Informe oficial

Host Access Management and Security Server (MSS)
MSS Advanced Authentication Add-On

Uso de la autenticación basada en varios factores para autorizar el acceso al mainframe

MICRO FOCUS

Las contraseñas son malas

Sinceramente, la autenticación de los usuarios con nombres de usuario y contraseñas ya no es eficaz. ¿Por qué? Porque los usuarios son poco cuidadosos con sus contraseñas. Eligen contraseñas obvias y las utilizan una y otra vez. Además, las escriben en notas adhesivas que cualquiera puede encontrar.

Pero los usuarios no son el único problema

Cuando se confía en nombres de usuario y contraseñas, prácticamente le está dejando vía libre a los piratas informáticos. Los delincuentes tecnológicos escriben avanzados algoritmos para buscar algún puerto de entrada. Por lo tanto, cuando se utiliza la misma contraseña para múltiples aplicaciones, los piratas informáticos que han averiguado una contraseña pueden fisgonear donde quieran. Por ejemplo, un pirata informático podría robar la contraseña de un usuario de Facebook y así obtener acceso a toda su infraestructura corporativa. Este es un gran motivo de preocupación.

La conclusión es que los nombres de usuario y las contraseñas son cosas que un usuario tiene que saber. Y esas cosas se pueden averiguar o robar con relativa facilidad. No son suficientemente seguras por sí mismas.

Las antiguas contraseñas del mainframe son aún peores

Los problemas con las contraseñas que acabamos de describir también se aplican a las contraseñas del mainframe. La diferencia es que las contraseñas del mainframe para aplicaciones antiguas (las que se necesitan para gestionar su negocio y que contienen todos sus datos más confidenciales) son de solo ocho caracteres y no distinguen entre mayúsculas y minúsculas. Creadas hace décadas, en una época más segura, las aplicaciones de mainframe estaban bien codificadas con contraseñas débiles de ocho caracteres porque esto era suficiente. Pero eso fue hace mucho, mucho tiempo...

¿Qué es la autenticación basada en varios factores (MFA)?

La MFA combina varias fuentes de identificación para autorizar el acceso. Las soluciones de MFA más eficaces combinan al menos dos de los siguientes tres tipos de fuentes de identificación:

- Algo que *sepa*, como un código PIN o una contraseña.
- Algo que *tenga*, como una tarjeta de acceso, un teléfono o un testigo.
- Algo que *sea*, como una huella dactilar, un escáner de retina, un reconocimiento de voz o un reconocimiento facial.

Al solicitar al menos dos de estas tres fuentes de identificación, se incrementan los requisitos de autenticación y el riesgo de infracción de la seguridad se reduce enormemente.

¿Qué no es la MFA?

Que su banco le pida su PIN y el número de la seguridad social no *es* MFA. Los PIN y los números de la seguridad social son dos cosas que *sabe*. MFA combina dos de las tres *fuentes:* cosas que sabe, tiene o es.

La MFA, cada vez más necesaria

Las organizaciones son cada vez más conscientes de los riesgos asociados a la autenticación basada en un solo factor para las transacciones en línea. "El informe sobre infracción de la seguridad informática de Verizon de 2013 señaló a la autenticación basada en un solo factor como el principal responsable de los fallos de seguridad; además destacó que el 76 % de las intrusiones en la red en 2012 se realizaron tras el robo de credenciales o la debilidad de las mismas". La MFA puede resolver este costoso problema haciendo que los pagos electrónicos sean tan rápidos y fiables como los pagos en metálico.

La proliferación de nuevas regulaciones gubernamentales, como HIPAA, también está impulsando la adopción de la MFA. El 26 de marzo de 2013 entraron en vigor las nuevas normas del Departamento de salud y servicios sociales estadounidense. Estas normas aumentan los requisitos de seguridad y confidencialidad de HIPAA para los socios comerciales (entre otros, contratistas, proveedores y proveedores de servicios) que prestan servicios en nombre de un proveedor de servicios de salud o que proporcionan soluciones que integran datos médicos o de pacientes. Tras costosas multas por haber incumplido las normas, muchas organizaciones están adoptando la MFA.

Si la MFA tiene tantos aspectos positivos, ¿por qué no la hemos estado utilizando?

Los cambios suelen ir acompañados de cierta resistencia, y la migración a MFA no es una excepción. La resistencia a la MFA suele estar relacionada con uno o más de los siguientes motivos:

- **Falta de información**: los métodos de autenticación biométrica (por ejemplo, escáneres de huellas digitales) ya se han incorporado a los smartphones y los PC. Pero muchas empresas no saben cómo incorporar esta nueva tecnología a las infraestructuras de seguridad establecidas.

- **El temor a lo desconocido**: por ejemplo, ¿dificultará la MFA la experiencia del usuario? Puesto que la facilidad de uso a menudo se traduce en eficiencia, las organizaciones son reacias a cambiar el statu quo por cualquier razón, aunque sea en pro de una seguridad aún mayor.
- **Miedo al fracaso**: para sacarle el máximo partido a la MFA, deberá adoptarla de forma generalizada. De lo contrario, obtendrá resultados mediocres. El calibre de la implantación necesaria puede ser un factor desalentador.

En lo que respecta a la aplicación de la MFA para autorizar el acceso al mainframe, el origen de la resistencia puede ser aún más difícil de vencer.

La MFA y el mainframe

Si bien la seguridad del acceso a aplicaciones empresariales se ha incrementado para hacer frente a amenazas cada vez más sofisticadas, la seguridad de las aplicaciones de mainframe ha estado paralizada durante décadas. Puede preguntarle a cualquier profesional de seguridad de TI si cree que las contraseñas de ocho caracteres que no distinguen entre mayúsculas y minúsculas proporcionan un nivel adecuado de autenticación para el acceso a datos sensibles. La respuesta será un "No" rotundo. Aun así, el mainframe suele quedar fuera de las discusiones relacionadas con MFA.

El problema es el siguiente: el mainframe, tan sólido y fiable, suele quedar aislado del resto de la empresa. Los administradores de TI consideran que es mejor dejárselo a los expertos en mainframe. Dichos expertos, los administradores de sistemas mainframe, saben que la reforma de aplicaciones de mainframe para trabajar con contraseñas complejas y seguras es arriesgada, difícil y cara. No tienen ninguna intención de poner en peligro el historial de fiabilidad del 99,999 % del mainframe. Por mucho que les preocupe la seguridad, se sienten estancados.

Lo que se necesita para vencer su resistencia es ampliar la gran seguridad centralizada de las aplicaciones de mainframe sin poner en peligro las operaciones de la empresa.

La solución de Micro Focus

De hecho, existe un modo seguro, fácil de gestionar y económico de ampliar la gran seguridad centralizada de las aplicaciones de mainframe. Se llama Micro Focus® Host Access Management and Security Server (MSS). MSS integra el mainframe con el sistema de gestión de acceso e identidades (IAM), de forma que gestiona y protege el acceso al mainframe a través de los emuladores de terminal de Micro Focus.

MSS se sitúa entre el usuario y el mainframe y utiliza su estructura de autenticación LDAP existente para validar las credenciales de un usuario antes de otorgarle acceso al mainframe. En otras palabras, los usuarios no pueden llegar a la pantalla de conexión del host hasta que no se hayan autenticado y autorizado mediante credenciales sólidas de IAM, (es decir, con contraseñas complejas y seguras).

MSS trabaja junto con un producto adicional llamado MSS Advanced Authentication para proporcionar una autenticación lo más segura posible para sus sistemas mainframe. Juntos, actualmente estos dos productos son compatibles con 14 métodos de autenticación diferentes: desde tarjetas inteligentes y códigos de verificación basados en texto de dispositivos móviles hasta escáneres de huella dactilar y retina. De entre estas opciones, puede seleccionar las que su organización pueda adoptar y mantener más fácilmente.

MSS y MSS Advanced Authentication pueden instalarse en un servidor o en el mainframe, lo que sea mejor para su negocio. Proporciona una solución flexible y muy segura para acceder al mainframe que no pone en peligro las operaciones de la empresa.

Una nueva perspectiva de la MFA para el mainframe

Cuando una nueva tecnología se pone en marcha, suele fallar porque nadie es capaz de valorar todas las implicaciones. En lo que a la MFA respecta, hay varios aspectos que debe tener en cuenta antes de comenzar:

- Establecer y aplicar una directiva global de autenticación (en lugar de adoptar un enfoque fragmentado con adquisiciones ad-hoc).
- Conseguir que la MFA sea fácil de gestionar (evitando emplear métodos de autenticación diferentes para cada sistema).
- Conseguir que la MFA sea fácil de usar (puede aplicar la entrada única al mismo tiempo para simplificar el proceso de autenticación).

Si utiliza el modo adecuado, la MFA facilita los procesos a los usuarios. Al fin y al cabo pasar el dedo por el escáner e introducir un PIN es más sencillo que recordar un nombre de usuario y una contraseña.

Qué debe buscar en un proveedor de MFA

Para garantizar que la MFA se integra correctamente, tenga en cuenta estos factores durante su búsqueda:

- Busque soluciones que ofrezcan varias aplicaciones y opciones de autenticación.
- No se ate a un único tipo de autenticación física, es decir, no permita que su elección de hardware determine su filosofía de autenticación.
- Busque proveedores que desarrollen un marco de trabajo abierto, que se actualice conforme vayan surgiendo nuevas tecnologías.
- Busque proveedores que le faciliten el uso del sistema.

No tiene sentido solicitar una autenticación muy segura para acceder a las aplicaciones empresariales, pero una autenticación débil para acceder a aplicaciones de mainframe esenciales, es decir, aquellas con las que se dirige el negocio. Su capacidad de respuesta ante las amenazas debe evolucionar al mismo ritmo que ellas. Micro Focus le ofrece un modo de hacerlo seguro, fácil de gestionar y económico.

Argentina
+54 11 5258 8899

Chile
+56 2 2864 5629

Colombia
+57 1 622 2766

México
+52 55 5284 2700

Panamá
+507 2 039291

España
+34 91 781 5004

Venezuela
+58 212 267 6568

Micro Focus
Sedes corporativas
Reino Unido
+44 (0) 1635 565200

www.microfocus.com

www.microfocus.com