Assure Multi-Factor Authentication

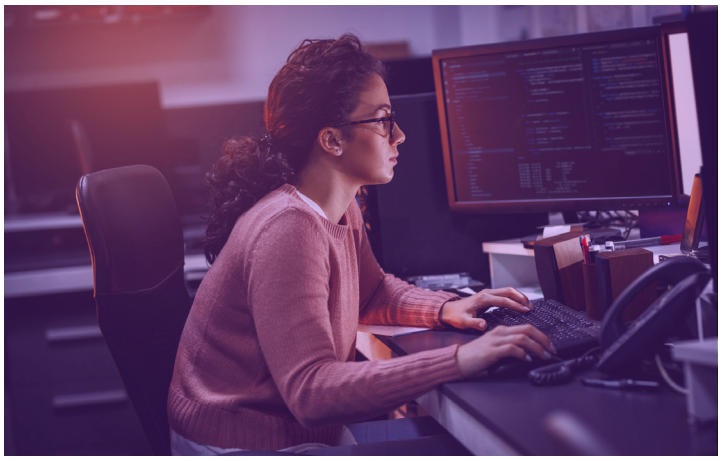
Renforcer la sécurité des mots de passe avec l'authentification multifacteur

Alors que les cas de vols ou corruptions de données dues à l'exploitation d'informations d'identification continuent de faire la une des journaux, il est évident que les mécanismes de protection par un simple mot de passe ne sont plus suffisants. Les organisations ont besoin d'une couche de protection supplémentaire qui soit également facile à utiliser et qui n'impose pas de charge supplémentaire aux administrateurs.

L'authentification multifacteur est devenue une méthode courante pour renforcer la sécurité, car elle exige qu'un utilisateur fournisse plus d'un facteur d'identification avant d'accéder à un système, à une application ou à ses données. Ces facteurs peuvent inclure quelque chose qu'il connaît (identifiant, mot de passe, code PIN), quelque chose qu'il possède (compte de messagerie, smartphone, dispositif à jeton) ou physique (empreinte digitale, balayage de l'iris).

Assure Multi-Factor Authentication, un module Assure Security, améliore la sécurité de votre système IBM i et des applications métiers de base. Avec Assure Multi-Factor Authentication vous pouvez :

- Ajouter une couche d'authentification
- Répondre aux exigences réglementaires et aux recommandations de PCI DSS 3.2, HIPAA, 23 NYCRR 500, Swift Alliance Access et autres.
- Lancer une authentification multifacteur basée sur des règles uniquement pour les utilisateurs ou les situations spécifiques qui le nécessitent.
- Réduire le risque d'accès non autorisé aux systèmes, aux applications et aux données
- Réduire le risque de vol de données et ses coûts et conséquences
- Conserver un historique des échecs de l'authentification multifacteur pour les alertes, les rapports ou l'intégration à une solution SIEM.
- L'utilisation d'Assure Multi-Factor Authentication peut être étendue pour prendre en charge le libre-service des mots de passe et le principe dit « des quatre yeux » des modifications supervisées des données sensibles.



Les mots de passe à eux seuls sont insuffisants. La fréquence des brèches dues à des mots de passe volés ou devinés et à des attaques informatiques par force brute nécessite un niveau supplémentaire de sécurité pour l'authentification des utilisateurs.

Authentification multifacteur puissante et flexible

L'authentification multifacteur d'Assure garantit une tranquillité sans faille en veillant à ce que seules les personnes autorisées aient accès à vos systèmes et à vos données sensibles, et offre la flexibilité nécessaire pour répondre aux besoins de votre environnement et de votre entreprise. L'authentification multifacteur peut être intégrée à l'écran de connexion de l'IBM i 5250 ou invoquée à la demande.

Lorsqu'elle est intégrée à l'écran de connexion, vous pouvez choisir entre une authentification en une ou deux étapes. L'authentification en une seule étape nécessite à la fois le mot de passe de l'utilisateur et un jeton pour l'authentification. L'utilisateur n'est pas informé de l'échec si l'un des deux est incorrect, ce qui permet une véritable authentification multifacteur. Avec le processus en deux étapes, un écran de jeton apparaît après l'ouverture de session IBM i.

Le moteur de règles d'Assure Multi-Factor Authentication permet de configurer facilement la solution pour qu'elle appelle les écrans d'authentification multifacteur uniquement pour les utilisateurs ou les situations spécifiques qui le nécessitent. Des critères de règles sont disponibles pour spécifier quels utilisateurs doivent s'authentifier via Assure Multi-Factor Authentication selon qu'ils soient :

- sont enregistrés ou non enregistrés
- sont des utilisateurs à capacité limitée
- sont membres de profils de groupes spécifiques
- possèdent des pouvoirs spéciaux
- utilisent un dispositif spécifique
- s'authentifient à partir d'un sous-système ou d'un iASP spécifique
- ont une adresse IP particulière
- s'authentifient à une certaine date ou heure.

Si Assure Multi-Factor Authentication est appelé à la demande, soit manuellement, soit dans un programme, le programme appelant peut également être spécifié comme critère. Des règles prédéfinies sont fournies pour vous aider à démarrer rapidement. Avec Assure Multi-Factor Authentication vous avez aussi le choix de la méthode d'authentification:

- **Authentificateur intégré** - Assure Multi-Factor Authentication dispose d'un service d'authentification intégré qui transmet un jeton par email et/ou par pop-up. Cette méthode est recommandée pour les environnements sensibles aux coûts.
- **Authentication compatible RADIUS** – Assure Multi-Factor Authentication contient un client RADIUS qui fonctionne nativement sur IBM i pour les organisations qui souhaitent utiliser un authentificateur basé sur RADIUS ou mis en place sur leur propre serveur RADIUS. Cela inclut des authentificateurs tels que les DUO Authenticator et Microsoft Azure Authenticator.
- **RSA SecurID®** – Assure Multi-Factor Authentication est certifiée par RSA comme étant conforme à SecureID pour servir les environnements les plus exigeants grâce à l'intégration avec les serveurs RSA RADIUS et les services RSA RADIUS en cloud. Les services en cloud RSA prennent en charge la biométrie, telle que l'empreinte digitale ou l'image faciale d'un téléphone portable, en plus des méthodes traditionnelles de jeton de messagerie vocale, de jeton SMS et d'approbation en mode « push ».

Les échecs d'authentification peuvent être enregistrés par Assure Multi-Factor Authentication à des fins de surveillance et de transmission facultative à un serveur SIEM.

Self-Service user re-enablement et changement de mot de passe Assure Multi-Factor

L'authentification à la demande Assure Multi-Factor peut également être utilisée pour permettre aux utilisateurs de réactiver leur profil ou de modifier leur mot de passe en cas d'oubli. S'ils sont configurés, les utilisateurs peuvent répondre à des questions de sécurité préconfigurées et/ou recevoir un jeton à usage unique via un pop-up, un email ou un dispositif RSA SecurID avant d'apporter des modifications à leur profil.

Le principe dit "des quatre yeux" pour les modifications supervisées de données sensibles

Pour les opérations pouvant avoir des impacts significatifs sur le serveur, ou pour des modifications de données si sensibles qu'elles doivent être supervisées par une deuxième paire d'yeux, Assure Multi-Factor Authentication peut être utilisé pour appliquer une politique dit « des quatre yeux ». Lorsqu'un utilisateur souhaite effectuer une telle modification ou opération, un administrateur désigné reçoit un email contenant un jeton à usage unique ainsi que des informations sur l'identité de l'utilisateur qui fait la demande et le numéro de poste. L'administrateur peut alors saisir le jeton à usage unique dans l'écran de l'utilisateur et observer la modification pendant qu'elle est effectuée.

Certification RSA

Visitez https://community.rsa.com/docs/DOC-92160 pour consulter le guide RSA SecurID Access Implementation pour Assure Multi-Factor Authentication.