Autenticación Multifactorial

La autenticación multifactorial (MFA, por sus siglas en inglés) es un enfoque para proteger datos y aplicaciones con múltiples niveles donde un sistema requiere que el usuario presente una combinación de dos o más credenciales con el fin de verificar su identidad e iniciar sesión. MFA aumenta la seguridad porque incluso si una credencial se ve comprometida, los usuarios no autorizados no podrán cumplir con el segundo requisito de autenticación y no podrán acceder al espacio físico, el dispositivo informático, la red o la base de datos.

¿Por qué deberían los funcionarios electorales estatales y locales estar interesados en MFA?

La implementación de MFA hace que sea más difícil para un adversario obtener acceso a bases de datos seguras, aplicaciones y otros activos de infraestructura electoral. MFA puede ayudar a evitar que los adversarios obtengan acceso a los activos de su organización incluso si las contraseñas se ven comprometidas mediante ataques de phishing u otros medios.

Con mayor frecuencia, una combinación de identidad de usuario y contraseña por sí sola no brinda suficiente protección contra un inicio de sesión no autorizado. Uno de los principales inconvenientes de utilizar únicamente un sistema de identificación y contraseña es el requisito de mantener una base de datos de contraseñas.
Las técnicas para descifrar de contraseñas son cada vez más sofisticadas y la informática de alto poder es cada vez más asequible. Estos factores reducen cada día más la seguridad de los sistemas y recursos protegidos con contraseña.

¿Cómo funciona MFA?

MFA requiere que los usuarios del sistema o de la red presenten dos o más credenciales al iniciar sesión para verificar su identidad antes de que se les autorice acceso. Cada factor de autenticación adicional agregado al proceso de inicio de sesión aumenta la seguridad. Un inicio de sesión típico de MFA debe requerir que el usuario presente alguna combinación de los siguientes elementos:

- **Algo que usted sabe:** Como una contraseña, número de identificación personal (PIN, por sus siglas en inglés)) o respuestas a preguntas de seguridad;
- **Algo que usted tiene:** Como una tarjeta inteligente, un token móvil o un token de hardware; y
- **Alguna forma de factor biométrico** (p. ej., huella digital, reconocimiento de voz)

Por ejemplo, MFA puede requerir que los usuarios inserten una identificación de tarjeta inteligente en un lector de tarjetas (primer factor) y luego ingresen una contraseña (segundo factor). Un usuario no autorizado en posesión de la tarjeta no podría iniciar sesión sin conocer también la contraseña; asimismo, la contraseña es inútil sin acceso físico a la tarjeta.

La seguridad adicional que ofrece MFA puede simplificar el proceso de inicio de sesión del usuario mediante el uso de inicio de sesión único de ser posible. Un sistema de inicio de sesión único permite a los usuarios autenticados acceder a un entorno desde el cual pueden usar varias aplicaciones protegidas, sin necesidad de iniciar sesión por separado cada vez.

Considere implementar una capacidad de MFA para proteger los sistemas de registro de votantes, los sistemas de informes de la noche de las elecciones u otros sistemas de IT de las oficinas electorales. Los cronogramas y costos de implementación varían según la solución de MFA que su organización elija y los activos que proteja.
Estas opciones van desde implementar un entorno de inicio de sesión único hasta complementar un sistema existente de inicio de sesión basado en contraseña con un segundo factor de autenticación, como un código único de uso por tiempo limitado entregado a través de un token o de un generador de aplicaciones para teléfonos inteligentes.