Informe oficial

Un nuevo enfoque para las contraseñas del mainframe: líbrese de ellas

opentext™

Un nuevo enfoque para las contraseñas del mainframe: líbrese de ellas

Las contraseñas son necesarias para las empresas. Su tarea es garantizar que solo los usuarios autorizados tienen acceso a su bien más preciado: la información. Dado la función esencial que desempeñan, no nos sirve cualquier contraseña. La contraseña ideal debe ser larga y compleja. También debe ser distinta para cada aplicación. Y no olvidemos que se debe actualizar regularmente.

Las contraseñas también representan un peligro para las empresas. Hay que crearlas, recordarlas y cambiarlas constantemente, lo que representa una complicación añadida para los usuarios. Del mismo modo, gestionar y aplicar las directivas de contraseñas también supone una carga para el equipo de TI. Afortunadamente, los sistemas de gestión de acceso e identidades (IAM, por sus siglas en inglés) y entrada única (SSO) facilitan esta tarea. Los usuarios solo tienen que iniciar sesión una vez para tener acceso a la mayor parte de los recursos de su empresa.

A la mayor parte, sí, pero no a *todos*. Por desgracia, IAM y SSO no son compatibles con sus sistemas más importantes, es decir, aquellos que realmente hacen funcionar la empresa: los sistemas mainframe.

"Queremos tener acceso al mainframe, a cualquier lugar y en cualquier dispositivo"

Actualmente, los usuarios esperan tener acceso a todos los recursos de su empresa, incluido el mainframe, sin importar el momento, el lugar o el tipo de dispositivo. Sin embargo, otorgarles un acceso al mainframe sin restricciones desbordaría a los administradores de la red del equipo de TI y a los administradores de sistemas mainframe.

¿Por qué? Porque, en lo que respecta a la seguridad de acceso, podríamos comparar a la red y al mainframe con dos islas completamente independientes. Cada una emplea su propio sistema para controlar el acceso. Cada una cuenta con su propio dirigente. Y ninguna de las dos está dispuesta a ceder parte del control sobre su dominio en beneficio de la otra.

A pesar de la dependencia mutua y de las ventajas que se podrían conseguir si trabajaran juntas, los dirigentes de dichas islas no ven ninguna solución posible a sus problemas de integración.

La isla de la red

Los administradores de la red de TI tienen especial interés en fortalecer la seguridad de acceso al mainframe, ya que son ellos los que gestionan las aplicaciones de emulación de terminal que permiten dicho acceso. No obstante, no existe ninguna manera factible de ampliar la gran seguridad de la red para acceder al mainframe gracias a sus contraseñas seguras facilitadas por la IAM.

La mayor parte de las aplicaciones de mainframe fueron creadas hace décadas, cuando no había tantos riesgos para la seguridad. Por aquel entonces, no existían las redes abiertas, las arquitecturas orientadas a servicios ni los piratas informáticos malintencionados. Las aplicaciones de mainframe estaban bien codificadas con contraseñas débiles de ocho caracteres porque eso era suficiente. Pero eso fue hace mucho, mucho tiempo...

Volver a escribir sus aplicaciones de mainframe en estos momentos resulta arriesgado, caro y perjudicial para el rendimiento, incluso en el caso de encontrar un programador de mainframe que siga en activo. La única opción restante para aplicar una sola contraseña con la que acceder a todos los recursos de la red, incluido el mainframe, es reducir la complejidad de las contraseñas de la empresa y hacerlas de ocho caracteres. Y esta opción no es del agrado de nadie.

La isla del mainframe

Los administradores de los sistemas de mainframe saben que, aunque durante décadas la comunidad de piratas informáticos lo haya ignorado, ahora su mainframe se ha convertido en el blanco de sus ataques. Aunque no disponen de IAM, cuentan con RACF o Top-Secret para autenticar y autorizar el acceso al mainframe. Esta solución, aunque es totalmente válida, no soluciona el problema de las contraseñas débiles de ocho caracteres.

A pesar de lo mucho que les gustaría fortalecer sus contraseñas y reforzar el control de acceso, los administradores de sistemas mainframe no ceden en una cosa: bajo ninguna circunstancia pondrán en peligro el historial de fiabilidad del 99,999 % del mainframe. Pero, en su fuero interno, saben que eso es exactamente lo que deberían hacer si quisieran integrar el acceso al mainframe con los servidores de red. Simplemente no pueden permitirse el tiempo de inactividad constante que se suele asociar con los problemas de seguridad de red de la otra isla.

Problemas con las contraseñas del mainframe

A pesar de sus muchas posibilidades, los mainframes tienen ciertas peculiaridades que los convierten en unos "bichos raros" en el contexto de la empresa moderna. Una de estas particularidades es la contraseña de las aplicaciones de mainframe. ¿Por qué puede resultar un problema?

- **Autenticación débil**
  Pregunte a cualquier experto de seguridad si piensa que una contraseña de ocho caracteres y sin distinción entre mayúsculas y minúsculas es lo suficientemente eficaz para proteger datos confidenciales. La respuesta será un rotundo "no". Hay estrictas directivas asociadas a las contraseñas de la empresa. No obstante, por las razones que hemos mencionado antes, estas directivas no se pueden aplicar al acceso al mainframe.

Defensa en profundidad gracias a MSS

Puede añadir más capas de seguridad todavía al combinar MSS con los siguientes componentes adicionales:

- **MSS Security Proxy Add-On**
  Ofrezca un cifrado de extremo a extremo y aplique el control de acceso en los perímetros con la tecnología de seguridad patentada.
- **MSS Advanced Authentication Add-On**
  Habilite la autenticación basada en varios factores para autorizar el acceso a los valiosos sistemas host.
- **MSS Automated Sign-On for Mainframe Add-On**
  Habilite la entrada automática en las aplicaciones IBM 3270 a través de su sistema de gestión de acceso e identidades.
- **MSS PKI Automated Sign-On Add-On**
  Permita que las aplicaciones automatizadas PKI puedan entrar en los sistemas fundamentales de la empresa.
- **MSS Terminal ID Management Add-On**
  Asigne ID de terminal de forma dinámica en función del nombre de usuario, el nombre DNS, la dirección IP o el repositorio de direcciones.

Gracias a MSS y sus productos adicionales, por fin existe una manera práctica de modernizar la seguridad del mainframe sin tener que recodificar.

Cómo funciona Automated Sign-On for Mainframe

Al trabajar con el servidor de certificados de acceso digitales (DCAS) de IBM z/OS, Automated Sign-On for Mainframe obtiene un R PassTicket temporal y de un solo uso para la aplicación de destino. Este devuelve el ID de usuario del mainframe y el PassTicket a la macro de inicio de sesión del emulador del terminal, que a su vez envía las credenciales al mainframe para que el usuario pueda iniciar sesión en la aplicación.

- **Comportamiento peligroso de los usuarios**
  En estos tiempos en los que queremos tener acceso instantáneo a cualquier recurso, un paso adicional en el momento de iniciar sesión resulta una pérdida de tiempo para la mayoría de los usuarios. Parémonos a pensar en ello. ¿A quién le apetece introducir una contraseña diferente cada vez que abre una nueva aplicación, especialmente si tiene que abrir cinco o seis al día? Por este motivo, los usuarios buscan alternativas más cómodas, como no cerrar la sesión o dejar sus estaciones de trabajo encendidas (y desprotegidas) cuando tienen que ausentarse.
- **Restablecimiento de la contraseña del mainframe**
  Los usuarios que tienen acceso a varias aplicaciones o mainframes deben recordar varias contraseñas. Nadie puede memorizarlas todas, así que recurren a prácticas nada recomendadas, como apuntarlas en notas adhesivas o realizar leves cambios en las contraseñas cuando es necesario actualizarlas. Además, los usuarios se olvidan de ellas, por lo que deben restablecerse. Al contrario que ocurre con las contraseñas de red, los usuarios no pueden restablecer la contraseña del mainframe. Un empleado de TI debe interrumpir lo que esté haciendo y emplear su valioso tiempo en realizar esta laboriosa y trivial tarea.

El inicio de sesión en el mainframe con una contraseña de ocho caracteres es una práctica que hay que renovar, ya sea por los riesgos para la seguridad que conlleva, los problemas de usabilidad o los quebraderos de cabeza que produce al personal de TI.

El puente hacia una solución de seguridad común

Nuestras dos islas no han evolucionado en paralelo. En la isla de la red, la seguridad para acceder a las aplicaciones de la empresa se ha reforzado para hacer frente a amenazas cada vez más sofisticadas. En la isla del mainframe, no ha habido ningún cambio en la seguridad incluida en las aplicaciones más importantes (y que data de hace décadas).

Por suerte, por fin hay una manera de que las aplicaciones de mainframe dispongan de una gran seguridad centralizada sin poner en peligro las operaciones de la empresa. Se llama OpenText™ Host Access Management and Security Server (MSS). MSS integra el mainframe en su sistema IAM, lo que le permite construir un puente entre las dos islas.

Más concretamente, MSS trabaja junto a su sistema IAM para proporcionarle un método de gestión centralizado y reforzar la seguridad del 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 mediante credenciales sólidas de IAM, (es decir, con contraseñas complejas y seguras) y estén autorizados.

Junto a Automated Sign-On for Mainframe, uno de sus componentes adicionales, MSS le permite librarse de las contraseñas del mainframe. Efectivamente, los usuarios ya no tienen que introducir una contraseña adicional para iniciar sesión en sus aplicaciones de mainframe una vez completado el proceso de autenticación en MSS. La solución realiza esta tarea por ellos. Es una victoria a dos bandas para los usuarios (ya no tienen que recordar una contraseña de ocho caracteres poco segura) y los equipos de TI preocupados por la seguridad (ya no tienen que preocuparse de gestionar contraseñas).

MSS puede instalarse en un servidor o en el mainframe, lo que sea mejor para su empresa. Es una solución para el acceso al mainframe flexible, escalable y muy segura que le permite olvidarse de las contraseñas del mainframe.

Segura, fácil de gestionar y económica

Hace mucho, mucho tiempo, sus valiosos datos del mainframe se transferían por canales seguros, a y desde terminales de confianza. Pero eso fue hace mucho, mucho tiempo... Hoy en día, blindarse contras las amenazas de Internet requiere contar con la protección de mayor seguridad disponible. Ha llegado el momento de dejar atrás las débiles contraseñas de ocho caracteres. Construya un puente hacia el método de autenticación más fuerte que existe, lo que le permitirá garantizar que solo los usuarios autorizados tienen acceso a sus datos más valiosos. MSS le permite cumplir este objetivo de una manera segura, fácil de gestionar y económica.

Más información en
www.microfocus.com/opentext

Póngase en contacto con nosotros

El blog de Mark Barrenechea, director general de OpenText

262-ES0080-001 | O | 09/23 |

opentext™