Livre blanc

Guide de déploiement de l'authentification multifacteur

Janvier 2023

Sommaire

Introduction : Comment renforcer les défenses face à des brèches qui prennent de l'ampleur

Les cyberattaques sophistiquées ne cessent d'augmenter et les attaques basées sur les identifiants y sont pour beaucoup. D'après un rapport récent, les attaques e-mail ciblant les entreprises ont enregistré une hausse de 48 % au cours du premier semestre 2022. Par rapport au semestre précédent, plus de deux tiers de ces attaques étaient des tentatives de phishing d'identifiants (e-mail contenant un lien malveillant conçu pour voler des informations de comptes sensibles). Lors de ces attaques, 265 marques ont vu leur identité usurpée.

Le passage au télétravail a incité les cybercriminels à multiplier les tactiques d'ingénierie sociale comme le phishing et à exploiter les brèches de données pour prendre le contrôle de comptes vulnérables. En conséquence, l'authentification multifacteur (MFA) a gagné en popularité, car il s'agit d'une méthode efficace pour renforcer la fiabilité de l'authentification des utilisateurs. Le MFA permet aux entreprises de sécuriser l'accès à toutes leurs ressources, dont les applications web et mobiles grand public/professionnelles, dans un monde toujours plus dispersé et hybride. Les pouvoirs publics, les organismes de réglementation et les entreprises ont pris conscience du rôle crucial joué par le MFA dans la mise en place d'une sécurité Zero Trust dernier cri (sur le principe « ne jamais faire confiance, toujours vérifier »).

Aujourd'hui, l'authentification multifacteur est devenue un aspect clé de toute bonne stratégie de sécurité axée sur l'identité. Ainsi, en janvier 2022, un décret a été adopté par l'OMB (Office of Management and Budget) des États-Unis. Il stipule qu'une authentification multifacteur résistante au phishing est désormais une condition indispensable à la modernisation de la cybersécurité au sein des agences fédérales américaines.

Avec l'évolution des pouvoirs publics, des entreprises et des cybercriminels, la nature de l'authentification multifacteur change aussi, ce qui explique l'essor de l'authentification sans mot de passe (passwordless) et l'importance accrue des terminaux, gérés et non gérés, dans l'évaluation du niveau de sécurité.

Ce guide a pour but de vous expliquer les bonnes pratiques à respecter pour tirer pleinement parti des promesses de l'authentification multifacteur, y compris la mise à niveau vers l'authentification sans mot de passe. Nous y examinerons les résultats d'une enquête réalisée en partenariat avec IDG qui démontre le rôle majeur joué par la gestion des identités et des accès (IAM, Identity and Access Management) dans une stratégie de sécurité et d'authentification moderne, et présente les priorités et tendances d'adoption de vos pairs. Ce guide nous donnera également l'occasion d'aider les entreprises à comprendre les principaux éléments à prendre en compte lors de la conception d'une solution MFA, par exemple :

- Implémentation d'une protection de pointe contre le phishing
- Compréhension des politiques et des réglementations
- Examen de l'évolution des besoins en matière d'accès

Sur la base des observations notées lors de notre collaboration avec les équipes produits et ingénierie, nous conclurons par quelques conseils pratiques à l'intention des entreprises qui développent une solution MFA pour leurs applications.

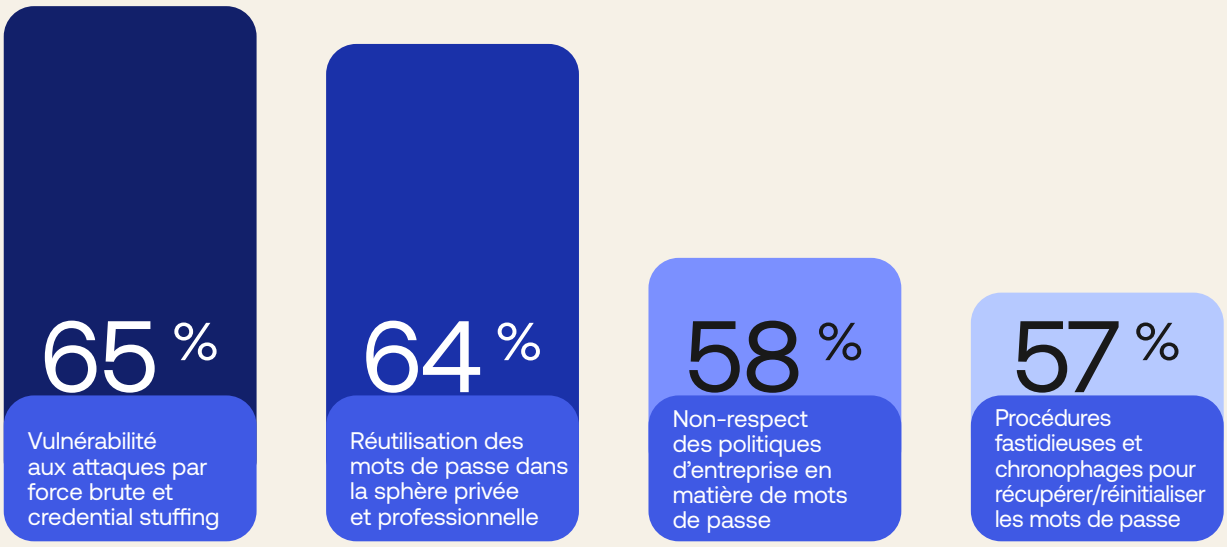
Déploiement d'un MFA résistant au phishing dans le cadre d'une stratégie IAM efficace

Aujourd'hui, les menaces axées sur l'identité revêtent de nombreuses formes, par exemple les malwares, le piratage et le phishing. Celles-ci ont de nombreuses répercussions en aval, notamment le vol d'identifiants, la compromission de comptes et l'exfiltration de données. Pour prévenir ces menaces courantes, les entreprises doivent renforcer leur niveau de sécurité, et la première ligne de défense est l'identité. Les entreprises s'en remettent toujours aux anciennes approches de gestion des identités, comme les applications et les pare-feux on-premise, ce qui les rend malheureusement très vulnérables aux attaques sophistiquées. Fondamentalement, elles s'appuient sur un dispositif lent, complexe et fragmenté pour protéger leur entreprise et leurs collaborateurs.

Analysons plus en détail ces chiffres et ce qu'ils signifient : l'enquête menée en collaboration avec IDG révèle certains chiffres et problèmes spécifiques identifiés par des responsables IT et sécurité concernant l'authentification sécurisée.

Principaux problèmes liés aux mots de passe

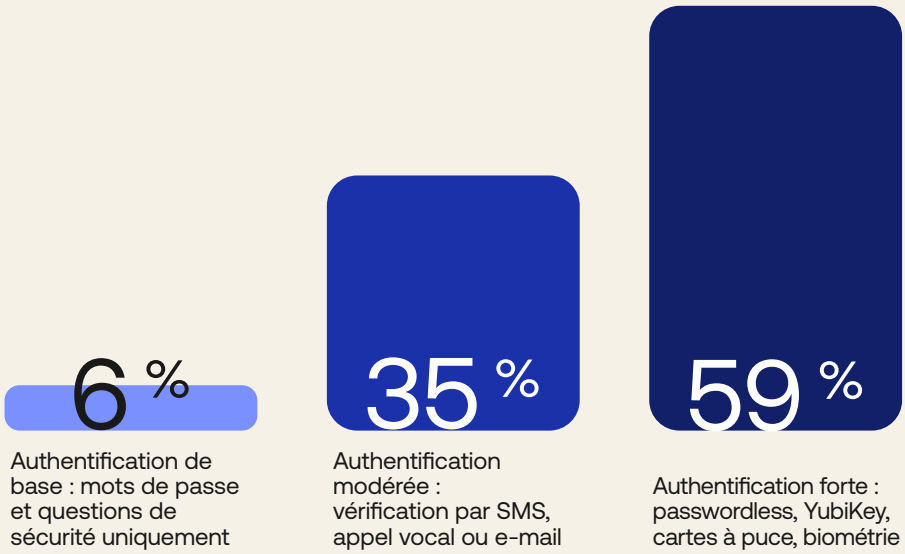
Plus de 1 000 employés	**70 %**
500-999 employés	**52 %**



Observation : les répondants citent plusieurs problèmes liés aux mots de passe, dont le vol des identifiants et l'utilisation des mêmes mots de passe pour les comptes professionnels et privés.

Niveau MFA le plus logique pour l'entreprise

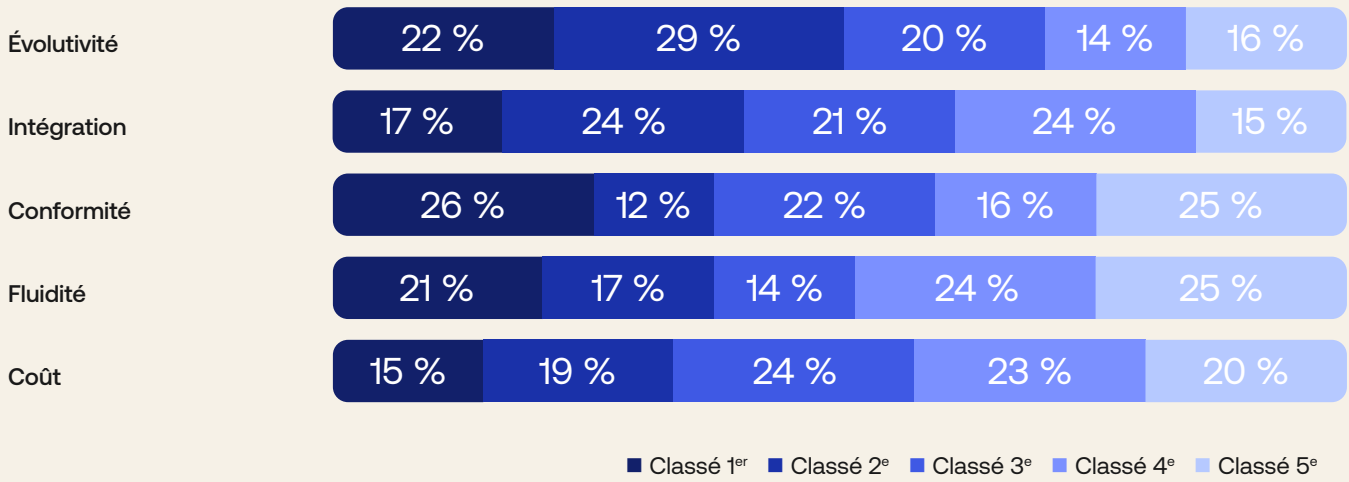
VP IT et échelons supérieurs	**73 %**
Responsable ou directeur-trice IT	**53 %**



Observation : plus de la moitié (59 %) déclarent que la solution MFA la plus forte possible est la plus appropriée pour leur entreprise

Importance des critères lors du choix d'une solution MFA

Les entreprises ont dû classer les cinq critères par ordre décroissant : du plus important au moins important.



Observation : 51 % classent l'évolutivité parmi les deux principaux facteurs à prendre en compte lors du choix d'une solution MFA.

Analyse du niveau d'assurance offert par les différents facteurs d'authentification

En règle générale, un système d'authentification valide l'identité à l'aide de l'un des trois types de facteurs ci-dessous :

- Une information que vous connaissez (mot de passe)
- Un élément que vous possédez (carte à puce PIV)
- Une caractéristique qui vous est propre (empreinte digitale)

Pour encore renforcer la sécurité, le MFA emploie au moins deux types de facteurs, voire plus. Si l'option la plus courante reste le mot de passe associé à un jeton à durée limitée, à une notification push vers une application mobile ou à un facteur biométrique, il existe différentes approches en matière d'authentification multifacteur. Chacune d'elles possède ses avantages et ses inconvénients.

Divers types d'authentificateurs sont disponibles, chacun étant associé à un degré de force qui lui est propre. Okta classe les authentificateurs selon les niveaux d'assurance suivants :

FAIBLE : mots de passe ; questions de sécurité ; mots de passe à usage unique (OTP) via SMS, appel vocal ou e-mail ; et applications OTP comme Authy et Google Authenticator

MOYEN : notifications push vers une application mobile et mots de passe à usage unique via un jeton matériel

ÉLEVÉ : cartes à puce PIV (Personal Identity Verification) ou CAC (Common Access Card), FIDO 2.0 / WebAuthn + CTAP2

Bien entendu, le niveau d'assurance n'est pas le seul critère pris en compte par les organisations qui cherchent à renforcer leur authentification multifacteur. Les authentificateurs doivent également être faciles à déployer et à utiliser par les collaborateurs et les clients. En outre, ils doivent être capables de résister à des menaces spécifiques, par exemple, les attaques Man-in-the-Middle (MitM) ou Adversary-in-the-Middle (AitM). Quoi qu'il en soit, pour renforcer la sécurité, rien ne peut remplacer les facteurs d'assurance les plus élevés.

Ainsi, si vous optez pour un facteur comme le SMS, les utilisateurs seront rapidement opérationnels, mais le niveau d'assurance n'est pas très élevé. Certaines menaces de sécurité courantes, par exemple le piratage des cartes SIM ainsi que les attaques de smishing et vishing de grande envergure, compromettent le niveau d'assurance que l'authentification par SMS peut offrir. C'est pourquoi nous recommandons vivement d'utiliser des facteurs MFA plus forts, par exemple Okta Verify Push ou la biométrie (via WebAuthn ou, dans le cas des agences gouvernementales américaines, des cartes à puce PIV/CAC).

Bonnes pratiques pour la conception d'une authentification multifacteur forte

1. Évaluer régulièrement la pertinence de ses politiques MFA

Avant de déployer une solution MFA, vous devez évaluer les risques de sécurité et les menaces spécifiques auxquels votre organisation est exposée. Quels ressources et vecteurs d'attaque vous préoccupent-ils le plus ? Des politiques bien pensées et basées sur le risque doivent déclencher des demandes d'authentification renforcée lorsque le risque est particulièrement élevé.

Par exemple, une politique pourrait exiger un second facteur toutes les 8 heures lors d'une connexion à partir d'un réseau connu, ou uniquement exiger ce second facteur en cas de connexion depuis un nouveau terminal ou emplacement géographique. De même, il est envisageable d'appliquer une politique plus stricte à un groupe d'utilisateurs ayant accès à des données sensibles — par exemple, des développeurs ou des cadres supérieurs ayant respectivement accès au code source ou à des données sensibles. Vous pouvez exiger un type de facteur plus fort ou leur demander de répondre à des invites MFA supplémentaires. Vous pouvez même envisager d'implémenter l'authentification multifacteur pour certaines actions sensibles au sein des applications. En implémentant des contrôles plus granulaires pour les opérations jugées extrêmement sensibles (par exemple l'approbation des bons de commande ou le transfert de fonds), vous pouvez d'une part réduire le risque et d'autre part, mettre en place une sécurité qui satisfait les exigences liées à une conformité continue.

En fin de compte, toute vérification supplémentaire doit être aussi transparente et fluide que possible. Elle doit favoriser une bonne expérience utilisateur sans sacrifier la sécurité.

2. Prévoir et s'adapter à différentes demandes d'accès

Pour les utilisateurs disposant d'un accès à Internet mais d'une couverture mobile faible, voire inexistante — comme 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 bâtiment en béton —, une authentification par SMS ou appel vocal ne sera pas une option viable. Dans de tels scénarios, Okta Verify avec notifications push ou un mot de passe à usage unique (OTP) constitue une meilleure alternative, le chiffrement des communications s'opérant alors sur la connexion Internet du téléphone. Les dispositifs matériels qui génèrent des mots de passe à usage unique à durée limitée (TOTP) ou basés sur des événements ne nécessitent aucun canal de communication et sont plus difficiles à pirater ou à copier. Toutefois, outre qu'ils peuvent être coûteux à déployer, ces objets constituent une contrainte supplémentaire pour les utilisateurs, qui peuvent les oublier chez eux ou même les perdre. C'est la raison pour laquelle ce type de facteurs n'est pas forcément la meilleure option pour les prestataires à court terme et les entreprises à forte rotation d'effectifs.

Les organisations doivent choisir des facteurs MFA capables de prendre en charge un large éventail de scénarios. Il est rare en effet qu'une solution universelle puisse être adaptée à toutes les situations. De manière générale, les conseils de déploiement suivants permettent de renforcer la sécurité et d'offrir une expérience utilisateur optimale :

- Proposez aux utilisateurs un choix entre plusieurs facteurs afin qu'ils aient toujours une solution de secours. Si l'un des facteurs d'authentification est un mot de passe, faites en sorte que la fonction Breached Password Detection avertisse l'utilisateur et bloque son utilisation en cas de compromission.
- Activez uniquement des types de facteurs forts et antiphishing et passez à l'authentification multifacteur sans mot de passe ou aux cartes à puce PIV/CAC pour organismes gouvernementaux chaque fois que possible.
- Vérifiez l'origine de l'URL web avant l'authentification. Les identifiants doivent être liés au domaine d'où émane la demande d'accès.
- Si votre matériel est compatible, autorisez les utilisateurs à utiliser la biométrie comme deuxième facteur (par exemple Windows Hello et Touch ID). Cela simplifie l'expérience de l'utilisateur final et renforce la fiabilité de l'authentification des utilisateurs.

3. Pour les applications sensibles, appliquer des authentificateurs résistants au phishing à niveau d'assurance élevé dans le cadre des politiques MFA

Comme nous l'avons mentionné précédemment, les authentificateurs ne résistent pas tous au phishing. Ils offrent des degrés divers de résistance au social engineering, dès lors qu'ils représentent un certain coût et risque pour les cybercriminels cherchant à prendre le contrôle d'un compte. Ainsi, les mots de passe à usage unique envoyés par SMS peuvent être interceptés relativement facilement. En revanche, l'authentification push résiste mieux aux campagnes de phishing d'identifiants statiques que les authentificateurs s'appuyant sur un mot de passe à usage unique.

Combiner les notifications push et une demande d'authentification à l'aide d'un nombre — qui invite l'utilisateur vérifiant une demande push d'identifier un nombre présenté sur la page de connexion — offre une résistance plus élevée à une série de techniques utilisées par les cyberadversaires, et notamment les attaques exploitant la lassitude liée au MFA. Ce sont les authentificateurs matériels qui offrent les plus hauts niveaux d'assurance.

La définition la plus fiable de la résistance au phishing est donnée par le NIST (National Institute of Standards and Technology). Selon cet organisme, la résistance au phishing exige que le canal en cours d'authentification soit lié de façon cryptographique au résultat généré par l'authentificateur. Plus simplement, cela signifie que le domaine (par exemple l'adresse) du site web auquel vous vous connectez est lié à votre authentificateur. Vous avez ainsi l'assurance que ce dernier ne fournira pas vos identifiants à une page web de phishing.

La plateforme Okta propose plusieurs authentificateurs correspondant à cette définition. Okta prend en charge les authentificateurs WebAuthn FIDO2 itinérants (par exemple les clés de sécurité) et ceux liés au terminal (comme Face ID, Touch ID ou Windows Hello). Okta prend également en charge l'authentification par carte à puce PIV dans les politiques de connexion d'une application pour accéder à certaines applications spécifiques. Selon votre modèle de déploiement, FastPass (l'authentificateur sans mot de passe lié au terminal d'Okta) correspond aussi à cette définition. Imposer l'utilisation d'au moins un authentificateur à l'épreuve du phishing élimine le risque d'attaques de phishing sophistiquées via des attaques de social engineering et AitM.

4. 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 justifie certainement un déploiement MFA. 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 méthodes d'authentification forte sur trois. La norme SOX est moins centrée sur la technologie et plus sur la réussite d'un 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 qu'elles ont été respectées. Documentez soigneusement votre processus de configuration et d'implémentation afin de pouvoir apporter la preuve de votre conformité en cas d'audit. Vous vous en féliciterez plus tard, et votre entreprise vous en sera reconnaissante.

5. Modéliser l'authentification multifacteur pour sécuriser des effectifs hybrides en constante augmentation

Compte tenu de la popularité croissante du travail à distance ou hybride des collaborateurs et des prestataires, il est indispensable de renforcer la sécurité lors de l'accès aux ressources du cloud. Idéalement, l'onboarding des nouveaux collaborateurs doit avoir lieu dans les bureaux, où les collaborateurs en place sont en contact direct avec le service IT. Mais le télétravail pose de nouveaux défis au déploiement du MFA et au dépannage.

Pour accélérer ce déploiement, il est préférable d'activer des facteurs qui permettent aux utilisateurs d'être rapidement opérationnels (par exemple la biométrie intégrée aux terminaux ou des authentificateurs d'applications mobiles comme Okta Verify) et ne les obligent pas à attendre de recevoir un jeton matériel. Ils sont ainsi en mesure d'accéder rapidement aux ressources dont ils ont besoin pour travailler. Pour l'onboarding à distance des nouvelles recrues, certaines organisations organisent désormais des sessions d'onboarding virtuelles et envoient des instructions de configuration à l'adresse e-mail personnelle des collaborateurs, afin de les mettre au courant avant même qu'ils aient accès à leur adresse e-mail professionnelle.

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

Dans les environnements de travail ayant adopté une politique BYOD (Bring Your Own Device), on note une augmentation marquée du nombre de collaborateurs utilisant un terminal personnel pour accéder aux ressources d'entreprise. Toutefois, la présence de terminaux non gérés s'accompagne de plusieurs défis de taille. Parmi les sociétés acceptant le BYOD, nombreuses sont celles qui subissent des brèches de données via les terminaux de leurs collaborateurs, d'où le besoin impérieux d'une sécurité renforcée pour ce vecteur de menaces.

Les politiques Device Assurance vous permettent de vérifier toute une série d'attributs du terminal en rapport avec la sécurité dans le cadre de vos politiques d'authentification, par exemple la version du système d'exploitation, le chiffrement de disque, la détection du débridage ou d'un accès root. De cette façon, les politiques Device Assurance ajoutent une couche de sécurité supplémentaire aux règles de votre politique d'authentification pour valider le niveau de sécurité du terminal utilisé.

Un autre élément à prendre en considération est le fait que les collaborateurs téléchargent régulièrement des données d'entreprise sur leur ordinateur de bureau ou portable. Il est donc important d'exiger qu'ils répondent à une demande d'authentification après avoir saisi un mot de passe pour déverrouiller leur ordinateur. La plupart des directives de conformité imposent l'utilisation de l'authentification multifacteur. L'implémenter au niveau de l'ordinateur réduit le risque d'attaque de ce dernier et protège les données en cas de perte ou de vol d'un ordinateur portable.

Quoi qu'il en soit, tout ce qui est en possession de l'utilisateur 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 à prendre les mesures suivantes en cas de perte d'un terminal :

- Fermeture des sessions en cours et demande de réauthentification de l'utilisateur
- Dissociation du terminal du compte utilisateur et des droits d'accès correspondants
- Suppression à distance des informations de l'entreprise sur les terminaux mobiles (ce qui est souvent prévu sur les terminaux fournis par l'entreprise)

Il est également important d'effectuer un audit des activités du compte utilisateur qui ont eu lieu 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 de support IT pour vérifier son identité peut, par exemple, lui permettre de rester productif pendant l'implémentation des facteurs de remplacement.

7. Prévoir l'implémentation de l'authentification multifacteur adaptative

Si l'authentification multifacteur renforcée peut vous permettre de contrôler précisément quand et comment appliquer le MFA, sa configuration exige toutefois mûre réflexion. Même avec des politiques et critères bien définis, il se peut que vous souhaitiez prendre des décisions d'accès dynamiques en fonction des changements de contexte liés à l'utilisateur ou au terminal.

Le MFA adaptatif peut s'avérer utile dans de tels cas puisqu'il identifie les modèles d'accès récurrents, 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 ne se déplacent jamais en temps normal. Les politiques axées sur les risques peuvent également s'appliquer en cas d'événement suspect. Citons par exemple l'activation de l'authentification renforcée lors de tentatives d'accès à des ressources via un proxy non autorisé, ou encore le blocage automatique des adresses IP malveillantes connues. L'authentification multifacteur adaptative 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 souplesse nécessaire pour traiter les utilisateurs de manière individuelle.

8. Déployer graduellement votre MFA

Rares sont les politiques et déploiements complexes qui fonctionnent parfaitement d'emblée. Sachant qu'un changement de processus peut potentiellement impacter tous les collaborateurs, il est conseillé d'évaluer son efficacité au fur et à mesure de son déploiement, pour ensuite affiner les politiques selon les résultats. Le déploiement doit être graduel. L'utilisation de l'authentification multifacteur doit être limitée dans un premier temps à l'équipe IT et/ou sécurité avant d'étendre son utilisation à d'autres groupes d'utilisateurs. Familiarisez-vous dès que possible avec la fonctionnalité d'audit, qui vous sera très utile pour résoudre les problèmes de configuration et ajuster les politiques par la suite.

Par exemple, une fois le MFA mis en place pour un groupe spécifique d'utilisateurs, faites appel à des outils d'audit pour contrôler ponctuellement son adoption et son utilisation. Il peut également être intéressant de mettre en place un mécanisme de retour utilisateur. Même si les utilisateurs ne prennent pas toujours le temps d'envoyer des commentaires, une piste d'audit peut vous donner certaines informations utiles 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 problèmes peuvent être liés 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 de donner à toutes les parties prenantes l'assurance que le système fonctionne comme prévu et que les nouvelles politiques de sécurité sont bien adoptées.

9. Proposer des formations aux utilisateurs

Déployer le MFA pour réduire les risques que présentent les accès reposant sur un simple mot de passe est devenu une pratique de sécurité incontournable dans un monde toujours plus numérique. Certains utilisateurs peuvent toutefois trouver cette nouvelle méthode fastidieuse et craindre que ce changement leur fasse perdre un temps précieux dans une journée de travail déjà bien remplie. Il est donc essentiel de veiller à ce que tous les collaborateurs — équipe de direction, équipes IT ou encore utilisateurs finaux — comprennent bien les raisons de cette transition vers l'authentification multifacteur. Obtenir l'adhésion de toute l'organisation garantit que chacun accepte et comprend son rôle dans le maintien de la sécurité de l'entreprise. Une formation peut aider les utilisateurs à prendre conscience des avantages offerts par ces mesures de sécurité supplémentaires.

Plusieurs approches sont envisageables. Par exemple, le service IT peut envoyer des e-mails annonçant les changements à venir ou encore organiser des exercices de simulation de phishing pour démontrer que même les collaborateurs les plus avertis peuvent être amenés à divulguer leurs identifiants. Pensez à inclure des captures d'écran, des FAQ et des informations de contact pour que les collaborateurs sachent à qui s'adresser en cas de problème.

Évaluation de la vulnérabilité du processus de récupération de comptes

L'authentification multifacteur n'est sécurisée que si le processus de récupération de comptes l'est également. Dans de nombreuses affaires récentes relayées par les médias, les pirates ont réussi à 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 MFA 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 pour récupérer son compte s'il ne parvient pas à accéder à son jeton logiciel. Dans un tel 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 un chargé de clientèle de transférer les appels ou les SMS vers un numéro qu'il contrôle ?

Comme chaque deuxième facteur nécessite une méthode de remplacement fiable, les organisations doivent concevoir des processus de récupération sécurisés. Vous pouvez privilégier différentes approches selon les circonstances, mais pensez toutefois à respecter les bonnes pratiques suivantes :

Les processus de récupération du facteur principal et secondaire doivent être indépendants.
Il est capital de dissocier la récupération du deuxième facteur de celle du premier. Sans quoi, si un cybercriminel a accès au premier facteur d'authentification, vous ne pouvez pas compter sur le second puisqu'il pourrait être réinitialisé avec le mot de passe compromis. Le processus de récupération du deuxième facteur doit être totalement indépendant de celui du mot de passe. Par exemple, si vous utilisez un e-mail pour récupérer le premier facteur, employez un autre canal pour le facteur secondaire.

Sollicitez l'aide d'un administrateur.
Un administrateur peut implémenter une méthode d'authentification à niveau d'assurance élevé dans divers scénarios. 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 très coûteuse, 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.

Protection des flux de connexion contre les attaques par force brute et credential stuffing

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 compromission d'un mot de passe.

Analysez les journaux et les alertes.
Collectez et analysez les tentatives de demande 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 téléphone mobile 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 dans le cas d'attaques par force brute classiques.

Conception qui concilie gestion des risques, ergonomie et maîtrise des coûts

Quel que soit le contexte, la conception d'une fonctionnalité MFA a des répercussions importantes sur la sécurité, l'ergonomie et le coût. Un deuxième facteur à niveau d'assurance plus élevé peut dans certains cas compliquer inutilement la tâche des utilisateurs et des administrateurs, ce qui freine l'adoption du MFA pour votre produit 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 différents groupes d'utilisateurs.
Les risques varient en fonction des groupes d'utilisateurs et exigent par conséquent des niveaux d'assurance 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 plus forts pour les administrateurs, et offrir des options plus pratiques aux utilisateurs normaux. Dans les scénarios grand public, les préférences varieront d'un utilisateur à l'autre, selon le compromis recherché entre sécurité et ergonomie. Une option plus familière avec un niveau d'assurance moins élevé, telle que le SMS, peut se révéler plus sûre qu'une option à niveau d'assurance élevé peu adoptée.

Optez pour l'authentification et les identités fédérées.
L'identité fédérée, également appelée authentification unique (SSO) fédérée, est une méthode qui consiste à lier l'identité d'un utilisateur dans différents systèmes de gestion des identités, ce qui lui permet de basculer rapidement d'un système à l'autre tout en préservant sa sécurité. Dans les scénarios d'entreprise, de nombreuses sociétés mettent en place un système d'authentification et un MFA 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 et partenaires. Ces utilisateurs peuvent ainsi implémenter l'authentification MFA de manière autonome, ce qui leur permet d'optimiser les points précédents en fonction de leur contexte et de leurs contraintes spécifiques. Un partenaire 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.

Okta change la donne

Grâce à son approche innovante de la gestion des identités, Okta est idéalement placé pour aider les entreprises à prendre le contrôle de la gestion des identités, dont le MFA, et réduire ainsi les brèches de données et d'autres répercussions négatives. Okta vous offre les avantages suivants :

Activation rapide de l'authentification multifacteur pour vos collaborateurs et vos clients

- Déployez rapidement et facilement le MFA avec plus de 7 000 connecteurs prêts à l'emploi dans le réseau d'applications d'Okta.
- Étendez la couverture aux applications on-premise grâce à la prise en charge des protocoles RADIUS, RDP, ADFS et LDAP, ainsi qu'à l'authentification basée sur l'en-tête et Kerberos via Okta Access Gateway.
- Mettez en place des politiques d'accès intelligentes et contextualisées en fonction des attributs de connexion et des terminaux.
- Limitez la dépendance vis-à-vis des mots de passe avec l'authentification unique (SSO) et sans mot de passe (passwordless).

Centralisation des identités en toute sécurité

- Simplifiez la gestion des comptes.
- Unifiez l'accès pour offrir aux utilisateurs un accès simplifié sans mot de passe et une expérience de meilleure qualité.
- Réduisez les risques et la prolifération des identités en limitant l'accès aux services via des connexions SAML intelligentes.

Réduction de la surface d'attaque et réponse rapide en cas de compromission des mots de passe

- Automatisez le provisioning et le déprovisioning pour accélérer l'onboarding tout en éliminant les comptes orphelins.
- Étendez les politiques de sécurité aux applications personnalisées via le protocole SCIM, les kits SDK et les API très complètes d'Okta.
- Fournissez le niveau d'accès approprié aux applications nécessaires au moment opportun grâce à des workflows de demande d'accès et à une gestion complète du cycle de vie des identités.

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

Pour en savoir plus sur les solutions Okta Adaptive MFA, consultez la page suivante : https://www.okta.com/fr/products/adaptive-multi-factor-authentication/

Conclusion : Roadmap pour réussir son parcours MFA

L'authentification multifacteur est devenue une bonne pratique largement adoptée par les développeurs pour sécuriser l'accès à leurs applications. Toutefois, en arrière-plan, vous devez prendre de nombreuses mesures pour tirer le meilleur parti de la sécurité MFA sans perturber le travail de vos collaborateurs. Les bonnes pratiques à respecter consistent, entre autres, à analyser le processus de récupération du deuxième facteur, à concevoir des systèmes capables de résister aux attaques par force brute et à trouver le meilleur compromis entre sécurité, ergonomie et coût.

Une approche automatisée et moderne du MFA peut aider les entreprises à contrôler l'accès, à automatiser la récupération en toute sécurité et à réduire considérablement le risque de brèches de données.

Livre blanc

Guide de déploiement de l'authentification multifacteur

okta

Okta France
Tour Europlaza
20 avenue André Prothin
92400 Courbevoie - France
+33 01 85 64 08 80