yubico

Por qué la estrategia de autenticación multifactor (MFA) de tu móvil atrae a los ciberdelincuentes y cómo evitarlo

Estamos en un momento de crisis para la ciberseguridad. Durante la crisis sanitaria de la COVID, los ciberataques se dispararon en un 300%.[1] En 2020, se produjo un secuestro de datos cada 10 segundos,[2] y los casos de phishing se duplicaron.[3] El coste medio de una violación de seguridad de datos alcanzó su cifra más alta en 17 años en 2021, llegando a los 4.24 millones de dólares.[4]

A pesar de la creciente frecuencia y sofisticación de los ciberataques, muchas compañías siguen utilizando métodos de autenticación multifactor (MFA) tradicionales como nombres de usuario y contraseñas, y autenticación vía teléfono móvil, para proteger el acceso a aplicaciones y datos sensibles. En estas compañías, los resultados son inesperados: ataques que penetran en sus defensas y empleados frustrados.

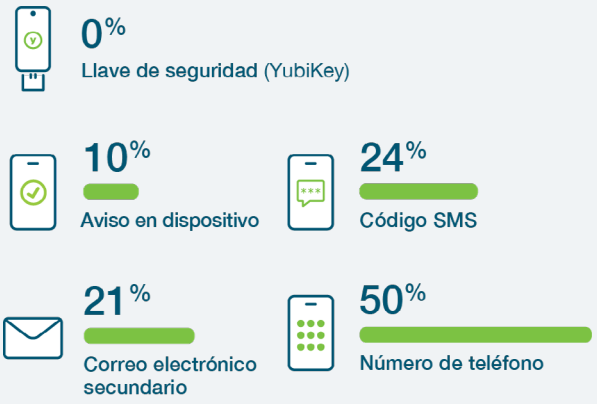
Por qué la autenticación vía teléfono móvil pone en riesgo a tu compañía

Si bien cualquier forma de MFA proporciona una mayor seguridad que la autenticación tradicional basada en nombre de usuario y contraseña, no todas las formas de MFA son iguales. De hecho, los métodos de MFA como los SMS, las contraseñas de un solo uso (OTP) y las notificaciones push son altamente susceptibles al phishing, ataques de intermediario (MiTM), malware, duplicación de SIM, y las apropiaciones de cuenta.

La omnipresencia y facilidad de acceso a los dispositivos móviles es precisamente lo que los hace tan susceptibles al phishing. En la MFA vía teléfono móvil, no existen garantías de que la clave privada vaya a acabar en un lugar seguro en el dispositivo móvil. Los dispositivos móviles están altamente expuestos a ataques a través de aplicaciones, comunicación, sistemas operativos y la tecnología Secure Element. Hoy en día, cada vez más, los hackers roban OTP y notificaciones push interceptándolas o mediante phishing, de manera que delincuente y el robo de la cuenta son invisibles para el usuario.

Investigaciones conducidas por Google, la Universidad de Nueva York y la Universidad de California San Diego a partir de 350,000 intentos reales de secuestro de datos demostraron que la autenticación por SMS y vía teléfono móvil no resulta demasiado efectiva a la hora de prevenir robos de cuenta.[5] La investigación descubrió que una OTP vía SMS solo bloqueaba el 76% de los ataques dirigidos, mientras que las notificaciones automáticas solo bloqueaban el 90%. Esto quiere decir que hay un índice de un 10% de ataques exitosos como mínimo. Teniendo esto en cuenta, no se trata de si seremos víctimas de un ataque, sino de cuándo lo seremos.

Riesgo de secuestro de cuenta según tipo de seguridad



Además de ser menos segura, la autenticación vía teléfono móvil no es fácil de usar para el usuario. Cuando se emplea la autenticación vía teléfono móvil como los SMS o las OTP en la autenticación de dos factores (2FA) o la MFA, los empleados deben esperar para recibir e introducir los códigos proporcionados por SMS o aplicaciones de autenticación. Todo esto depende de la disponibilidad de conectividad móvil, que el teléfono esté suficientemente cargado, y otros matices que pueden afectar a la experiencia del usuario. A esto hay que añadir que el tiempo y la complejidad del proceso de autenticación reducen la productividad de los empleados, a la vez que exponen a la compañía.

[1] Rachel England, FBI Sees Cybercrime Reports Increase Fourfold During COVID-19 Outbreak, (20 de abril de 2020)

[2] Phil Muncaster, One Ransomware Victim Every 10 Seconds in 2020, (25 de febrero de 2021)

[3] Internet Crime Complaint Center, 2020 Internet Crime Report, (17 de marzo de 2021)

[4] IBM Security, Cost of a Data Breach Report, (28 de julio de 2021)

[5] Kurt Thomas et Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (17 de mayo de 2019)

La autenticación vía teléfono móvil también deja áreas expuestas en el marco de la MFA

Aunque las compañías pueden dar prioridad o incluso obligar a usar MFA vía teléfono móvil, hay casos en los que los empleados no pueden o no quieren usar la autenticación vía móvil. No sólo porque puede haber poca cobertura móvil en algunas zonas geográficas, sino también porque los empleados pueden negarse a utilizar dispositivos personales para trabajar o no quieren permitir a los administradores acceder a sus dispositivos. También pueden darse restricciones o requisitos de cumplimiento, y algunos empleados quizá no sepan utilizar un smartphone.

Si la alternativa es utilizar nombres de usuario y contraseñas, la compañía se vuelve incluso más vulnerable al phishing y la apropiación de cuentas.

A medida que las compañías avanzan hacia una nueva manera de trabajar, en la que el trabajo en remoto e híbrido se ha convertido en la norma, confiar en la seguridad perimetral ya no es una opción efectiva. Las compañías que utilizan la autenticación vía teléfono móvil en la actualidad deben reevaluar su estrategia de MFA a largo plazo y valorar el cambio a soluciones de MFA más modernas y resistentes al phishing.

En estos casos, las llaves de seguridad de hardware proporcionan a las compañías una amplia cobertura de posibles operaciones de negocios y grupos de usuarios, asegurando una mayor seguridad y una mejor experiencia para el usuario.

Crear una estrategia de MFA segura a largo plazo

Para proteger a tu compañía del phishing, las cuentas de los usuarios deberían estar protegidas con una 2FA o MFA potente, que utilice llaves de seguridad de hardware para proteger el acceso con los niveles más altos de defensa contra el phishing, a la vez que proporciona la mejor experiencia al usuario. Con las llaves de seguridad de hardware de los nuevos protocolos de autenticación, los usuarios pueden utilizar una sola llave de seguridad para cientos de servicios, con un par de llaves (pública y privada) único generado para cada servicio. La información nunca se comparte entre servicios, y la llave privada se almacena en el elemento seguro de la llave del hardware y no puede ser filtrada. Además, las llaves de seguridad de hardware piden a los usuarios tocar o presionar un botón para demostrar su presencia. De esta manera, las llaves de seguridad de hardware acaban con los ataques remotos, de intermediario y de phishing, de forma que, al contrario de lo que ocurre con los SMS y otras formas de autenticación vía aplicación móvil, solo el servicio registrado puede iniciar la petición de autenticación.

Las compañías también deben dar cuenta de las normas actualizadas que se esperan en los próximos años, especialmente a raíz del COVID-19. Aunque la autenticación vía teléfono móvil pueda considerarse 'suficiente' hoy en día, es posible que no cumpla con los futuros estándares de la MFA. Una inversión en seguridad enfocada al futuro preparará a las compañías para formas de acceso más modernas y seguras, como la autenticación sin contraseña, además de para el cumplimiento de los estándares a largo plazo.

Las YubiKeys proporcionan una forma de autenticación resistente al phishing, y un medio de transición a la autenticación sin contraseña

La YubiKey de Yubico es una llave de seguridad de hardware que está diseñada para proporcionar un alto nivel de seguridad y para evitar el phishing y otras formas de secuestro de cuentas en el momento, posibilitando una autenticación segura a gran escala. Es la única solución demostrada por investigadores independientes para acabar al 100% los robos de cuentas, incluyendo los ataques de phishing masivos y dirigidos[6].

Una sola YubiKey funciona de manera uniforme en sistemas tradicionales y modernos y aplicaciones multiprotocolo con soporte para SmartCard (PIV), OTP, OpenPGP, FIDO U2F y FIDO2/WebAuthn. Y, para las compañías que quieren iniciar su camino hacia la autenticación sin contraseña, la YubiKey proporciona un medio de transición desde los sistemas actuales hacia un futuro moderno y sin contraseñas.

Prepara tu empresa con una inversión en seguridad enfocada al futuro, que no solo ofrece una alta protección, sino que también puede ayudarte en la transición hacia nuevos requisitos de cumplimiento. Las compañías de más riesgo y más preocupadas por su seguridad del mundo confían en la YubiKey para que la autenticación de dos factores y multifactor y la autenticación sin contraseña sean seguras y resistentes al phishing.

	Autenticación vía teléfono móvil	YubiKey
Resistente al phishing	–	✓
Siempre segura	–	✓
Rentable	–	✓
Fácil de usar	–	✓
Cobertura 360°	–	✓
Enfocada al futuro	–	✓

[6] Kurt Thomas et Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (17 de mayo de 2019)

Yubico AB
Kungsgatan 44
2.ª planta
SE-111 35 Estocolmo
(Suecia)

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 EE. UU.
844-205-6787 (gratuito)
650-285-0088