Livre blanc

La nouvelle approche en matière de mots de passe mainframe : ne plus en avoir

opentext™

La nouvelle approche en matière de mots de passe mainframe : ne plus en avoir

Dans une entreprise, les mots de passe sont indispensables. Ils garantissent que seuls les utilisateurs autorisés accèdent aux ressources les plus précieuses : les informations. Étant donné leur rôle stratégique, les mots de passe doivent remplir certains critères. Le mot de passe idéal est long et complexe. Il est différent pour chaque application et est régulièrement mis à jour.

Les mots de passe sont également une menace pour l'entreprise. Les utilisateurs doivent constamment créer, mémoriser et modifier des mots de passe, ce qui alourdit leur charge de travail. L'équipe IT doit gérer et appliquer des stratégies de mot de passe, ce qui est tout aussi fastidieux. Heureusement, les systèmes modernes Identity and Access Management (IAM) NetIQ et la technologie Single Sign-On (SSO) sont d'un grand secours. Les utilisateurs peuvent se connecter une seule fois pour accéder à la plupart des ressources de l'entreprise.

À *la plupart* d'entre elles, mais pas à *toutes*. Malheureusement, les systèmes IAM et le SSO ne fonctionnent pas sur les systèmes les plus stratégiques, ceux qui assurent le fonctionnement de votre entreprise : les systèmes mainframe.

« Donnez-nous un accès au mainframe partout, à tout moment et sur tous les types de périphériques »

Les utilisateurs d'aujourd'hui s'attendent à bénéficier d'un accès partout, à tout moment et sur tout type de périphérique aux ressources de l'entreprise, mainframe compris. Cependant, le fait d'accorder un accès illimité au mainframe est un véritable cauchemar pour les administrateurs de ces systèmes et du réseau.

Pourquoi ? Parce que lorsqu'il s'agit de fournir un accès sécurisé, le réseau et le mainframe sont comme deux îlots autonomes. Chacun possède son propre système de contrôle des accès. Chacun a son propre dirigeant. Et aucun de ces dirigeants ne souhaite renoncer à un contrôle quelconque sur son domaine au bénéfice de l'autre.

Malgré leur dépendance mutuelle et les avantages qui pourraient découler de leur collaboration, les dirigeants de chaque îlot ne voient pas comment surmonter les obstacles à l'intégration.

L'îlot du réseau

Les administrateurs réseau ont tout intérêt à améliorer la sécurité de l'accès au mainframe, car ils gèrent les applications d'émulation de terminal qui rendent cet accès possible. Mais, il n'existe aucun moyen d'étendre la sécurité réseau renforcée, basée sur des mots de passe complexes gérés par le système IAM, jusqu'à l'îlot du mainframe.

La plupart des applications mainframe ont été conçues il y a plusieurs décennies, à une époque plus sûre. Les réseaux ouverts, les architectures orientées services et la cybercriminalité n'existaient pas. Les applications mainframe étaient codées à l'aide de mots de passe faibles à huit caractères, car ce type de sécurité était suffisant. Ce n'est plus le cas.

Reconcevoir les applications mainframe aujourd'hui (à condition de trouver un programmeur de mainframe encore en activité) est à la fois dangereux, coûteux et source de perturbations. La seule manière d'appliquer un mot de passe unique pour accéder à toutes les ressources réseau, mainframe inclus, consiste à réduire les mots de passe de toute l'entreprise à huit caractères. Personne ne souhaite recourir à cette solution.

L'îlot du mainframe

Les administrateurs de systèmes mainframe savent que les pirates informatiques, après avoir largement ignoré le mainframe pendant des années, le prennent aujourd'hui pour cible. Ils ne disposent pas de systèmes IAM, mais utilisent RACF ou Top-Secret pour authentifier et autoriser l'accès au mainframe. Bien que ces outils soient efficaces, ils restent cantonnés à des mots de passe faibles à huit caractères.

Même s'ils souhaitent renforcer les mots de passe (et le contrôle d'accès), les administrateurs de systèmes mainframe sont inflexibles sur un point : en aucun cas ils ne mettront en péril la fiabilité de 99,999 % du mainframe. Or, ils ont l'impression que c'est ce qui se produirait s'ils tentaient d'intégrer l'accès au mainframe aux serveurs de l'îlot du réseau. Et ils ne peuvent pas se permettre les constantes interruptions de service habituellement associées aux problèmes de sécurité réseau.

Les problèmes liés aux mots de passe mainframe

Aussi capables soient-ils, les mainframes présentent des particularités qui relèvent de l'excentricité dans l'entreprise moderne. L'une de ces particularités est le mot de passe requis pour accéder aux applications mainframe. Ce point est problématique à plusieurs égards :

- **L'authentification faible**
  Demandez à n'importe quel expert en sécurité informatique s'il pense que des mots de passe à huit caractères non sensibles à la casse sont suffisants pour protéger les données sensibles. Il vous répondra fermement que non. Les mots de passe d'entreprise sont régis par des stratégies rigoureuses. Mais, pour les raisons expliquées plus haut, ces stratégies ne peuvent pas être appliquées à l'accès au mainframe.

Défense en profondeur avec MSS

Vous pouvez même multiplier les couches de sécurité en associant MSS aux extensions suivantes :

- **Extension Security Proxy de MSS**
  Fournissez un chiffrement de bout en bout et contrôlez l'accès au périmètre au moyen d'une technologie de sécurité brevetée.
- **Extension Advanced Authentication de MSS**
  Activez l'authentification multi-critères pour autoriser l'accès à vos serveurs stratégiques.
- **Extension Automated Sign-On for Mainframe de MSS**
  Fournissez une connexion automatisée aux applications IBM 3270 par le biais de votre système de gestion des accès et des identités.
- **Extension PKI Automated Sign-On de MSS**
  Fournissez une connexion automatisée avec PKI à vos systèmes d'entreprise stratégiques.
- **Extension Terminal ID Management de MSS**
  Allouez dynamiquement des ID de terminal en fonction du nom d'utilisateur, du nom DNS, de l'adresse IP ou de la réserve d'adresses.

Grâce à MSS et à ses extensions, vous disposez enfin d'un moyen pratique de moderniser la sécurité du mainframe sans rien recoder.

Fonctionnement d'Automated Sign-On for Mainframe

En association avec IBM z/OS Digital Certificate Access Server (DCAS), l'extension Automated Sign-On for Mainframe obtient une référence PassTicket à usage unique, limitée dans le temps, pour l'application cible. Elle renvoie l'ID utilisateur mainframe et la référence PassTicket à la macro de connexion de l'émulateur de terminal, qui renvoie à son tour les références au mainframe afin de connecter l'utilisateur à l'application.

- **Les comportements à risque des utilisateurs**
  À l'ère de l'accès instantané, l'étape de connexion supplémentaire exigée pour accéder au mainframe est une perte de temps pour la plupart des utilisateurs. Pensez-y. Qui a envie de saisir un mot de passe différent chaque fois qu'il ouvre une nouvelle application, surtout s'il doit en ouvrir cinq ou six par jour ? Les utilisateurs trouvent donc des solutions de contournement, comme ne pas se déconnecter ou laisser leur poste de travail allumé (et non protégé) lorsqu'ils quittent le bureau.
- **Le calvaire de la réinitialisation des mots de passe mainframe**
  Les utilisateurs qui accèdent à plusieurs applications depuis différents systèmes mainframe doivent se souvenir de plusieurs mots de passe. Comme c'est impossible, ils ont recours à des solutions incompatibles avec les principes de sécurité, comme des post-its ou une modification minimale du mot de passe au moment de sa mise à jour. Malgré tout, les utilisateurs oublient leurs mots de passe et ceux-ci doivent être réinitialisés. Contrairement aux mots de passe réseau, les mots de passe mainframe ne peuvent pas être réinitialisés par l'utilisateur. Un informaticien doit s'interrompre dans son travail pour réaliser cette tâche banale et chronophage.

Au vu des risques en matière de sécurité, du manque de convivialité et des problèmes de gestion informatique qu'elle entraîne, la pratique qui consiste à se connecter au mainframe à l'aide d'un mot de passe à huit caractères doit être mise à jour.

Le pont qui comble les écarts en matière de sécurité

Nos deux îlots n'ont pas évolué en parallèle. Sur l'îlot du réseau, la sécurité qui encadre l'accès aux applications d'entreprise s'est renforcée pour faire face aux menaces toujours plus sophistiquées. Sur l'îlot du mainframe, la sécurité définie au moment de la conception des applications stratégiques n'a pas changé depuis des décennies.

Fort heureusement, il existe enfin un moyen d'étendre la sécurité robuste et gérée de manière centralisée aux applications mainframe sans compromettre les opérations métiers : OpenText™ Host Access Mana gement and Security Server (MSS). MSS intègre le mainframe au système IAM en construisant un pont entre les deux îlots.

Plus précisément, MSS fonctionne avec votre système IAM afin de centraliser la gestion et la sécurisation de l'accès au mainframe via les émulateurs de terminal Micro Focus. Placé entre l'utilisateur et le mainframe, il 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 accéder à l'écran de connexion au serveur qu'après avoir été authentifiés et autorisés par le biais de références IAM (et donc de mots de passe) complexes.

Si vous l'associez à l'une de ses extensions (Automated Sign-On for Mainframe), MSS élimine même la nécessité d'utiliser des mots de passe mainframe. En effet, les utilisateurs n'ont plus besoin de passer par l'étape supplémentaire qui consiste à saisir un mot de passe pour se connecter aux applications mainframe après l'authentification MSS. MSS s'en charge à leur place. Avec cette solution, tout le monde est gagnant : les utilisateurs n'ont plus besoin de se souvenir de mots de passe à huit caractères, et l'équipe chargée de la sécurité informatique ne s'occupe plus de la gestion des mots de passe.

Vous pouvez installer MSS sur un serveur ou sur le mainframe, selon ce qui convient le mieux à votre entreprise. Vous bénéficiez ainsi d'une solution d'accès au mainframe flexible, évolutive et hautement sécurisée qui ne nécessite plus aucun mot de passe mainframe.

Une solution sûre, facile à gérer et économique

Autrefois, vos précieuses données de mainframe circulaient en toute sécurité d'un terminal à l'autre. Ce n'est plus le cas. Aujourd'hui, il vous faut le plus haut niveau de protection pour les protéger des menaces sur Internet. Il est temps d'abandonner les mots de passe faibles à huit caractères qui appartiennent au passé. Au lieu de cela, construisez un pont vers le plus haut niveau d'authentification possible, et soyez certain que seuls les utilisateurs autorisés accèdent aux données les plus précieuses. MSS offre un moyen sûr, facile à gérer et économique d'y parvenir.

Pour en savoir plus, rendez-vous sur
www.microfocus.com/opentext

Communiquez avec nous

Blog du PDG d'OpenText Mark Barrenechea

262-FR0080-001 | O | 08/23 | © 2023 Open Text

opentext™