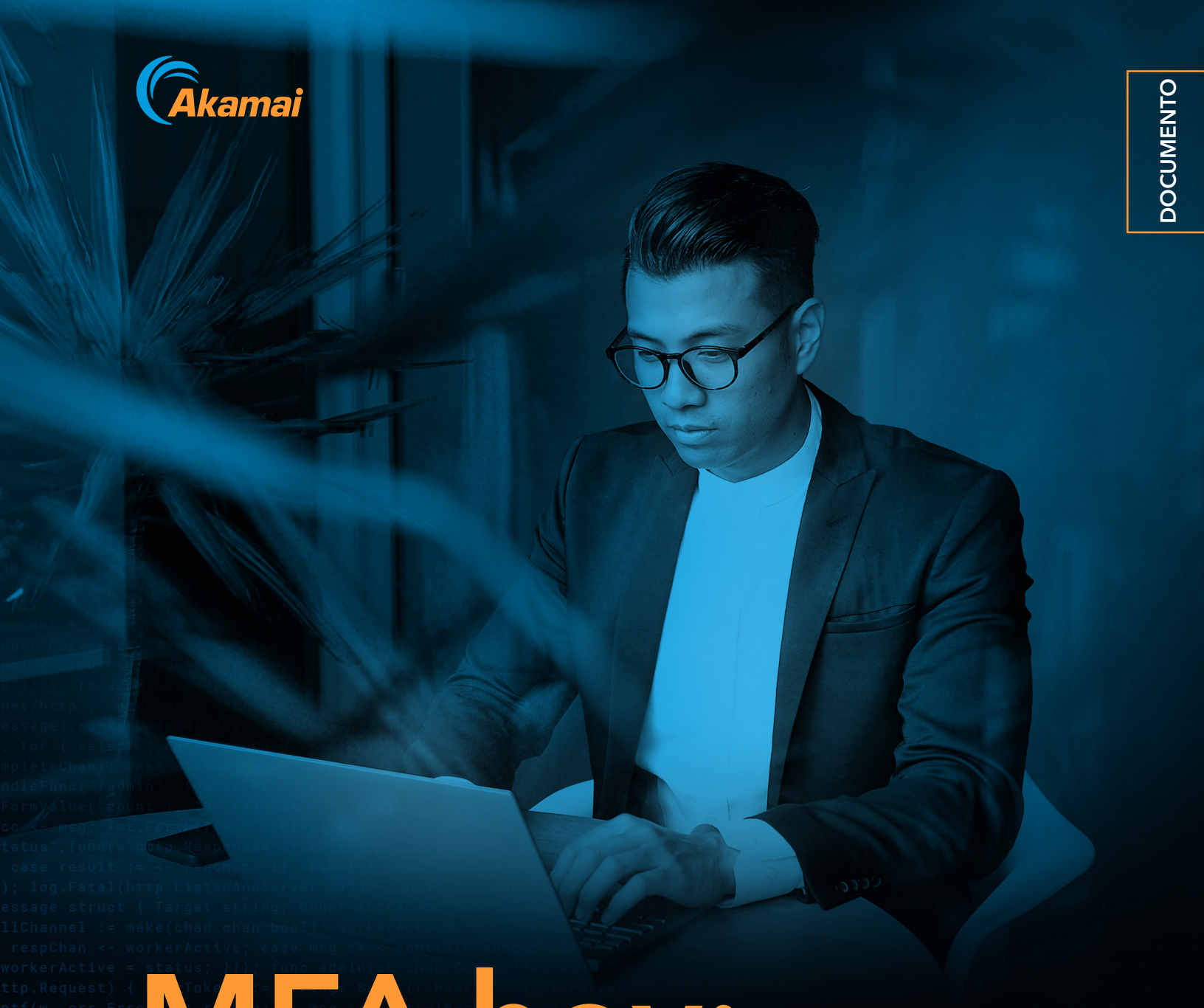
Akamai

DOCUMENTO



MFA hoy: ¿un espejismo de seguridad?

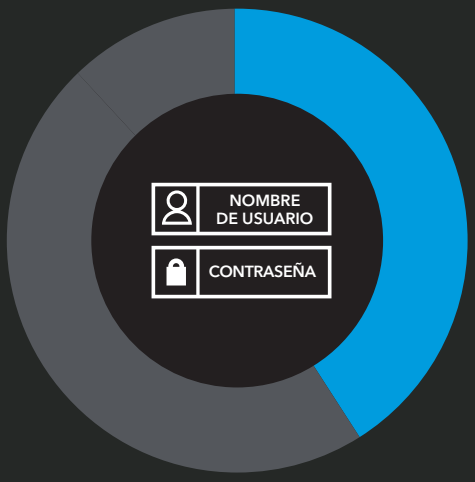
Los nombres de usuario y las contraseñas no son suficientes

El 80 % de las filtraciones de seguridad está relacionado con el uso de credenciales robadas.[1] Si bien se debe en parte a descuidos en relación con las contraseñas, incluso las contraseñas más complejas e indescifrables generadas por algoritmos son vulnerables.[2] Una auditoría reciente en la Dark Web descubrió 15 000 millones de inicios de sesión ilegítimos a partir de 100 000 vulneraciones.[3]

El imperativo de la conectividad digital, la dependencia de los servicios en la nube y la realidad de los entornos híbridos, junto con la excesiva confianza en las contraseñas, dejan a los usuarios en una posición vulnerable ante innumerables vectores de ataque de autenticación:

- **Credential Stuffing**
- **Ataques de rociado de contraseñas ("password spraying") y otros mecanismos de fuerza bruta**
- **Exhibición local y esfuerzos internos**
- **Phishing e ingeniería social**
- **Registro de pulsación de tecla**
- **Proxy malicioso y campañas de respuesta**

La pandemia mundial no ha hecho más que agravar la situación y ha puesto de manifiesto la necesidad del acceso seguro independiente de la ubicación y del dispositivo. Teniendo en cuenta que el 100 % de las infracciones relacionadas con las credenciales ocurre después de la autenticación del usuario, parece evidente que las contraseñas no están cumpliendo su función de autenticación segura.



A pesar de sus conocidas debilidades, el 41 % de las organizaciones aún cree que los nombres de usuario y las contraseñas son una de las herramientas de gestión del acceso más eficaces.[4]

---

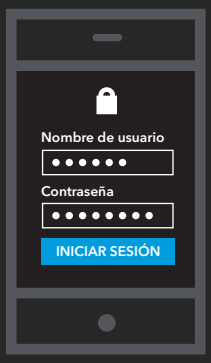
500 %

Akamai ha observado que los ataques de phishing, ingeniería social, Credential Stuffing y fuerza bruta van en aumento. Entre marzo y mayo de 2020, el malware experimentó un aumento de casi un 500 %.

Los beneficios de MFA

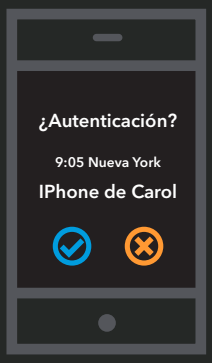
En este contexto, no es de extrañar que la popularidad de la tecnología de autenticación multifactorial (MFA) siga una trayectoria ascendente. En pocas palabras, MFA protege a las empresas mediante el uso de más de una fuente de validación para verificar la identidad antes de permitir el acceso.

La tecnología MFA requiere la combinación con éxito de al menos dos de estas tres credenciales de autenticación:



Algo que sabe

Autenticación basada en el conocimiento. Puede ser una contraseña, un PIN, la respuesta a una pregunta de seguridad o incluso una fotografía.



Algo que tiene

Autenticación basada en token (de hardware o software). Puede ser una tarjeta inteligente o un token de seguridad (key fob), o bien una contraseña de un solo uso, una notificación push o un código SMS recibido en un dispositivo móvil.

Algo que es

Autenticación contextual o biométrica. Puede ser una acción, señales de ubicación o temporales, una huella dactilar, el reconocimiento facial, un patrón de voz o una firma.

La implementación de una solución MFA reduce significativamente el riesgo de acceso no autorizado y vulneraciones del sistema. De hecho, las organizaciones que utilizan MFA tienen un 99,9 % menos de probabilidades de sufrir un ataque que aquellas que no lo hacen.[5] MFA hace posible y agiliza el acceso seguro en todos los entornos: aplicaciones en la nube, en las instalaciones, basadas en la Web, SaaS e IaaS. Una solución MFA también es un componente fundamental para migrar la seguridad empresarial a marcos como Zero Trust y SASE.

Al requerir algo más que un nombre de usuario y una contraseña, unificar la experiencia de inicio de sesión e integrarse con otras herramientas de seguridad nativas de la nube, las tecnologías MFA también tienen el potencial de aumentar la facilidad de uso y la productividad del usuario. Es más, la gestión centralizada de la autenticación resuelve muchas preocupaciones y satisface muchos requisitos relacionados con el cumplimiento.

Las soluciones MFA tradicionales no son tan seguras como se cree

Un hacker puede manipular fácilmente un servicio MFA basado en una notificación push estándar para apropiarse de la cuenta. A menos que se refuerce con medidas de seguridad adicionales, las actuales tecnologías MFA suponen cierto nivel de riesgo.

MFA es un método de seguridad perimetral, pero la nube y el estilo de trabajo actual no tienen perímetro. La tecnología MFA no está diseñada para detener ataques no relacionados con inicios de sesión. Solo protege el inicio de sesión en el perímetro, cuando el usuario intenta acceder al sistema. Los cibercriminales han desarrollado mecanismos de ingeniería social y phishing relativamente simples pero altamente eficaces para sacar partido de esta realidad.

Considere esta situación:

1. **Como resultado de alguna forma de ingeniería social, un empleado introduce un nombre de usuario y una contraseña reales en un sitio falso (phishing) configurado por un atacante.**
2. **Una vez obtenidas las credenciales, el atacante las utiliza en el portal de inicio de sesión real.**
3. **Esto genera el envío de una notificación push al teléfono del empleado.**
4. **El empleado acepta la notificación push como parte del proceso habitual de inicio de sesión.**
5. **El atacante ha completado dos formas de verificación y se le ha concedido acceso.**

Este es el punto débil de seguridad crítico de una notificación push estándar: cualquier atacante con un conjunto de credenciales robadas puede lograr enviar notificaciones push al teléfono de un empleado. Lo único que se interpone entre una violación de seguridad y el curso normal de la actividad empresarial es la capacidad del empleado de distinguir una notificación push legítima de una estafa. Entre miles de empleados, basta con el fallo de uno de ellos para que el atacante acceda al sistema.

MFA a prueba de phishing

Una solución MFA realmente segura utiliza los estándares FIDO2. En el nivel más básico, esto significa que la tecnología proporciona la seguridad en lugar de depender de las decisiones del usuario.

¿Cómo es esto posible? Los estándares FIDO2 utilizan un par de técnicas que evitan el phishing.

En primer lugar, la solicitud de autenticación (el desafío de MFA) siempre se envía a la estación de trabajo donde se originó la solicitud de acceso. El navegador de esa estación de trabajo dirigirá la solicitud de autenticación a cualquier clave de seguridad vinculada localmente. En el escenario descrito anteriormente: en lugar de que el atacante consiga que el servicio MFA envíe la notificación push al teléfono del empleado, el desafío de MFA volverá a la estación de trabajo del atacante. Dado que el atacante no tiene la clave de seguridad del empleado, no hay posibilidad de respuesta. De este modo, se impide el robo de la cuenta.

Definición: estándares y especificaciones de autenticación

Fast IDentity Online (FIDO) Alliance

Organismo responsable del desarrollo, uso y cumplimiento de los estándares de autenticación.

FIDO2

Término general para el conjunto más reciente de especificaciones de autenticación de FIDO Alliance. Los estándares que se incluyen son CTAP1, CTAP2 y WebAuthn. El estándar FIDO2 permite a los usuarios utilizar dispositivos habituales para autenticarse fácilmente en servicios online tanto en entornos móviles como de escritorio.

WebAuthn

Un estándar web publicado por el World Wide Web Consortium (W3C) que es un componente principal de FIDO2. El objetivo del proyecto es estandarizar una interfaz para autenticar a los usuarios en aplicaciones y servicios basados en la Web mediante el uso de criptografía de clave pública.

Protocolo CTAP (Client to Authenticator Protocol)

Especificación desarrollada por FIDO Alliance que permite la comunicación segura entre un autenticador de roaming (como un smartphone) y un autenticador interno (el cliente o la plataforma).

En segundo lugar, el navegador envía datos a la clave de seguridad junto con la solicitud de autenticación. Estos datos incluyen el nombre de dominio del origen que envió la solicitud de autenticación, tal como lo ve el navegador. Si el atacante simplemente enviara la solicitud de autenticación recibida a la estación de trabajo del empleado, estos datos incluirían el nombre de dominio del sitio de phishing. La clave de seguridad reconocería la discrepancia entre el nombre de dominio del sitio que registró originalmente y el nombre de dominio que solicita la autenticación y se negaría a responder. Una vez más, se impide el ataque.

Si una MFA más segura a prueba de phising es posible, ¿por qué no se aplica de forma generalizada? Se requieren claves de seguridad físicas, que son costosas y complejas. O al menos, se requerían hasta ahora.

MFA de última generación en el borde de Internet

Para los departamentos de TI, la evaluación e implementación de tecnologías MFA ha supuesto un gran desafío. Para lograr una seguridad óptima, deben gastar más en la implementación de hardware, la compra de claves de seguridad físicas para cada empleado y la gestión, distribución y operación de todas las claves. Deben además lograr que todos los usuarios acepten de buen grado la experiencia poco ideal que estas suponen: el uso y seguimiento de otra pieza más de hardware.

La alternativa es un nivel menor de seguridad con cómodas notificaciones push que reciben los empleados en sus smartphones y que no suponen un coste adicional. Por esto último es por lo que la MFA con notificaciones push está actualmente tan extendida. Y por eso mismo, son muchas las empresas en riesgo de sufrir un ataque.

Pero ya no es necesario tener que elegir entre la seguridad y el coste y la facilidad de adopción.

El servicio Akamai MFA presenta un nuevo factor de autenticación. Digitaliza la seguridad de FIDO2 con tan solo un smartphone y un navegador web, sin dejar de lado la experiencia familiar y sencilla de las notificaciones push, y se puede utilizar en cualquier plataforma como autenticador de roaming. No se requieren claves de seguridad físicas. La solución ofrece las funcionalidades más seguras de los estándares FIDO2 a un bajo coste, con facilidad de instalación y uso, así como interoperabilidad con proveedores de identidad habituales.

Proteja a su organización contra el phishing, el Credential Stuffing y el robo de cuentas con Akamai MFA. Obtenga más información acerca de la primera y revolucionaria tecnología MFA de Akamai y prepárese para un futuro realmente seguro y sin contraseñas.

Obtenga más información en akamai.com/mfa.

Fuente:

1. https://enterprise.verizon.com/resources/reports/dbir/
2. https://www.infosecurity-magazine.com/opinions/problem-password-everything-1/
3. https://www.forbes.com/sites/daveywinder/2020/07/08/new-dark-web-audit-reveals-15-billion-stolen-logins-from-100000-breaches-passwords-hackers-cybercrime/?sh=27fa6368180f
4. https://www.businesswire.com/news/home/20200616005047/en/Weakest-Link-Prevails-Overreliance-Passwords-Continues-Compromise
5. https://www.hipaajournal.com/multi-factor-authentication-blocks-99-9-of-automated-cyberattacks/