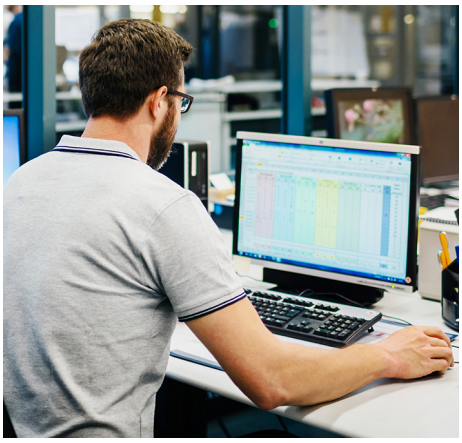
opentext™



Tome una decisión inteligente y opte por el inicio de sesión automatizado para el acceso al mainframe

Albert Einstein dijo que la definición de locura es hacer lo mismo una vez tras otra y esperar resultados diferentes. Asimismo, aplicar el mismo tipo de seguridad para el acceso al mainframe año tras año y esperar que se convierta en un método más seguro por arte de magia es, en realidad, una locura.

Aunque la protección del acceso a las aplicaciones empresariales ha evolucionado para adaptarse a las nuevas amenazas de seguridad, la propia protección del acceso a las aplicaciones de mainframe no ha cambiado en décadas. Este estancamiento se ha producido por tres razones clave:

- En primer lugar, las aplicaciones de mainframe heredadas siguen encargándose del trabajo más pesado en la mayoría de las empresas. Esto se debe a que cambiarlas es arriesgado, difícil y oneroso. Incluso encontrar los recursos humanos necesarios para actualizar los controles de acceso seguro de dichas aplicaciones es casi imposible.
- En segundo lugar, las empresas grandes suelen carecer de la voluntad interna necesaria para abrir la "caja de Pandora" del mainframe. Algunas de las cuestiones que surgen en el departamento de TI son: ¿Qué pasa si se estropea algo? ¿Y si es mucho más complicado de lo que pensábamos? ¿Y si nuestro negocio se hunde? No podemos llevar el mainframe a puerto seguro y arreglar todo mientras continuamos con nuestra actividad empresarial. Además, el precio de duplicar ese entorno es demasiado alto en términos de tiempo y dinero.
- En tercer lugar, existe la percepción de que el mainframe estará sano y salvo detrás del firewall, al que solo pueden acceder los usuarios autorizados. Sin embargo, no hay ninguna garantía de que alguien con malas intenciones pueda robar o piratear las credenciales de inicio de sesión del mainframe de un usuario. En estas aplicaciones antiguas se utilizan contraseñas débiles de ocho caracteres y sin distinción entre mayúsculas y minúsculas. Ningún administrador de red del planeta consideraría que esas contraseñas son lo suficientemente seguras para proteger nada, especialmente la información sujeta a propiedad intelectual o información de cliente.

La pregunta es, ¿cómo se rompe un patrón de locura cuando algunas de las razones de dicha conducta se basan en temores muy reales y lógicos?

Los sistemas de seguridad incoherentes de la empresa

La mayoría de las empresas cuentan con dos sistemas de seguridad. Uno es el de gestión de acceso e identidades (IAM), que se utiliza para proporcionar acceso a los recursos y aplicaciones de la empresa. Para acceder a los sistemas IAM se debe usar una contraseña segura, normalmente de un mínimo de 12 caracteres, y que incluya letras mayúsculas y minúsculas, números y caracteres especiales. Las contraseñas seguras son infinitamente más difíciles de robar o piratear.

Los sistemas mainframe tienen también su propio método de "IAM", comúnmente conocido como RACF o Top-Secret. Estos sistemas proporcionan autenticación y autorización para recursos de mainframe. El problema es que, según el diseño original, las aplicaciones que utilizan estos sistemas solo funcionan con contraseñas débiles de ocho caracteres.

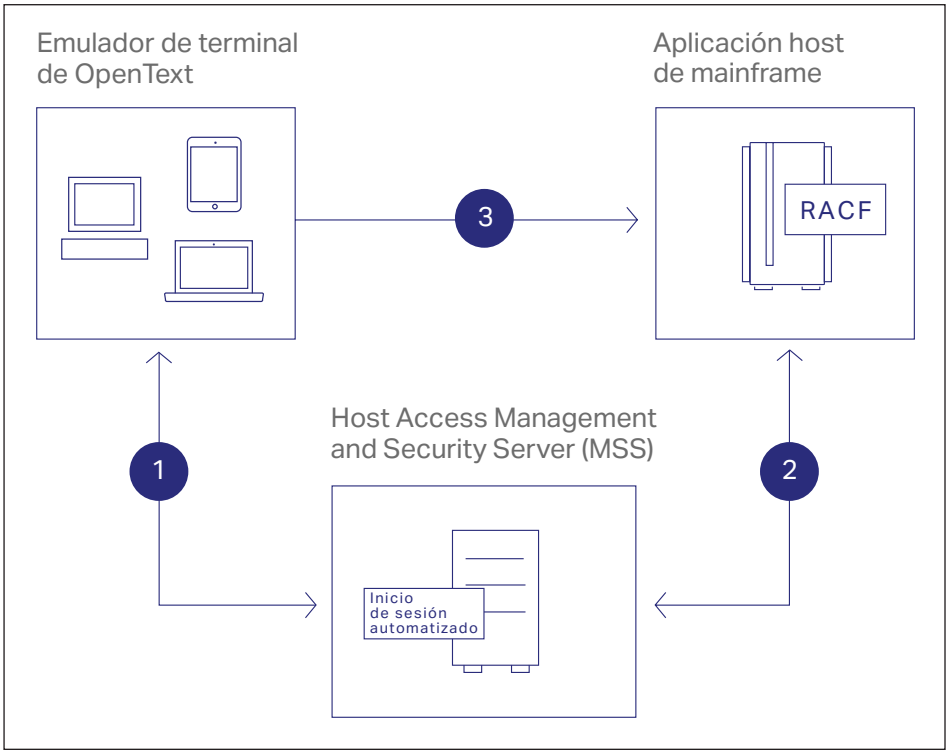
Así que tenemos dos sistemas independientes que proporcionan acceso a los recursos de la empresa. De modo que surge la siguiente pregunta: ¿por qué se necesita una autenticación muy segura para acceder a las aplicaciones empresariales, pero una autenticación débil para acceder a aplicaciones de mainframe esenciales, es decir, aquellas con las que se dirige el negocio? Es una locura.

El fin de la locura

¿Y si hubiera una forma de utilizar el sistema IAM para controlar y gestionar el acceso a su sistema host? De hecho, sí la hay. Se llama OpenText™ Host Access Management and Security Server (MSS).

MSS aporta finalmente algo de cordura a la empresa mediante la integración de su mainframe en el sistema de gestión de acceso e identidades (IAM) existente. MSS añade un punto de control de seguridad entre los usuarios que necesitan acceder al mainframe y los sistemas host. Utiliza la estructura de IAM actual, especialmente la autenticación segura, para autorizar acceso al mainframe.

MSS también proporciona un producto adicional (Automated Sign-On for Mainframe) para llevar la cordura a un nivel sin precedentes. Automated Sign-On for Mainframe ofrece un inicio de sesión automático para toda la aplicación de mainframe, de modo que los usuarios no tengan que introducir ningún ID ni contraseña. ¿Se lo imagina? No necesitaría contraseñas de mainframe nunca más.



1. El emulador inicia una sesión y solicita credenciales de usuario al sistema de inicio de sesión automatizado para acceder a la aplicación host.
2. El sistema de inicio de sesión automatizado solicita un PassTicket de un solo uso a RACF y lo envía de vuelta al emulador.
3. El emulador utiliza una credencial PassTicket de un solo uso para que el usuario se conecte a la aplicación host automáticamente.

Otros productos adicionales de MSS proporcionan más seguridad fundamental para el acceso de host:

- **MSS Security Proxy Add-On:** ofrece cifrado de extremo a extremo y aplica el control de acceso en los perímetros con una tecnología de seguridad patentada.
- **MSS Advanced Authentication Add-On:** habilita la autenticación basada en varios factores para autorizar el acceso a los valiosos sistemas host.
- **MSS PKI Automated Sign-On Add-On:** permite que las aplicaciones automatizadas PKI puedan entrar en los sistemas fundamentales de la empresa.
- **MSS Terminal ID Management Add-On:** asigna identificaciones de terminal de forma dinámica en función del nombre de usuario, el nombre DNS, la dirección IP o el repositorio de direcciones.

MSS y estos complementos aprovechan sus recursos e infraestructura existentes para que pueda utilizar aquello de lo que ya dispone para proteger y gestionar el acceso de host. Le ofrecen un valor de negocio estable a la vez que proporcionan un bajo importe total de propiedad. De esta forma, devuelven la cordura en materia de seguridad empresarial.

Más información en
www.opentext.com

Conecte con nosotros en

opentext™