CYBER READINESS
INSTITUTE

Guía de la autenticación multifactor

Siga estas directrices para comprender e implementar la autenticación multifactor en su organización

Las pequeñas y medianas empresas que buscan modos prácticos de mejorar su ciberseguridad deben implementar la autenticación multifactor (MFA) en toda su organización. Según **Microsoft**, el 99,9% de los ataques que ponen en peligro las cuentas se pueden bloquear simplemente mediante la MFA. La siguiente guía lo ayudará a familiarizarse con la MFA (también denominada autenticación de 2 factores "2FA") y lo ayudará a entender cómo implementar esta capacidad para mejorar su seguridad cibernética y la de su organización.

¿Qué es la MFA?

La MFA requiere que los usuarios presenten más de una prueba (credencial) cada vez que inicien sesión en una cuenta comercial (por ejemplo, correo electrónico de la empresa, nómina, recursos humanos, etc.). La MFA normalmente se divide en tres categorías: **algo que el usuario sabe** (una contraseña de 15 caracteres), **algo que el usuario tiene** (huella digital) o **algo que el usuario recibe** (un código enviado al teléfono o cuenta de correo electrónico del usuario).

¿Por qué es importante la AMF?

Los ciberdelincuentes quieren poner en peligro las credenciales de inicio de sesión y usarán una serie de técnicas, incluida la suplantación de identidad de su entidad financiera o socios comerciales para obtenerlas de un modo fraudulento. No obstante, si permite a sus empleados usar la MFA, protegerá la información y los datos de su empresa, además de proteger los de ellos.

El uso de contraseñas seguras de 15 caracteres es un paso fundamental, pero **la MFA ofrece una solución técnica centrada en el ser humano**. Gracias a la MFA, la contraseña del empleado ya no es la única línea de defensa cibernética de su empresa. Los piratas informáticos que pretenden robar los datos de su empresa simplemente no podrán adivinar o descifrar la contraseña de un empleado. En vez de eso, **la MFA protegerá a sus empleados y a su empresa de estos ataques**.

¿Cómo implemento la MFA?

La implementación de la MFA no requiere cambios de hardware de los ordenadores, dispositivos móviles o impresoras de su empresa. En cambio, existen numerosas herramientas gratuitas y de bajo coste basadas en software que los usuarios pueden descargar en sus dispositivos personales y de la empresa. Por ejemplo, es probable que su proveedor de correo electrónico ofrezca (y aconseje) la MFA. Por tanto, activar la MFA puede resultar tan fácil como hacer clic en una opción de su configuración.

Aún así, es posible que se pregunte cuál es el mejor modo de implementar la MFA en su plantilla. En primer lugar, debería **actualizar sus políticas y procedimientos con explicaciones específicas sobre sus expectativas**. Por ejemplo, todos los empleados deben implementar la MFA en la cuenta de correo electrónico de su empresa. A continuación, debería **celebrar sesiones de información y formación para la plantilla** en las que puede comunicar sus expectativas y políticas de MFA y explicar lo fácil que resulta el proceso para los empleados. Finalmente, debería **designar a alguien de su organización que acepte la responsabilidad de la preparación cibernética para ayudar a los empleados a solucionar problemas** a medida que comienzan a utilizar la MFA.

¿Dónde puedo obtener más información?

Ahora que tiene unos conocimientos básicos de la importancia de la MFA para su negocio y cómo puede implementarla, puede descubrir recursos y prácticas de preparación cibernética adicionales en **BeCyberReady.com**.

Acerca del CRI

El Cyber Readiness Institute es una iniciativa sin fines de lucro que reúne a líderes empresariales de todos los sectores y zonas geográficas para compartir recursos y conocimientos que impulsan el desarrollo de herramientas de ciberseguridad gratuitas para las pequeñas y medianas empresas (PYMES). Explore los elementos básicos de una buena ciberseguridad con nuestro kit básico o cree una cultura de preparación cibernética en su organización con el Programa de preparación cibernética autodirigido y disponible en línea. Nuestras guías sobre Recursos de trabajo remoto y Lugar de trabajo híbrido ofrecen consejos oportunos para abordar los cambiantes retos cibernéticos de hoy en día. Para obtener más información, visite **www.BeCyberReady.com**.