**Livres blancs**

Host Access Management and Security Server (MSS)
Extension MSS Advanced Authentication

# Utilisation de l'authentification multi-critères pour autoriser l'accès au mainframe

MICRO FOCUS

# Les mots de passe sont inefficaces

L'utilisation de noms d'utilisateur et de mots de passe n'est plus une méthode d'authentification efficace. Pourquoi ? Parce que les utilisateurs ne font pas suffisamment attention à leurs mots de passe. Ils choisissent des mots de passe faciles à deviner. Ils utilisent toujours le même mot de passe. Et ils notent leurs mots de passe sur des bouts de papier que n'importe qui peut trouver.

## Mais le problème ne vient pas uniquement des utilisateurs

En vous contentant de noms d'utilisateur et de mots de passe, vous laissez pratiquement la porte ouverte aux pirates informatiques. Les cybercriminels les plus doués écrivent des algorithmes avancés pour trouver des moyens d'accès. Ensuite, quand le même mot de passe est utilisé pour plusieurs applications, les pirates qui ont réussi à le décoder peuvent accéder à tout ce qu'ils souhaitent. Par exemple, un pirate peut voler le mot de passe Facebook d'un utilisateur et parvenir ainsi à accéder à l'ensemble de votre infrastructure d'entreprise. C'est une perspective très effrayante.

Les noms d'utilisateur et les mots de passe sont des éléments que les utilisateurs doivent connaître et qui peuvent être relativement facilement capturés ou volés. Seuls, ils ne suffisent pas à garantir votre sécurité.

## Les anciens mots de passe de mainframe sont particulièrement vulnérables

Les problèmes que nous venons de décrire s'appliquent également aux mots de passe permettant d'accéder au mainframe. La différence est que les applications mainframe (celles sur lesquelles repose votre entreprise et qui contiennent vos données les plus sensibles) sont seulement protégées par des mots de passe à huit caractères non sensibles à la casse. Conçues il y a plusieurs décennies, à une époque où la cybercriminalité n'était pas aussi développée, les applications mainframe étaient codées à l'aide de mots de passe faibles à huit caractères parce que ce type de sécurité était suffisant. Ce n'est plus le cas.

## Qu'est-ce que l'authentification multi-critères (MFA) ?

L'authentification multi-critères combine plusieurs sources d'identité afin d'autoriser l'accès. Les solutions de MFA les plus efficaces combinent au moins deux des trois types suivants de sources d'identité :

- Quelque chose que vous *connaissez*, par exemple un code PIN ou un mot de passe.
- Quelque chose que vous *possédez*, comme une carte, un téléphone ou un jeton.
- Quelque chose que vous *êtes*, par le biais de la prise d'empreintes, d'un scan rétinien, de la reconnaissance vocale ou de la reconnaissance du visage.

En exigeant au moins deux de ces trois types de sources d'identité, vous renforcez considérablement vos exigences en matière d'authentification et réduisez sensiblement le risque de violations de sécurité.

### Qu'est-ce qui n'est pas un exemple d'authentification multi-critères ?

Lorsque votre banque vous demande votre code PIN et votre numéro de sécurité sociale, il ne s'agit *pas* d'une authentification multi-critères. En effet, les codes PIN et numéros de sécurité sociale sont deux choses que vous *connaissez*. L'authentification multi-critères combine deux sources *différentes* sur trois parmi ce que vous connaissez, possédez ou êtes.

## Le besoin croissant d'authentification multi-critères

Les entreprises se rendent de plus en plus compte des risques associés à l'authentification à un seul critère des transactions en ligne. « Selon le rapport 2013 de Verizon sur les violations de données, qui dénonçait l'authentification à un seul facteur comme principal responsable des violations de sécurité, 76 % des intrusions réseau de 2012 exploitaient des informations de connexion volées ou faciles à deviner. » Il s'agit d'une tendance coûteuse qui peut être inversée grâce à l'authentification multi-critères, de manière à rendre les paiements électroniques aussi rapides et fiables que les paiements en espèces.

La prolifération de nouvelles réglementations officielles, notamment HIPAA, contribue également à l'adoption de l'authentification multi-critères. Le 26 mars 2013, de nouvelles réglementations du ministère américain de la Santé et des Services sociaux sont entrées en vigueur, étendant les exigences HIPAA en matière de sécurité et de confidentialité aux associés (notamment les sous-traitants, fournisseurs et fournisseurs de services) qui offrent des services pour le compte d'un prestataire de soins de santé ou qui fournissent des solutions qui s'intègrent aux données médicales ou aux données des patients. Confrontées à de lourdes amendes en cas de non-conformité, de nombreuses entreprises se tournent vers l'authentification multi-critères.

## Si l'authentification multi-critères présente autant d'avantages, pourquoi ne l'utilisons-nous pas encore ?

Les changements se heurtent souvent à de la résistance, et la migration vers l'authentification multi-critères ne fait pas exception. La résistance face à l'authentification multi-critères est généralement due à une ou plusieurs des raisons suivantes :

- **Manque d'information** : certaines méthodes d'authentification biométriques (tels que les lecteurs d'empreintes digitales) sont déjà intégrées aux smartphones et aux ordinateurs de bureau.

Mais de nombreuses entreprises ne savent pas comment incorporer ces nouvelles technologies dans leurs infrastructures de sécurité existantes.

- **Peur de l'inconnu** : certaines entreprises se demandent par exemple si l'authentification multi-critères va compliquer l'expérience utilisateur. Souvent, simplicité d'utilisation et efficacité vont de pair et les entreprises hésitent à modifier leurs processus pour quelque raison que ce soit, même pour renforcer leur sécurité.
- **Peur de l'échec** : afin de profiter pleinement de l'authentification multi-critères, vous devez la mettre en place de manière généralisée. Dans le cas contraire, vous obtiendrez des résultats médiocres. L'ampleur de la mise en oeuvre nécessaire peut être décourageante.

Et les causes de la résistance face à la mise en oeuvre de l'authentification multi-critères pour autoriser l'accès au mainframe peuvent être encore plus difficiles à surmonter.

## L'authentification multi-critères et le mainframe

Si la sécurité de l'accès aux applications d'entreprise a évolué pour faire face à des menaces de plus en plus sophistiquées, la sécurité de l'accès aux applications mainframe n'a pas changé depuis des décennies. Si vous demandez à n'importe quel professionnel de la sécurité informatique s'il pense que les mots de passe à huit caractères non sensibles à la casse offrent un niveau d'authentification adapté pour les données sensibles, la réponse sera toujours un non catégorique ! Et pourtant, le mainframe n'est généralement pas abordé lors des discussions sur l'authentification multi-critères.

Le problème est qu'aussi performant et fiable qu'il soit, le mainframe est généralement isolé du reste de l'entreprise. Les administrateurs informatiques préfèrent laisser ce domaine aux experts du mainframe. Ces experts (les administrateurs système mainframe) savent que reconfigurer les applications mainframe de manière à exiger l'utilisation de mots de passe complexes est un processus risqué, difficile et coûteux. Ils ne veulent pas compromettre la fiabilité à 99,999 % du mainframe. Bien qu'ils s'inquiètent de la sécurité, ils se sentent pris au piège.

Pour venir à bout de cette résistance, il faut trouver le moyen d'étendre une sécurité robuste et gérée de manière centralisée aux applications mainframe sans compromettre les opérations métiers.

## La solution proposée par Micro Focus

Il existe un moyen sûr, facile à gérer et économique d'étendre une sécurité robuste et gérée de manière centralisée aux applications mainframe. Micro Focus® Host Access Management and Security Server (MSS). MSS intègre votre mainframe à votre système de gestion des identités et des accès (IAM), de manière à gérer et sécuriser l'accès au mainframe par le biais de vos émulateurs de terminaux Micro Focus.

Placé entre l'utilisateur et le mainframe, MSS utilise votre structure d'authentification LDAP existante pour valider les références des utilisateurs avant de leur permettre d'accéder au mainframe. En d'autres termes, les utilisateurs ne peuvent pas accéder à l'écran de connexion à l'hôte tant qu'ils n'ont pas été authentifiés et autorisés par le biais de références IAM complexes, telles que des mots de passe complexes. MSS fonctionne conjointement avec l'extension MSS Advanced Authentication pour fournir l'authentification la plus sécurisée possible à vos systèmes mainframe. Ensemble, ces deux produits prennent actuellement en charge 14 méthodes d'authentification différentes, des cartes à puce et codes de vérification envoyés par SMS aux empreintes digitales et scanners rétiniens. Vous pouvez choisir parmi toutes ces options celles qui sont les plus faciles à mettre en oeuvre et à maintenir au sein de votre entreprise.

Vous pouvez installer MSS et MSS Advanced Authentication sur un serveur ou sur le mainframe, en fonction de ce qui convient le mieux à votre entreprise. Vous bénéficierez ainsi d'une solution d'accès au mainframe flexible et hautement sécurisée, qui ne compromet pas vos opérations métiers.

## L'authentification multi-critères adaptée au mainframe

La mise en oeuvre d'une nouvelle technologie est souvent synonyme d'échec car personne n'a pris en compte toutes les implications. Il y a plusieurs facteurs dont vous devriez tenir compte avant de vous lancer dans l'authentification multi-critères :

- Établissez et mettez en oeuvre une stratégie globale d'authentification (plutôt que d'opter pour des acquisitions ad-hoc).
- Assurez-vous que l'authentification multi-critères est facile à gérer (évitez d'utiliser différentes méthodes d'authentification pour différents systèmes).
- Assurez-vous que l'authentification multi-critères est facile à utiliser (envisagez de mettre en oeuvre le Single Sign-on par la même occasion, afin de simplifier le processus d'authentification).

Mise en oeuvre correctement, l'authentification multi-critères simplifiera la vie de vos utilisateurs. Après tout, il est plus facile de poser son doigt sur un lecteur d'empreintes digitales et d'entrer un code PIN que de mémoriser un nom d'utilisateur et un mot de passe.

## Facteurs à prendre en considération lors du choix d'un fournisseur d'authentification multi-critères

Pour une intégration transparente de l'authentification multi-critères, tenez compte des facteurs suivants pendant vos recherches :

- Cherchez des solutions proposant plusieurs options et applications d'authentification.
- Évitez la dépendance vis-à-vis d'un seul type d'authentification physique (en d'autres termes, ne laissez pas le matériel que vous choisissez vous dicter votre philosophie en matière d'authentification).
- Recherchez des fournisseurs qui se basent sur une structure ouverte, mise à jour rapidement au fur et à mesure du lancement de nouvelles technologies.
- Enfin, recherchez des fournisseurs qui vous faciliteront la vie.

Il est tout à fait illogique d'exiger une authentification complexe pour permettre l'accès aux applications d'entreprise et de se contenter d'une authentification faible pour permettre l'accès aux applications mainframe stratégiques, sur lesquelles repose votre entreprise. Les menaces de sécurité continuant à s'intensifier, votre entreprise doit être prête à relever ce défi. Micro Focus offre un moyen sûr, facile à gérer et économique d'y parvenir.

**Micro Focus**
**France**
+33 (0) 1 55 70 30 13

**Micro Focus**
**Siège social au Royaume-Uni**
Royaume-Uni
+44 (0) 1635 565200

**www.microfocus.com**

**www.microfocus.com**