CYBER READINESS
INSTITUTE

Guía de la autenticación multifactor

El Cyber Readiness Institute (CRI) realizó recientemente una encuesta global para medir el conocimiento y la implementación de la autenticación multifactor (MFA) entre las pequeñas y medianas empresas. Descubrimos que el 55 % de las pequeñas y medianas empresas (pymes) no conocen la autenticación multifactor ni sus beneficios de seguridad. Con esta guía actualizada, pretendemos dar a conocer la autenticación multifactor entre las pymes ofreciéndoles información procesable fácil de usar que pueden poner en práctica hoy mismo para proteger sus organizaciones de la mayoría de los ciberataques.

Los ciberdelincuentes quieren confiscar 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, al exigir a sus empleados que usen la MFA, protegerá la información y los datos de su empresa, además de proteger los de ellos. 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 lugar de ello, la MFA protegerá a sus empleados y a su empresa de estos ataques.

Si busca la forma más eficaz de mejorar su ciberseguridad hoy mismo, debe implementar la MFA de inmediato en toda su organización. Si bien esta guía está escrita para la pymes, se aplica a organizaciones de todos los tamaños. 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 y a entender cómo implementar esta funcionalidad para mejorar su seguridad cibernética y la de su organización.

¿Qué es la autenticación multifactor?

La autenticación multifactor, denominada a veces "autenticación de dos factores" (2FA), es un proceso de autenticación electrónica que requiere que los usuarios verifiquen su identidad de dos o más maneras antes de conceder el acceso a sus cuentas en línea. La MFA normalmente se divide en tres categorías: algo que sabes, algo que tienes o algo que eres. Algunos ejemplos de MFA que quizás conozca son los siguientes:

1. **Autenticación por SMS o correo electrónico: recibe y utiliza un código único a través de un mensaje de texto en su teléfono móvil o por correo electrónico para demostrar su identidad.**
2. **Autenticación por software: descarga y utiliza una aplicación móvil en su teléfono para demostrar su identidad.**
3. **Autenticación biométrica: utiliza una huella dactilar o el escaneo facial para demostrar su identidad.**
4. **Notificación push: su teléfono le pedirá que permita o bloquee un intento de inicio de sesión.**

¿Mi empresa debería utilizar la MFA?

Sí, usted y todos los miembros de su empresa deberían utilizar la MFA en todas las cuentas relacionadas con sus operaciones comerciales. Por ejemplo, debe utilizar la MFA en cuentas de correo electrónico, contabilidad y recursos humanos para proteger los datos de sus clientes, socios y empleados. De hecho, si algunos de los programas o servicios que utiliza no tienen MFA, debería considerar usar una alternativa que sí tenga esta funcionalidad.

Si un ciberdelincuente obtiene acceso a sus cuentas comerciales, puede robar su dinero e información. Los ciberdelincuentes pueden cerrar su negocio durante días, semanas o más tiempo. La MFA es una forma importante de mantener su sistema a salvo de los agentes malintencionados.

¿Qué personas de mi empresa deberían usar la MFA?

Todas. La MFA debería ser obligatoria en todos los dispositivos y servicios de la empresa, especialmente en el correo electrónico y el intercambio de archivos.

¿El uso de la MFA cambia la necesidad de utilizar contraseñas seguras?

Las contraseñas seguras son una forma de autenticación y MFA se basa en otras formas (como un código de acceso de un solo uso, la huella dactilar, etc.). Cuando accede al correo electrónico del trabajo, recupera archivos de una unidad compartida o inicia sesión en cualquier servicio en línea, la contraseña con otra forma de autenticación constituye la autenticación multifactor.

¿Qué debo tener en cuenta al seleccionar una solución de MFA para mi empresa?

Es importante considerar algunos factores clave al seleccionar la solución de MFA adecuada para su empresa:

1. **¿La solución es accesible para todos los empleados, tanto si trabajan en la oficina como de forma remota?**
2. **¿Es fácil de usar?**
3. **¿Hay recursos de formación disponibles para enseñar la solución a mis empleados?**
4. **¿El proveedor ofrece soporte las 24 horas del día?**

¿Cómo implemento una política de MFA en mi empresa?

En primer lugar, el director ejecutivo debe designar un líder para gestionar el proceso de implementación de la MFA, que incluirá una campaña de mensajes y sesiones de formación para los empleados. Es importante 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.

A continuación, trabaje con el líder para determinar los sistemas y datos que deben protegerse, decidir qué tecnología de MFA es mejor para esas necesidades específicas y, finalmente, evaluar el impacto que tendrá en los empleados.

Es importante recordar que implementar la MFA en toda la organización puede entrañar desafíos, pero una comunicación clara permitirá que la implementación se realice con éxito. La celebración de sesiones informativas y cursos para los empleados en los que pueda comunicar sus expectativas y políticas de MFA y explicar lo fácil que resulta el proceso para los empleados ayudará a realizar con éxito la implementación.

¿Cómo comunico la importancia de la MFA a mis empleados?

Cree una campaña para informar a los empleados de los beneficios de utilizar la MFA y el riesgo de no hacerlo. Puede utilizar carteles físicos o anuncios publicitarios en sus edificios para explicar por qué está haciendo la transición a la MFA. Centre sus esfuerzos en informar a sus usuarios y explicar por qué está realizando este cambio, dejando claro a los empleados que la MFA está ahí para apoyarlos y proteger sus cuentas, y que no deben considerarla una molestia o una política de seguimiento en el lugar de trabajo.

¿Hay algún tipo de MFA más seguro que otros?

Hay una variedad de opciones de MFA disponibles para su empresa, pero lo más importante que debe recordar es que cualquiera de estas opciones es mejor que ninguna. Considere el tamaño de su empresa y la cantidad de empleados al seleccionar una opción de MFA que sea segura pero que no sea demasiado onerosa para los empleados.

¿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 obtener recursos y prácticas de preparación cibernética adicionales en BeCyberReady.com. Además, consulte la información gratuita de CISA para obtener información adicional sobre MFA **aquí.**

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**.