KnowBe4

Cómo puede ser hackeada su MFA: por qué los ciberdelincuentes están usando la ingeniería social

Debido a las décadas de ataques exitosos contra métodos de autenticación de un solo factor, como nombres de usuario y contraseñas, se está generando un movimiento a gran escala hacia soluciones de autenticación multifactor (multi-factor authentication, MFA) más seguras. Esta tendencia se ha observado, en los últimos años, en los servicios y sitios web más populares, incluidos los que son propiedad de Google, Microsoft, Facebook y X, que ahora ofrecen tanto soluciones tradicionales de nombre de usuario y contraseña como opciones de MFA más seguras.

Anteriormente, la MFA era utilizada por organizaciones y sitios web que requerían la mayor garantía de seguridad. En la actualidad, los tokens de MFA son comunes y cuestan tan solo unos dólares por dispositivo.

La amplia adopción de la MFA es una excelente noticia para la seguridad cibernética y ayudará a derrotar muchas amenazas que, de lo contrario, podrían tener más éxito contra soluciones de autenticación de un solo factor. Dicho esto, la capacidad de la MFA para reducir el riesgo de seguridad informática ha sido exagerada por muchos proveedores y defensores, lo que hace creer erróneamente que la aplicación de la MFA implica que todos los ataques que tuvieron éxito contra la autenticación de un solo factor no pueden tener éxito contra la MFA. Por ejemplo, muchos administradores y usuarios de la MFA creen que el phishing por correo electrónico ya no es una amenaza porque los usuarios no pueden ser engañados para proporcionar sus credenciales de inicio de sesión. Esto no es así.

Si bien la MFA reduce riesgos específicos de seguridad informática, muchos ataques que podrían tener éxito contra la autenticación de un solo factor también pueden tenerlo contra soluciones de MFA. En definitiva, aunque las soluciones de MFA son más seguras que las soluciones de autenticación de un solo factor, no son infalibles.

Cómo se hackea la autenticación multifactor

Existe más de una docena de formas de hackear soluciones de MFA. Independientemente de las afirmaciones de los proveedores de soluciones de MFA, todas son vulnerables a ciertos métodos de hackeo. En general, a medida que una MFA se hace más segura, más difícil se vuelve para el usuario final utilizarla. La seguridad siempre implica un compromiso entre usabilidad y seguridad, y la MFA no es la excepción.

Las tácticas para hackear soluciones de MFA se pueden agrupar en cuatro métodos principales: ingeniería social, manipulación técnica, ataque físico y mixto.

Ingeniería social	Manipulación técnica	Ataques físicos	Mixto
La ingeniería social implica que el usuario final utiliza la solución de MFA de forma tal que, sin querer, da lugar a su elusión o uso indebido.	La manipulación técnica se refiere a los métodos de explotación y manipulación que no dependen de que el usuario humano cometa errores.	Ataques físicos, como copiar huellas dactilares de dispositivos físicos/teclados.	Muchos métodos de hackeo de MFA combinan dos o más de estos métodos, aunque la gran mayoría requiere ingeniería social junto con un ataque técnico.

Aquí se encuentran las 15 tácticas principales que los ciberdelincuentes pueden usar para hackear las MFA, agrupadas según los cuatro métodos principales mencionados anteriormente.

Hackeos de ingeniería social

- Falsificar la autenticación.
- Ataques a preguntas de recuperación.
- Soporte técnico de ingeniero social.

Hackeos técnicos

- Predicción de identificador único de sesión.
- Ataque de hacker en el punto final.
- Modificación maliciosa de software o hardware de MFA.
- Generadores de códigos duplicados.
- Ataques de skimming.
- Secuestros de sujeto.
- Ataques de fuerza bruta.
- MFA con errores.
- Ataques físicos.

Hackeos Mixtos

- Secuestro de sesión.
- Ataques de cambio de SIM.
- Ataques de degradación de recuperación.

El elemento humano en el hackeo de MFA: tácticas de ingeniería social

De los cuatro métodos principales utilizados para evadir la MFA, la ingeniería social representa el desafío más singular. Las tácticas de ingeniería social y phishing se han convertido en herramientas altamente efectivas en el arsenal de hackers y ciberdelincuentes que buscan comprometer la MFA. Ahora, los ciberdelincuentes aprovechan la manipulación psicológica y las técnicas engañosas para explotar las vulnerabilidades humanas y evadir esta medida de seguridad avanzada.

El phishing, una técnica de ingeniería social prevalente, implica engañar a las personas para que divulguen información delicada, como nombres de usuario, contraseñas o incluso códigos de MFA. Los ciberdelincuentes a menudo emplean diversos medios, como correos electrónicos, mensajes de texto o llamadas telefónicas, para hacerse pasar por entidades confiables y crear un sentido de urgencia o miedo para que las víctimas actúen precipitadamente y sin pensar. Al imitar la comunicación legítima de bancos, proveedores de servicios o colegas, los atacantes manipulan a las personas para que entreguen sus credenciales y tokens de MFA sin darse cuenta.

Una táctica de phishing común es la creación de sitios web engañosos que se asemejan mucho a los legítimos. Los usuarios desprevenidos, pensando que están accediendo a un servicio conocido, ingresan sus credenciales y códigos de MFA, y proporcionan a los ciberdelincuentes, sin saberlo, las claves para eludir

las capas de seguridad. Los atacantes también pueden usar campañas de phishing por correo electrónico, enviar mensajes aparentemente auténticos que instan a los destinatarios a hacer clic en enlaces maliciosos o descargar archivos adjuntos infectados. Una vez que la víctima interactúa con estos elementos, su información delicada se ve comprometida.

Otro camino que explotan los ciberdelincuentes es la tendencia humana a confiar en figuras de autoridad. Al hacerse pasar por personal de soporte de TI, gerencia o colegas, los hackers pueden manipular a las personas para que proporcionen códigos de MFA u otros datos de autenticación bajo el pretexto de medidas de seguridad necesarias. Esta técnica de ingeniería social se aprovecha de la inclinación natural a seguir instrucciones de figuras de autoridad percibidas y logra eludir las protecciones que la MFA pretende aplicar.

Cómo defenderse de ataques contra la MFA

Las MFA son un componente crítico de las estrategias modernas de ciberseguridad, pero no son infalibles. La MFA no previene el phishing o los ataques de ingeniería social, por lo que es crucial, al usar o considerar la MFA, que la capacitación en concientización sobre seguridad sea un componente clave de su estrategia de seguridad general.

A continuación, encontrará un resumen de las defensas clave de ingeniería social y técnica que su organización debe considerar al usar la MFA.

Defensas sociales

Es crucial que las organizaciones y las personas prioricen la educación y concientización en ciberseguridad. Los programas de capacitación que enseñan a los usuarios a reconocer intentos de phishing, verificar la autenticidad de la comunicación y adoptar un escepticismo saludable pueden reducir significativamente la tasa de éxito de los ataques de ingeniería social. Implementar sistemas avanzados de detección de amenazas que analicen el comportamiento del usuario y los patrones de comunicación también puede mejorar la posición de seguridad general, e identificar y mitigar posibles amenazas antes de que comprometan información delicada.

Además, la capacitación en concientización sobre seguridad mejora la comprensión de los usuarios sobre la importancia de la autenticación multifactor. Los participantes aprenden cómo la MFA agrega una capa adicional de seguridad al requerir múltiples formas de identificación, como contraseñas y códigos temporales. Este conocimiento fomenta una apreciación por las medidas de protección vigentes y anima a las personas a seguir las prácticas recomendadas al utilizar la MFA, lo que reduce la probabilidad de ser víctima de manipulación.

Aquí hay seis puntos clave para recordar:

- Comprender que no hay nada, incluida cualquier solución de MFA, que sea infalible.
- Integrar la concientización sobre el hackeo de MFA en la capacitación en concientización sobre seguridad.
- No caer en engaños haciendo clic en enlaces fraudulentos.
- Bloquear los enlaces fraudulentos tanto como sea posible.
- Asegurarse de que los usuarios sepan que una URL es legítima antes de hacer clic.

Defensas técnicas

- Habilitar la MFA REQUERIDA siempre que sea posible.
- Evitar usar la MFA basada en SMS siempre que sea posible.
- Utilizar soluciones de MFA "1:1", que requieren que el cliente esté registrado previamente con el servidor.

- Utilizar/requerir autenticación bidireccional, mutua, siempre que sea posible.
- ¿Su solución de MFA combate específicamente el robo de tokens de sesión y/o los ataques de reproducción maliciosos (es decir, resistente a la reproducción)?
- ¿El soporte de su proveedor de MFA puede ser manipulado mediante ingeniería social?
- Asegurarse de que los proveedores de MFA utilicen el ciclo de vida de desarrollo seguro (secure development lifecycle, SDL) en su programación.
- Asegurarse de que la MFA tenga habilitada la "limitación de intentos fallidos" o el "bloqueo de cuenta".
- Distribuir los factores en diferentes "canales" o "bandas" (dentro o fuera de banda).
- Proteger y auditar los atributos de identidad utilizados por la MFA para la identificación única de los inicios de sesión de MFA.
- No responder a las preguntas de restablecimiento de contraseña con respuestas honestas.
- Fomentar y utilizar sitios y servicios que utilicen autenticación dinámica, donde se soliciten factores adicionales para circunstancias de mayor riesgo.
- Comprender los riesgos de los sistemas de "secreto compartido".
- Para la autenticación basada en transacciones, es necesario enviar al usuario todos los detalles críticos fuera de banda antes de que se transmita/requiera la confirmación.

Conclusión

Los hackers y ciberdelincuentes continúan explotando tácticas de ingeniería social y phishing para eludir la autenticación multifactor. A medida que avanza la tecnología, también lo hacen los métodos empleados por los adversarios. Reconocer la importancia de los factores humanos en ciberseguridad e implementar programas de concientización y capacitación integrales son pasos esenciales para fortalecer las defensas contra estas amenazas.

OBTENGA MÁS INFORMACIÓN

Contáctenos para obtener más información sobre cómo la capacitación en concientización sobre seguridad puede fortalecer sus defensas cibernéticas.

KnowBe4 Brazil | Av. Ibirapuera, 2315, Indianópolis, CEP 04029-200 | São Paulo-SP | Tel.: +55 (0800) 761-2668 | www.KnowBe4.com | Correo electrónico: Sales@KnowBe4.com