LIVRE BLANC

Authentification Multifacteur pour IBM i

Introduction

Les mécanismes standards de protection par des mots de passe, utilisés pendant des années, ne suffisent plus. Les failles de sécurité causées par des mots de passe devinés, ou conservés dans des endroits non sécurisés (ex. : notés sur des Post-It) ou par des attaques en force, ont obligé les services informatiques à mettre en place une gestion des mots de passe renforcée et mieux contrôlée. Les pressions réglementaires, les bonnes pratiques et la peur de subir de nouvelles attaques ont conduit les entreprises à adopter les procédures de l'Authentification Multifacteur (MFA-Multi-factor authentication en anglais). Les utilisateurs doivent saisir une information en plus du mot de passe, en particulier lors de l'accès à des systèmes contenant des données sensibles ou de grande valeur.

Conformité à la Réglementation et incitation à l'Authentification Multifacteur

Les réglementations de mise en conformité, en forte augmentation, impactant aujourd'hui les activités telles que le commerce, les banques, les établissements financiers, la santé, et autres industries, imposent ou recommandent vivement de mettre en œuvre la MFA. Parmi ces réglementations, on peut citer :

- **PCI DSS** – « Payment Card Industry Data Security Standard » est un standard de sécurité des données pour les entreprises détenant des informations sur les cartes de crédit. PCI DSS 3.2 exige de tous les utilisateurs se connectant à distance au CDE (cardholder data environment, ou environnement de données des cartes bancaires) d'être sécurisés par la MFA, y compris les administrateurs et les fournisseurs externes.
  La MFA était, dans le passé, demandée uniquement pour les accès à distance au CDE. La nouvelle exigence indique à présent que tout accès administratif via des réseaux internes doit également être validé par la méthode MFA. Au sein de certaines entreprises, ceci peut concerner un grand nombre de personnes. En effet, dans un environnement IBM i, il est courant de constater que plusieurs profils utilisateurs détiennent des droits d'administrateur, *SECADM ou *ALLOBJ, et accèdent au CDE.

- **23 NYCRR 500** – Un grand nombre d'établissements financiers et d'assurance ont l'obligation de répondre aux exigences définies par les State of New York Department of Financial Services dans leur réglementation de cybersécurité portant sur les entreprises fournissant des services financiers au sein de cet État. Le règlement s'applique aux institutions qui exercent des activités à New York, peu importe où leur siège social se situe. La section 500.12(b) de cette réglementation stipule : « L'authentification Multifacteur doit être utilisée par toute personne ayant accès aux réseaux internes de l'organisme, depuis un réseau externe ; à moins que, le RSSI de cette entité ait approuvé par écrit l'utilisation similaire de contrôles d'accès sécurisés. »
- **FFIEC** – Le Federal Financial Institutions Examination Council (FFIEC) fournit des directives concernant l'utilisation de la MFA dans un environnement de banque en ligne, avec des attentes minimums pour l'authentification de transactions en ligne à « haut risque » impliquant l'accès du client à des informations critiques et/ou aux mouvements des avoirs. Plus précisément, il stipule : « En tant que seul mécanisme de contrôle, l'authentification à facteur unique est considérée comme inadaptée dans le cas de transactions à risque élevé impliquant l'accès aux informations du client ou à des mouvements de fonds vers d'autres destinataires. »
- **Autres réglementations** – Il existe d'autres réglementations de conformité qui mentionnent ou évoquent les bénéfices de la MFA, telles que, HIPAA, Swift Alliance Access, RGPD, SOX, GLBA, etc.

Pour le moment, votre entreprise n'est peut-être pas poussée par les réglementations de conformité à implémenter la MFA, mais il y a fort à parier que ce soit le cas dans un avenir proche. Même en l'absence d'exigences légales, les meilleures pratiques en termes de sécurité vous recommandent vivement d'intégrer cette technologie pour mieux protéger vos données sensibles contre les accès non autorisés. Compte tenu des coûts et des perturbations considérables engendrés par une faille, il s'agit là d'une précaution judicieuse.

Fonctionnement de l'authentification Multifacteur

La MFA demande à l'utilisateur de s'authentifier avec au moins deux informations bien différentes (en sus du nom de l'utilisateur) qui prouveraient son identité. Pour qu'elles soient recevables par la MFA, ces preuves doivent appartenir à deux des trois catégories suivantes, également appelées facteurs d'authentification :

- Quelque chose que l'utilisateur connaît (p. ex. : mot de passe, PIN, phrase secrète)
- Quelque chose que l'utilisateur possède (p. ex. : compte de messagerie, smartphone, appareil générateur de codes)
- Quelque chose d'inhérent à l'utilisateur (p. ex. : empreinte digitale, scan de l'iris, reconnaissance vocale)

En demandant aux utilisateurs de fournir au moins deux facteurs d'authentification, la MFA réduit considérablement les chances qu'un cybercriminel accède au système. Effectivement, la probabilité est très faible qu'un pirate informatique puisse à la fois deviner/trouver/voler le mot de passe d'un utilisateur et obtenir l'utilisation du deuxième facteur d'authentification, exemple : le smartphone de l'utilisateur qui reçoit un code d'authentification.

Il est également important de souligner qu'une seconde utilisation du même facteur d'authentification ne constitue pas une MFA. En d'autres termes, si l'utilisateur fournit la réponse à une question de sécurité ou entre son code PIN une fois son mot de passe validé, cela revient à une authentification à un seul facteur, car il fournit deux formes de facteur d'authentification du même type: quelque chose qu'il connaît. Pour se conformer à la MFA, un utilisateur doit fournir deux ou plusieurs des différents facteurs d'authentification mentionnés ci-dessus ; exemple : quelque chose que l'utilisateur connaît (comme un mot de passe) et quelque chose que l'utilisateur possède (comme un mot de passe) et quelque chose qu'il possède (comme un code envoyé sur son smartphone).

Authentification Multifacteur et Authentification à deux facteurs : quelle est la différence ?

L'authentification à deux facteurs (2FA) est un terme souvent utilisé à la place de MFA. Différentes réglementations de conformité utilisent ce terme au lieu de MFA. Cependant, il existe bien une différence : 2FA désigne l'utilisation de deux facteurs d'authentification seulement, tandis que la MFA renvoie à l'emploi de deux facteurs d'authentification ou plus.

Authentification en une étape vs Authentification en plusieurs étapes

Selon la configuration de la Solution MFA, celle-ci peut être paramétrée pour demander à l'utilisateur des facteurs d'authentification en une ou plusieurs étapes. L'authentification en une étape invite l'utilisateur à saisir tous les facteurs d'authentification sur un seul écran ou une seule fenêtre, puis valide généralement tous les facteurs en une seule fois. L'authentification en plusieurs étapes demande quant à elle un facteur d'authentification sur un écran/fenêtre (un mot de passe, par exemple) et, si ce dernier est accepté, l'utilisateur doit fournir le facteur d'authentification suivant sur un autre écran/une autre fenêtre.

Il existe différentes raisons qui motivent les entreprises à utiliser l'une ou l'autre de ces méthodes, mais l'authentification en plusieurs étapes est considérée comme étant moins sécurisée, car elle révèle que le premier facteur était correct si l'utilisateur se voit demander le facteur d'authentification suivant. L'authentification en une étape représente la méthode la plus sûre. En cas d'échec de la connexion, il n'est pas dévoilé à la personne qui se connecte, quel facteur d'authentification a échoué. En d'autres termes, aucune information utile n'est divulguée à un éventuel pirate informatique. C'est la raison pour laquelle de nombreuses entités considèrent que l'authentification en plusieurs étapes ne relève pas vraiment de la MFA. Aussi, la réglementation PCI DSS reconnait uniquement l'authentification à une étape comme étant une méthode valide MFA si elle est implémentée de manière à ce que l'utilisateur ne puisse pas voir la cause d'un échec.

Méthodes et facteurs d'authentification complémentaires

Penchons-nous de plus près sur les deux facteurs d'authentification et les méthodes utilisées au-delà du premier facteur d'identification (qui est généralement quelque chose que l'utilisateur connaît, comme un mot de passe).

Quelque chose que l'utilisateur possède

Via l'utilisation d'une ligne fixe, d'un smartphone, d'un e-mail ou d'un appareil spécial, un deuxième facteur d'authentification est, dans la plupart des cas, fourni sous la forme d'un code spécifique (parfois appelé token). Afin d'empêcher que les codes soient sauvegardés et réutilisés, ils sont normalement à usage unique et expirent s'ils ne sont pas utilisés dans un délai précis. Le code est habituellement généré par un système d'authentification distinct ou un service d'authentification tiers (retrouvez plus d'informations sur ces services dans la section suivante). Les méthodes d'envoi de code les plus courantes sont :

- **Application sur smartphone** – Il existe une variété d'applications d'authentification mobiles sur smartphone qui offrent une interface avec le système auquel on souhaite accéder, et qui génère des codes à usage unique.
- **E-mail** – Les codes sont envoyés à l'adresse électronique de l'utilisateur. Pour que cette méthode soit sécurisée, il est impératif que les utilisateurs possèdent un identifiant d'email différent de celui de l'IBM i.
- **Appel sur une ligne fixe ou sur un numéro de portable** – Les codes sont envoyés sous forme d'un message audio à un ou plusieurs numéros de téléphone désignés et attribué(s) à un utilisateur.

- **SMS** – Les codes sont envoyés par SMS à un numéro de téléphone portable désigné. Bien que cette méthode continue d'être une manière courante de fournir des codes, un certain nombre de piratages de grande ampleur, fortement médiatisés et impliquant ce procédé a poussé de nombreux organismes, y compris le National Institute of Standards and Technology (NIST), à déconseiller son utilisation.
- **Appareils générateurs de code** – Généralement présentés sous la forme d'un petit appareil pouvant être attaché à un porte-clés, ces dispositifs sont dotés d'un ensemble de fonctionnalités et de méthodes permettant de fournir des codes d'authentification. Certains d'entre eux ont un fonctionnement très simple et affichent un code sur un petit écran intégré à l'appareil, qui est ensuite saisi par l'utilisateur. La distribution de codes à l'aide d'un appareil de ce type est plus sécurisée qu'une transmission par téléphone, smartphone, application ou e-mail. Cependant, il s'agit d'un moyen qui peut être plus onéreux à déployer, et à l'instar des smartphones, ces appareils ne sont pas à l'abri de la perte ou du vol.

Quelque chose d'inhérent à l'utilisateur

Au sein de certaines organisations, le deuxième voire le troisième facteur d'authentification provient de quelque chose d'inhérent à l'utilisateur, comme une empreinte digitale, le scan de l'iris, la reconnaissance faciale, etc. Selon la méthode utilisée, le coût d'implémentation de ce facteur d'authentification peut être élevé, il est donc principalement utilisé par les organismes détenant des données particulièrement sensibles.

Services d'authentification

Le code spécial d'authentification généré pour l'utilisateur peut provenir de différentes sources, en fonction de la méthode d'authentification et du niveau de sécurité nécessaire. Voici quelques exemples de services tiers d'authentification s'intégrant aux solutions MFA IBM i :

- **RADIUS** – Génère des codes pour de multiples plateformes informatiques au sein d'une organisation via un serveur spécifique d'entreprise.
- **RSA SecurID** – Fournit des codes via un matériel ou un logiciel, ou sur demande via un smartphone. Génère un code à usage unique qui expire dans les 60 secondes. Cette solution peut, en option, être associée au code PIN d'un utilisateur.
- **Authy et Twilio** – S'installe sur un appareil mobile ou un navigateur, fournit à la demande des codes soumis à un délai et à usage unique. N'exige pas de connexion cellulaire, car il fonctionne via une application mobile autonome. Peut également fournir des codes à un téléphone mobile ou fixe.
- **TeleSign** – Fournit des codes d'authentification par voie mobile ou vocale.
- **YubiKey** – Fournit des codes à l'aide d'une clé USB.

Il convient de noter que certains logiciels de MFA offrent leurs propres outils générateurs de codes, mais ils sont généralement utilisés uniquement dans un environnement à faible risque.

La MFA est intégrée aux processus IBM i de différentes manières

Syncsort fait partie des éditeurs qui proposent des solutions MFA pour IBM i. Les départements informatiques choisissent souvent d'acheter et d'implémenter l'une de ces solutions afin de s'épargner le processus laborieux consistant à en développer une eux-mêmes. Que la solution MFA provienne d'un tiers ou qu'elle soit développée en interne, il est essentiel qu'elle offre une certaine flexibilité dans la manière avec laquelle la MFA est invoquée, car les utilisateurs accèdent au serveur IBM i à partir de différents endroits et processus.

Le plus souvent, la MFA est présentée aux utilisateurs à partir de l'écran de connexion 5250 qui apparaît lorsqu'ils se connectent à un système. Cependant, vous n'avez peut-être pas besoin de la MFA pour tous les utilisateurs ou dans toutes les situations. C'est la raison pour laquelle votre solution de MFA doit permettre soit de sélectionner des utilisateurs individuels ou des groupes d'utilisateurs qui ont besoin de la MFA, soit de définir des situations spécifiques dans lesquelles les utilisateurs nécessitent la MFA. Par ailleurs, votre solution doit aller encore plus loin en vous permettant de définir différentes règles lorsque la MFA est sollicitée. Par exemple, il peut être judicieux d'avoir la possibilité d'activer ou de désactiver la MFA en fonction de certaines autorisations, adresses IP, types d'appareils, date/heure, et d'un large éventail d'autres critères.

Votre solution doit également vous permettre d'intégrer la MFA à vos applications et processus IBM i, à un niveau granulaire. Dans certains cas, vous souhaiteriez peut-être utiliser la MFA lorsqu'un utilisateur accède à une application sensible, et/ou s'apprête à modifier des données sensibles. Pour les départements utilisant l'IBM i, il est également important d'être en mesure d'intégrer la MFA aux applications web.

Journaliser les activités de MFA

À l'instar d'autres opérations de sécurité IBM i pour lesquelles il est important de journaliser les activités, il est essentiel que votre application de MFA génère des informations exhaustives dans un journal. Un fichier sécurisé ou un journal (tel que QAUDJRN) est souvent utilisé pour fournir une trace d'audit qui ne peut être modifiée. Bien évidemment, si votre entreprise utilise une console SIEM pour capturer les événements de sécurité à l'échelle de l'entreprise, il vous faudra intégrer la journalisation de votre solution de MFA à votre solution SIEM.

Deux types d'événements à loguer : les modifications apportées à la configuration de l'application de MFA, et les échecs d'authentification MFA.

- **Loguer les configurations d'application de MFA** – Les audits au niveau objet et au niveau utilisateur doivent être mis en place. Toute modification apportée aux fonctions de configuration MFA sera enregistrée.
- **Loguer les échecs d'authentification MFA** — Non seulement les échecs d'authentification doivent être logués mais il est

important que les administrateurs et RSSI en soient alertés. Certaines solutions de MFA permettent de désactiver automatiquement les profils utilisateurs dans certains cas d'échec d'authentification.

Fonctions additionnelles qui intègrent la MFA

Certaines solutions de MFA fournissent des fonctionnalités supplémentaires pouvant être utilisées dans certaines situations :

- **Le principe des « quatre yeux » pour les modifications et opérations supervisées** – Pour les opérations qui présentent un risque important ou pour les modifications de données si sensibles qu'elles doivent être supervisées par une autre personne. Certaines offres de MFA permettent de mettre en place ce que l'on appelle la politique des « quatre yeux ». Voici son fonctionnement : lorsqu'un utilisateur souhaite effectuer un changement ou une opération sensible, un administrateur responsable reçoit un e-mail contenant un code à usage unique ainsi que les informations relatives à l'identité de l'utilisateur à l'origine de la requête. L'administrateur peut alors saisir le code directement sur l'écran de l'utilisateur et observer la modification ou l'opération en cours.
- **Réactivation de profil et changement de mots de passe en libre-service** – La technologie d'authentification multifacteur peut être utilisée pour aider les utilisateurs à réactiver leur profil ou à modifier un mot de passe oublié sans l'intervention de l'administrateur, permettant ainsi à ce dernier de se concentrer sur d'autres priorités. Exemple : un utilisateur peut répondre à des questions de sécurité préconfigurées et/ou recevoir un code à usage unique via une fenêtre pop-up, e-mail ou sur un appareil avant de modifier son profil.

Syncsort peut vous aider

La MFA est une technologie puissante qui protège efficacement les données sensibles ccontre les tentatives d'accès malveillantes externes comme internes. Il existe un grand nombre d'approches et de fonctionnalités à étudier pour choisir la solution de MFA la mieux adaptée à votre organisation. C'est pourquoi il est si important de travailler avec une entreprise de confiance qui vous fournira une solution de MFA personnalisable, qui fonctionnera parfaitement au sein de vos environnements IBM i, et accompagnée de prestations d'experts et d'un support réactif. Réunissant les meilleures solutions du marché, Syncsort propose des solutions complètes, de sécurité IBM i et services associés, y compris, des options puissantes de MFA couvrant une large gamme de service d'authentification. Confiez à nos experts de sécurité IBM i vos besoins en termes de MFA.

En savoir plus sur www.syncsort.com.

À propos de Syncsort

Syncsort est le leader mondial de solutions logicielles Big Iron to Big Data. Nous gérons les données partout, pour que le monde continue d'avancer. Ce sont ces mêmes données qui alimentent l'apprentissage automatique, l'IA et l'analyse prédictive.
Nous nous appuyons sur plusieurs décennies d'expérience pour permettre à plus de 7000 clients, dont 84 sociétés du classement Fortune 100, d'extraire rapidement de la valeur de leurs données critiques et ce, à tout moment et en tout lieu.
Nos produits offrent un moyen simple d'optimiser, de garantir, et d'intégrer les données. Ils sont ainsi prêts à répondre aux besoins actuels et futurs.

En savoir plus sur syncsort.com.

syncsort