte du terminal, afin de détecter toute activité inhabituelle. En cas d'événement suspect, recherchez les éventuelles brèches et faites-les remonter, le cas échéant.

Une fois les premières mesures de sécurité prises, donnez à l'utilisateur les moyens de se remettre au travail, en lui fournissant un terminal de remplacement ou une autre méthode de connexion. Un appel au service d'assistance IT pour vérifier son identité peut, par exemple, lui permettre de rester productif en attendant l'implémentation des facteurs de remplacement.

7. Se préparer à réexaminer et réviser la configuration

Rares sont les politiques et déploiements complexes qui conviennent parfaitement d'emblée. Sachant qu'un changement de processus peut potentiellement impacter tous les collaborateurs, il est conseillé d'évaluer l'efficacité d'une solution MFA déployée et utilisée, pour ensuite affiner les règles suivant les observations effectuées.

Familiarisez-vous en amont du processus avec la fonctionnalité d'audit, qui vous sera très utile pour résoudre les problèmes de configuration et ajuster les politiques comme il convient. Une fois votre MFA déployé, faites appel à des outils d'audit pour vérifier ponctuellement le taux d'adoption et l'usage. Il peut également être judicieux de donner la possibilité aux utilisateurs de soumettre des commentaires.

Et si les utilisateurs ne prennent pas toujours le temps de rédiger un feedback écrit, une trace d'audit vous offrira une certaine visibilité sur leur expérience. Ont-ils dû s'y reprendre à trois fois pour saisir leur mot de passe à usage unique ? Ont-ils abandonné ? Ces difficultés peuvent être liées à une mauvaise configuration, à un manque de formation, ou tout simplement à un scénario qui n'avait pas été envisagé dans le plan de déploiement initial.

Utiliser des outils d'audit et encourager les collaborateurs à donner leur avis est le meilleur moyen d'assurer à toutes les parties prenantes que le système fonctionne comme prévu et que les nouvelles politiques de sécurité sont bien adoptées.

L'authentification multifacteur adaptative, un plus pour l'entreprise

Ces conseils constituent un excellent point de départ, et si l'authentification MFA renforcée peut vous permettre de contrôler précisément quand et comment appliquer l'authentification multifacteur, sa configuration exige toutefois mûre réflexion. Même avec des politiques et critères bien définis, il se peut que vous souhaitiez prendre des décisions sur le moment même, en fonction des changements de contextes liés à l'utilisateur ou au terminal.

Si vous souhaitez effectuer des changements dynamiques, testez la solution Okta Adaptive MFA, qui identifie les modèles d'accès, puis adapte la politique à chaque utilisateur ou groupe.

Ainsi, un deuxième facteur d'authentification peut être demandé périodiquement aux collaborateurs qui se déplacent et consultent régulièrement leurs e-mails depuis l'étranger, et systématiquement à ceux qui, en temps normal, ne se déplacent jamais. Les politiques axées sur les risques peuvent également s'appliquer en cas d'événement suspect. Citons par exemple l'activation de l'authentification forte lors de tentatives d'accès à des ressources via un proxy non autorisé, ou encore le blocage automatique des adresses IP malveillantes connues.

Okta Adaptive MFA est une solution efficace pour définir automatiquement des politiques dynamiques au fil du temps. Concrètement, elle offre à votre entreprise le niveau de sécurité exigé et la flexibilité nécessaire pour traiter les utilisateurs de manière individuelle.

Trois bonnes pratiques pour les ingénieurs et les chefs de produit

Introduction

Les publications expliquant comment concevoir une solution d'authentification sécurisée pour les systèmes informatiques ne manquent pas. Nous proposons ici des conseils pratiques, inspirés par notre expérience de collaboration avec des ingénieurs et des équipes produits, et destinés à ceux qui développent une solution d'authentification multifacteur pour leurs applications. Voici trois moyens de renforcer la sécurité d'une solution d'authentification MFA :

- **Déterminer et gérer la vulnérabilité du processus de récupération de comptes**
- **Protéger les flux de connexion des attaques par force brute**
- **Concilier gestion des risques, ergonomie et coût**

Nous partons ici du principe que le mot de passe a été compromis et qu'un deuxième facteur est nécessaire.

Déterminer et gérer la vulnérabilité du processus de récupération de comptes

L'authentification multifacteur n'est sécurisée que si ses flux de récupération de comptes le sont également. Dans de nombreux cas récents ultra-médiatisés, les pirates avaient su exploiter les vulnérabilités du processus de récupération pour prendre le contrôle d'un compte.

Prenons l'exemple de l'application web d'une entreprise qui intégrerait un dispositif d'authentification multifacteur basé sur un jeton logiciel installé sur le smartphone d'un utilisateur. Supposons que l'application permette à ce dernier d'enregistrer un numéro de téléphone pour recevoir un deuxième facteur de secours afin de récupérer son compte s'il ne parvient pas à accéder à son jeton logiciel. Dans ce cas, l'efficacité du deuxième facteur dépend du niveau de sécurité des processus utilisés par l'opérateur de télécommunications pour authentifier l'abonné et lui transmettre des appels ou des SMS. Un pirate parviendrait-il à usurper l'identité de l'utilisateur et à convaincre ou contraindre un chargé de clientèle de transférer les appels ou les SMS vers un numéro qu'il contrôle ?

Chaque deuxième facteur exige une méthode de remplacement. La question est donc de savoir comment mettre au point des flux de récupération sécurisés. Voici quelques conseils pour y parvenir, sachant que l'approche peut varier selon les circonstances :

- Indépendance des facteurs principaux et secondaires. Dissociez la récupération du deuxième facteur de celle du premier. Si un pirate a accès au premier facteur d'authentification, le deuxième devient inefficace s'il peut être réinitialisé sur simple saisie du mot de passe. En outre, le flux de récupération du deuxième facteur doit être totalement distinct de celui du mot de passe. Par exemple, si la récupération du mot de passe s'effectue par e-mail, veillez à récupérer le deuxième facteur par un autre canal.
- Faites intervenir un administrateur. Dans bien des cas, un administrateur est parfaitement capable de mettre en place une méthode d'authentification sophistiquée offrant des garanties élevées.

Dans les scénarios d'entreprise, les sociétés qui utilisent des secrets partagés issus des travaux ou du profil des collaborateurs, de l'organisation elle-même ou des relations humaines sont mieux armées pour authentifier leurs propres effectifs. L'approche consistant à demander au responsable d'un collaborateur d'authentifier cet utilisateur avant d'autoriser l'équipe IT à réinitialiser les identifiants MFA est particulièrement intéressante.

Dans les cas d'usage grand public, un administrateur peut interroger un utilisateur sur un grand nombre de secrets partagés. Par exemple, lors de l'onboarding, les applications bancaires réservées aux particuliers collectent diverses informations personnelles peu connues, qui deviennent des secrets partagés destinés à la récupération des comptes. Par ailleurs, les récents événements figurant dans l'historique de la personne avec l'application ou la société sont autant de secrets partagés possibles. L'évaluation d'un ensemble de secrets partagés peut être automatisée en ligne ou par voie vocale, ce qui offre la plupart du temps de meilleures garanties qu'un être humain, plus exposé au social engineering.

- Prévoyez un deuxième facteur de secours. De nombreuses situations exigent une méthode automatisée de récupération du deuxième facteur. C'est notamment le cas des produits desservant un grand nombre d'utilisateurs et dont l'assistance individuelle est hors de prix, ou lorsqu'il est nécessaire de réduire les coûts d'exploitation. En adhérant à plusieurs facteurs secondaires lors de l'onboarding, l'utilisateur peut récupérer un deuxième facteur en s'identifiant au moyen d'un second facteur de secours. Fournir aux utilisateurs une carte (physique ou imprimable) contenant une série de codes à usage unique pouvant servir de deuxième facteur de secours est une pratique judicieuse, simple et économique.

Protéger les flux de connexion des attaques par force brute

Plus les ressources informatiques bon marché se multiplient, plus les systèmes d'authentification sont exposés aux attaques par force brute. Plusieurs techniques simples permettent toutefois d'améliorer sensiblement la sécurité de l'authentification multifacteur en cas de piratage du mot de passe :

- Séquence de flux de connexion, limitation du débit et blocage de comptes. Placer la demande de deuxième facteur sur une page située en dessous de la page de connexion offre deux avantages. Premièrement, l'utilisateur est protégé contre les attaques destinées à bloquer son compte une fois le nombre maximal d'échecs de connexion atteint (sous réserve qu'une limitation du débit soit appliquée pour le premier facteur). Deuxièmement, dans la mesure où le deuxième facteur est dissimulé, le pirate a moins de visibilité sur une autre couche de sécurité. Instaurez une limitation du débit et une règle de blocage pour le deuxième facteur. Comme il est peu probable qu'un utilisateur se trompe plusieurs fois en entrant son jeton, la suspicion d'attaque doit se renforcer à chaque tentative ratée. Les temps de réponse doivent augmenter à chaque tentative afin de réduire le nombre maximal d'essais possibles par unité de temps, avec un verrouillage complet du compte (si possible) après plusieurs échecs successifs. Pour les facteurs secondaires à durée limitée, adaptez la limitation du débit à la durée de vie du jeton.
- Journaux et alertes. Collectez et analysez les tentatives de deuxième facteur ayant échoué. En cas d'échec de plusieurs demandes de deuxième facteur, alertez l'utilisateur ou un administrateur de ce comportement suspect, et invitez l'utilisateur à obtenir un nouveau jeton.
- Utilisez un jeton hors bande. Un deuxième facteur vérifié via un canal autre que celui du premier facteur est un gage de protection supplémentaire contre les attaques par force

brute (et par phishing). Ainsi, la tendance actuelle consiste à envoyer sur le smartphone de l'utilisateur une notification push contenant des détails sur la demande d'authentification et l'invitant à accepter ou refuser cette demande. Ce canal est inaccessible pour les attaques par force brute classiques.

Concilier gestion des risques, ergonomie et coût

Quel que soit le contexte, la conception d'une fonctionnalité d'authentification multifacteur a des répercussions importantes sur la sécurité, l'ergonomie et le coût. Un deuxième facteur offrant de meilleures garanties peut dans certains cas alourdir la tâche des utilisateurs et des administrateurs, ce qui freine l'adoption du MFA et réduit d'autant la sécurité. Voici quelques bonnes pratiques à mettre en œuvre pour trouver le juste équilibre entre gestion des risques, ergonomie et coût :

- Offrez des options adaptées à différentes populations d'utilisateurs. Les risques varient en fonction des populations d'utilisateurs et exigent par conséquent des niveaux de garantie différents. Par exemple, un administrateur peut avoir un périmètre d'accès plus large que celui d'un utilisateur lambda. Vous pouvez donc prévoir des facteurs secondaires relativement plus forts pour les administrateurs, et offrir des options plus pratiques aux utilisateurs. Dans les cas d'usage grand public, les préférences varient d'un utilisateur à l'autre, et une option offrant de faibles garanties, mais pratique et donc facilement adoptée, peut se révéler plus sûre qu'une option offrant une assurance maximale, mais boudée par les utilisateurs.
- Optez pour l'authentification fédérée. Dans les scénarios d'entreprise, de nombreuses sociétés mettent en place des systèmes d'authentification unique et multifacteur en local pour les identités dont elles assurent la gestion, et les fédèrent avec les ressources. Cette approche permet aux équipes de développement de produits de confier l'administration des politiques et des processus de sécurité aux clients. Les clients peuvent ainsi implémenter l'authentification MFA de manière autonome, ce qui leur permet d'optimiser les points précédents en fonction de leurs contextes et contraintes spécifiques. Un client peut par exemple adapter l'administration de la récupération de comptes à ses activités IT. Cette approche externalisée présente un autre avantage : elle permet aux utilisateurs d'accéder à la totalité des ressources avec un seul et même jeton.

Conclusion

Roadmap pour une authentification MFA efficace

En résumé, l'authentification multifacteur est une excellente méthode, qui permet aux développeurs d'applications de renforcer la sécurité d'accès à leurs solutions. Certaines conditions doivent être remplies pour sécuriser une fonctionnalité MFA, parmi lesquelles l'analyse du flux de récupération du deuxième facteur, la protection contre les attaques par force brute et l'équilibre entre sécurité, ergonomie et coût.

Une approche automatisée et moderne de l'authentification multifacteur aide à prendre le contrôle des identifiants pour réduire sensiblement le risque de brèche. Mais par quoi les entreprises doivent-elles commencer ?

Nous vous conseillons de vous concentrer sur quelques étapes clés :

1. Éliminer les mots de passe chaque fois que c'est possible
2. Utiliser des mots de passe forts et uniques dans les autres cas
3. Sécuriser les flux de récupération de comptes avec des facteurs principaux et secondaires indépendants
4. Optimiser la sécurité des applications stratégiques grâce à l'authentification forte

5. Adopter une stratégie unifiée pour les applications on-premise, cloud et mobiles
6. Automatiser le provisioning avec une définition précise des droits
7. Opter pour le déprovisioning à l'échelle de toute l'entreprise et améliorer la visibilité et le reporting
8. Générer en temps réel des alertes et des rapports centralisés sur tous les événements d'authentification
9. Intégrer la stratégie de gestion des identités avec les outils de sécurité en place
10. Étendre la gestion des identités et l'authentification multifacteur aux partenaires, fournisseurs et sous-traitants

Pourquoi choisir Okta pour l'authentification MFA ?

Grâce à son approche innovante de la gestion des identités, Okta est le mieux placé pour aider les entreprises à gérer les identités et l'authentification multifacteur afin de limiter les brèches. Avec la solution d'authentification multifacteur d'Okta, vous pouvez :

Généraliser l'utilisation de fonctions d'authentification MFA forte

- Déployer rapidement et facilement l'authentification MFA avec les 6 500 préintégrations d'Okta Integration Network
- Étendre la couverture aux applications on-premise grâce à la prise en charge des protocoles RADIUS, RDP, ADFS et LDAP
- Mettre en place des politiques d'accès intelligentes et contextualisées en fonction des attributs de connexion et des terminaux

Néanmoins, l'authentification forte n'est pas une protection absolue contre les brèches. Avec Okta, vous pouvez facilement :

Centraliser la gestion des identités

- Simplifier la gestion des comptes
- Unifier l'accès pour offrir aux utilisateurs un accès simplifié sans mot de passe
- Réduire les risques et la prolifération des identités en limitant l'accès aux services via des connexions SAML

Réduire la surface d'attaque

- Le provisioning et le déprovisioning automatisés accélèrent l'onboarding tout en éliminant les comptes orphelins
- La solution peut être étendue aux applications "maison" via le protocole SCIM, un kit SDK et l'API d'Okta
- La gestion complète du cycle de vie des utilisateurs garantit un niveau d'accès adapté aux applications appropriées grâce à des workflows de demande d'accès

Réagir plus rapidement aux tentatives de piratage

- Obtenir une vue centralisée de toutes les données d'authentification des applications cloud, mobiles et on-premise
- Repérer les comportements inhabituels et suspects
- Enrichir et étoffer votre environnement de cybersécurité via l'API SysLog Okta (Splunk, ArcSight, IBM QRadar, Palo Alto Networks, F5 Networks)

Pour découvrir à quel point il est facile d'administrer la solution Okta d'authentification Adaptive (AMFA) et de piloter le processus d'authentification, visionnez cette démo.

À propos d'Okta

Okta est un éditeur indépendant spécialisé dans la gestion et la protection des données d'identification, leader du secteur. La plateforme Okta Identity Cloud connecte et protège les collaborateurs des plus grandes entreprises au monde, en plus d'assurer une connexion sécurisée avec leurs partenaires, fournisseurs et clients. Grâce à son intégration avancée à plus de 6 500 applications, Okta Identity Cloud permet à n'importe quel utilisateur de se connecter facilement et en toute sécurité, tous terminaux confondus. Des milliers de clients, dont 20th Century Fox, Adobe, Dish Networks, Experian, Flex, LinkedIn et News Corp, font confiance à Okta pour améliorer leur productivité, doper leur chiffre d'affaires et préserver leur sécurité. Grâce à Okta, ils peuvent accéder facilement et sans risque aux technologies dont ils ont besoin pour accomplir leurs missions stratégiques.

Pour en savoir plus, consultez le site www.okta.com/fr ou suivez-nous sur www.okta.com/blog.