EVALUACIÓN

# Evaluación de riesgos: Seguridad de Multi-Factor Authentication (MFA)

*Descubra la escala de riesgos de las soluciones de autenticación actuales*

El ochenta por ciento de las filtraciones relacionadas con el pirateo informático implican el robo de credenciales de usuario o descuidos relacionados con las contraseñas[1]. Más de 613 millones de contraseñas han quedado expuestas a través de infracciones de datos[2]. Incluir la autenticación multifactorial (MFA) como capa de seguridad adicional para iniciar sesión puede reducir considerablemente el riesgo, aunque la mayoría de las soluciones de MFA tradicionales todavía pueden verse comprometidas con relativa facilidad.

**¿Cuál es el grado de madurez de la seguridad de autenticación en su organización? Descubra los riesgos de los modelos de autenticación actuales:**

# Riesgo más alto

Autenticación mediante nombre de usuario y contraseña


Las organizaciones que dependen únicamente de la seguridad de las credenciales para una autenticación segura son muy vulnerables a los ataques. Los nombres de usuario y las contraseñas son menos seguros que nunca. Los atacantes, muy entregados, roban los datos de acceso, los piratean y los recopilan para luego monetizarlos rápidamente y utilizarlos o venderlos en la Dark Web.

Cómo eluden los agentes maliciosos los nombres de usuario y las contraseñas:

- **Credential Stuffing**
- **Phishing**
- **Aplicación de contraseñas**
- **Fuerza bruta**
- **Anterior filtración de datos/contraseñas reutilizadas**
- **Restablecimiento de contraseña**
- **Registro de pulsaciones de teclas**
- **Descubrimiento local**

El hecho de que los usuarios tiendan a repetir las contraseñas en varios sitios supone una amenaza aún mayor para la seguridad de la empresa; por lo tanto, usted estará igual de expuesto que la cuenta personal menos segura de sus usuarios. Las vulnerabilidades inherentes incluso a las contraseñas más complejas generadas por algoritmos confirman la necesidad de la MFA. En definitiva, nunca es recomendable confiar en un solo nivel de seguridad, como la autenticación de factor único en este caso. La mejor seguridad siempre constituye varias capas de defensa.

# Riesgo medio-alto

Autenticación multifactorial (MFA) estándar


Incorporar la función de MFA a su infraestructura de seguridad de autenticación aumentará de forma inmediata la seguridad de su empresa. MFA, que incluye la autenticación de dos factores (2FA), requiere un mínimo de dos factores de autenticación distintos para verificar a un usuario. El primer factor suele ser una contraseña. El segundo (y posiblemente tercer) factor podría ser algo que usted conozca, como un PIN o una pregunta de seguridad; algo que usted tenga, como un dispositivo, un código/contraseña de un solo uso o un token de hardware/software; o algo más personal, entre los que se incluyen datos biométricos como la huella dactilar, la detección facial o señales contextuales como la ubicación.

Aunque la MFA tradicional reduce en gran medida el riesgo en comparación con la autenticación de factor único de nombre de usuario/contraseña, sigue siendo vulnerable ante diversos métodos para eludir la seguridad de autenticación:

- **Phishing**
- **Uso de proxies transparentes (ataques de tipo intermediario [MITM])**
- **Interceptación del código de autenticación por correo electrónico o SMS**
- **Credential Stuffing**
- **Ataques de repetición**
- **Intercambio de SIM**
- **Ingeniería social**
- **Vulnerabilidades en páginas online que trabajan con MFA**

Existen muchos ejemplos bien documentados de atacantes que eluden la autenticación multifactorial. Una de dichas infracciones de mayor repercusión de 2020 se llevó a cabo mediante la combinación de ingeniería social y phishing para eludir una solución de MFA, y podría haberse evitado con el uso de claves de seguridad física.

# Riesgo más bajo

MFA con FIDO2 mediante clave de seguridad física


FIDO2 es el método de autenticación basado en estándares más sólido disponible y resuelve las vulnerabilidades de seguridad de la MFA tradicional, lo que elimina los riesgos de phishing, así como los ataques de tipo intermediario (MITM) y de repetición. El estándar FIDO2 consta de la especificación de autenticación web del consorcio del World Wide Web y el correspondiente protocolo de autenticación de FIDO Alliance. Este modelo de autenticación abre las puertas al futuro de la MFA: la autenticación mediante credenciales criptográficas para iniciar sesión que nunca salen del dispositivo del usuario ni se almacenan en un servidor. FIDO2 también respalda la posible evolución hacia una autenticación sin contraseñas.

El inconveniente es que la única manera de habilitar la MFA con FIDO2 es adquirir claves de seguridad físicas para que cada usuario las utilice como factor de autenticación.

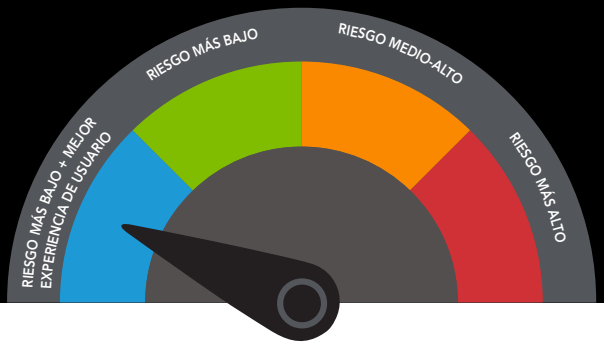
Aunque FIDO2 es el estándar más seguro, la implementación mediante claves de seguridad físicas puede plantear bastantes desafíos:

- **Coste de adquisición y mantenimiento de claves de cada usuario**
- **Complejidad de distribución y gestión de las claves**
- **Sustitución de claves físicas perdidas**
- **Incapacidad para actualizar o parchear claves físicas**
- **Distribución desigual: solo ciertos empleados obtienen claves**

La adquisición, configuración, expedición y gestión de claves físicas para todos los empleados es costoso y requiere mucho tiempo. Además, exigir a los usuarios que conecten una clave física en su dispositivo para cada inicio de sesión disminuye la productividad, puesto que contribuye a una experiencia de usuario compleja.

# Riesgo más bajo + mejor experiencia de usuario

MFA de última generación en el borde de Internet




Akamai MFA es una solución con FIDO2 de última generación que incluye un factor de autenticación a prueba de phishing y protegido por criptografía. El servicio emplea una aplicación para smartphone en lugar de una clave de seguridad física, lo que resuelve los problemas que a menudo impiden a las empresas implementar la MFA con FIDO2. Se puede implementar de forma rápida y sencilla a través de un smartphone existente para ofrecer el máximo nivel de seguridad de autenticación y una experiencia de usuario impecable. Akamai MFA elimina el riesgo de suplantación de identidad y respalda la posible evolución hacia el futuro de la autenticación sin contraseña.

Obtenga más información sobre Akamai MFA y solicite una prueba gratuita de 60 días en este enlace: **akamai.com/mfa**.

## Fuente:

1. https://www.infosecurity-magazine.com/blogs/pwned-passwords-business-risk/
2. https://haveibeenpwned.com/Passwords

Akamai garantiza experiencias digitales seguras a las empresas más importantes del mundo. La plataforma inteligente de Akamai en el borde de Internet llega a todas partes, desde la empresa a la nube, para garantizar a nuestros clientes y a sus negocios la máxima eficacia, rapidez y seguridad. Las mejores marcas del mundo confían en Akamai para lograr su ventaja competitiva gracias a soluciones ágiles que permiten destapar todo el potencial de sus arquitecturas multinivel. En Akamai mantenemos las decisiones, las aplicaciones y las experiencias más cerca de los usuarios que nadie; y los ataques y las amenazas, a raya. La cartera de soluciones de seguridad en el Edre, rendimiento web y móvil, acceso empresarial y distribución de vídeo de Akamai está respaldada por un servicio de atención al cliente y análisis excepcional, y por una supervisión ininterrumpida, durante todo el año. Para descubrir por qué las marcas más importantes del mundo confían en Akamai, visite www.akamai.com, blogs.akamai.com, o siga a @Akamai en Twitter. Puede encontrar los datos de contacto de todas nuestras oficinas en www.akamai.com/locations. Publicado el 21 de marzo.