yubico

WHITE PAPER

Los Principales 5 Conceptos erróneos de autenticación utilizando un teléfono móvil

Desmistificando el mito frente a la realidad de MFA heredado

Contenido

Introducción

$3.89 Millones

costo promedio de una brecha de seguridad[3]

$1+ Millón

Costo de una brecha de seguridad cuando el factor es un trabajador remoto[4]

100+ Ataques

Cada día para el 70% de las organizaciones

61%

de las violaciones de datos se remontan a las credenciales[6]

A pesar de la creciente marea y la sofisticación de los ataques cibernéticos, muchas organizaciones continúan utilizando métodos de autenticación heredados, como nombres de usuario y contraseñas o autenticadores basados en dispositivos móviles, para asegurar el acceso a aplicaciones y datos críticos y sensibles. Pero estos métodos no ofrecen la mejor seguridad, son altamente susceptibles a los ataques de phishing, ataques "man in te middle" (MITM), malware, intercambio de SIM y robo de cuentas. Tampoco ofrecen, la mejor experiencia de usuario. En todas estas organizaciones, los resultados son inesperados: los ataques que penetran en sus defensas y los empleados que están frustrados. ¿Por qué está pasando esto?

Si bien cualquier forma de autenticación de multi factor (MFA) ofrece mayor seguridad que la autenticación típica de nombre de usuario y contraseña, no todas las formas de MFA sreadas de la misma forma. La investigación de Google, NYU y UCSD, basada en 350,000 intentos de secuestro en el mundo real, demostró que los SMS y los autenticadores móviles no son muy eficientes para prevenir los robos de cuentas y ataques específicos. La investigación reveló que una OTP basada en SMS solo bloqueaba el 76% de los ataques y una aplicación "push" solo bloqueaba el 90%[1], Esto es como mínimo, una tasa de penetración del 10%. Con este enfoque, no es una cuestión de si lo atacarán, es una cuestión de cuándo.

Los nombres de usuario y las contraseñas y la autenticación basada en dispositivos móviles también contribuyen a la complejidad de autenticación, lo que hace que los empleados se sientan abrumados con la experiencia de autenticación. El empleado promedio tiene que usar y recordar 191 contraseñas, siendo el 61% las mismas o similares[2] y donde la autenticación a base del móvil, como SMS y OTP se utiliza para dos factores (2FA) o MFA, los empleados deben esperar para ingresar los códigos entregados por SMS o aplicaciones del autenticador. Todo esto se suma al tiempo y la complejidad de la autenticación y reduce la productividad de los empleados, mientras tanto, dejan a la organización expuesta.

A medida que las organizaciones cambian a una nueva forma de trabajar, donde el trabajo remoto e híbrido es la norma a largo plazo, es imperativo darse cuenta que confiar en la seguridad del perímetro ya no es eficiente, y que métodos de autenticación legados y débiles, como nombres de usuario y contraseñas, y los autenticadores basados en dispositivos móviles, pueden poner a la organización en riesgo de ser hackeada. Las organizaciones que hoy utilizan autenticación basada en nombres de usuario y contraseña, o aquellas que están utilizando autenticadores basados en móviles, u otras formas de MFA heredadas deben reevaluar su estrategia de MFA a largo plazo y considerar cambiar a las soluciones MFA modernas.

En este documento, revelaremos la imagen real de la autenticación móvil y mostraremos que centrarse en los empleados es la forma en que las organizaciones pueden encontrar un enfoque de MFA más seguro y amigable para el usuario.

Formas Comunes de Autenticación en un Móvil

Hay muchas formas de autenticación utilizando un móvil, cada una ofrece diferentes grados de seguridad y experiencia de usuario. Si bien ciertas formas de autenticación móvil ofrecen mayor seguridad que otras, es importante tener en cuenta que ningún autenticador basado en dispositivos móviles puede detener el robo de cuentas al 100%.

53%

de las organizaciones continúan elegiendo la autenticación basada en dispositivos móviles como forma de MFA.[7]

OTP

Un código de acceso o una contraseña de una sola vez (OTP) es un código que es válido solo para una sesión de inicio de sesión o transacción, generalmente enviada a través de SMS a un teléfono móvil.

TOTP

TOTP (contraseña de una sola vez basada en el tiempo) es un código (token), generado utilizando HMAC (SharedSecret, Timestamp) que cambia cada pocos segundos o minutos, generalmente enviados a través de SMS, o, a veces, una aplicación Autenticador.

Aplicación Push

Un intento de autenticación envía una alerta a una aplicación en el dispositivo móvil de un usuario. Los usuarios ven los detalles de la autenticación y aprueban o deniegan el acceso.

Aplicación Autenticador

Una aplicación de autenticador instalada en un dispositivo móvil que es TOTP se basa y genera un código de acceso aleatorio cada 30 segundos que se utilizarán para la autenticación de inicio de sesión o de dos factores.

Autenticación incorporada

Un autenticador incorporado (también conocido como autenticador de plataforma) está integrado en una plataforma del dispositivo cliente , y aprovecha un módulo de plataforma de confianza interno (TPM) o bien, un elemento seguro, atando la credencial al dispositivo.

En la siguiente sección, cubriremos los cinco principales conceptos erróneos de la autenticación basada en teléfonos móviles que ponen a las organizaciones en riesgo de robos de de cuentas e incrementan los costos de OPEX y CAPEX, si no se abordan

Concepto Érroneo #1: La Autenticación en un móvil es segura

Realidad: La autenticación en un móvil pone a las organizaciones en riesgo

Los dispositivos móviles tienen una gran superficie de ataque que incluye las aplicaciones, sistemas operativos, tecnología de elementos seguros y comunicación, cada uno representa un vector de ataque, sin mencionar la implicancia si un dispositivo se pierde o es robado, también elimina todos los accesos a 2FA / MFA y en consecuencia a las aplicaciones.

La seguridad sigue siendo el mayor concepto érroneo sobre la autenticación basada en un móvil, no todos los tipos de métodos de autenticación móviles se crean iguales. Es importante recordar que los dispositivos móviles se construyen para la comunicación, no para la seguridad. El espectro de seguridad de la autenticación móvil a continuación muestra un perfil de riesgo decreciente de izquierda a derecha, pero nunca se elimina por completo. Muchas organizaciones piensan que “la autenticación móvil es lo suficientemente buena”. Pero en realidad, cada autenticador móvil se puede ser atacado por phishing.

En MFA basado en dispositivos móviles, el segundo factor está vinculado al dispositivo móvil. Esta es una bandera roja, debido a tres aspectos: no hay garantía real de que la clave privada termine en un elemento seguro en el dispositivo móvil, el código OTP o la clave privada podrían ser interceptados de alguna manera y es imposible asegurar prueba de posesión, es decir que la clave llegue a quien tiene que llegar; o en términos del Instituto Nacional de Estándares y Tecnología (NIST), es imposible probar que es resistente a la suplantación de identidad. Los dispositivos móviles tienen una gran superficie de ataque que incluye las aplicaciones, los sistemas operativos, la tecnología de elementos seguros y la comunicación, cada uno representa un vector de ataque, sin mencionar la implicancia si un dispositivo se pierde o es robado, también elimina todos los accesos a 2FA / MFA y en consecuencia a las aplicaciones.

Los hackers de hoy en día se apropian cada vez más de códigos de uso único y notificaciones “push” mediante la interceptación o el phishing, con el atacante y la toma de control de la cuenta casi invisibles para el usuario. El riesgo de interceptación de SMS es tan alto que el NIST declaro a los SMS obsoletos como método de autenticación.[8]

En un artículo reciente de VICE, un hacker ético demostró lo fácil que era redirigir mensajes de texto para “robar” las cuentas de redes sociales de un voluntario.[9] Todo lo que se necesitaba eran solo $ 16 y unos segundos para controlar en forma completa e invisible de las cuentas que habían sido protegidas por MFA basado en OTP

Los ciberdelincuentes de hoy tienen herramientas amplias y económicas a su disposición para crear sitios web de phishing, inyectar malware en el dispositivo, interceptar mensajes de texto o utilizar el intercambio de SIM para interceptar, omitir o frustrar de alguna otra manera la MFA heredada de una manera que es casi indetectable para el usuario final.

Todos los autenticadores móviles pueden ser hackeados

Los robos de cuentas ocurren cuando un hacker obtiene acceso a las credenciales de un usuario. Esto puede provenir de muchas formas:

- Pishing
- Relleno de Credentiales
- Ataque por Fuerza Bruta
- Ataque Man-in-the-middle (MiTM)
- Malware
- OAuth phishing
- Intercambio de SIM

Después de arrestar a 10 personas por ”piratear”r teléfonos móviles, la agencia de policía de la UE Europol dijo que se cree que la red criminal ha robado información personal y más de $ 100 millones (€ 82,4 millones) en criptomonedas, afirmando que el “intercambio de SIM” se puede hacer engañando la compañía telefónica con “técnicas de ingeniería social” o mediante el uso de un “infiltrado corrupto”. [10]

Como se señaló en el borrador de la Estrategia Federal Zero Trust, “muchos enfoques de autenticación multifactor no protegerán contra ataques sofisticados de phishing, que pueden falsificar de manera convincente aplicaciones e involucrar una interacción dinámica con los usuarios. Se puede engañar a los usuarios para que proporcionen un código de una sola vez o respondan a una solicitud de seguridad que otorgue al atacante acceso a la cuenta “. [11]

Cuando la autenticación basada en móvil depende de las personas, se crea una receta para el riesgo. La gente comete errores. No actualizan su software. Descargan una aplicación insegura. Hacen clic en un enlace o responden a una llamada que en realidad fue un ataque de phishing. En otras palabras, ninguna cantidad de capacitación en seguridad puede eliminar por completo los riesgos de los ataques de phishing modernos.

Si siempre ha creído que la autenticación móvil es segura, no está solo. Solo el 22% de los que respondieron una encuesta de Yubico son conscientes de que la seguridad podría ser un problema con la autenticación basada en SMS.[12] Por lo tanto, los actores maliciosos tienen un largo camino para penetrar las defensas de una organización con la actual e insuficiente seguridad de las cuentas.

Phishing

Los atacantes engañan a los usuarios para que proporcionen información confidencial, tales como las credenciales.

Relleno de Credenciales

Credenciales robadas utilizadas para obtener acceso no autorizado a cuentas de usuario a través de solicitudes de inicio de sesión automatizadas a gran escala dirigidas contra una Aplicación web.

Ataque por Fuerza Bruta

Ataque sistemático con todas las contraseñas posibles hasta encontrar la correcta.

Ataque Man-in-the-middle (MiTM)

El atacante intercepta en secreto y posiblemente altera las comunicaciones entre dos partes.

Malware

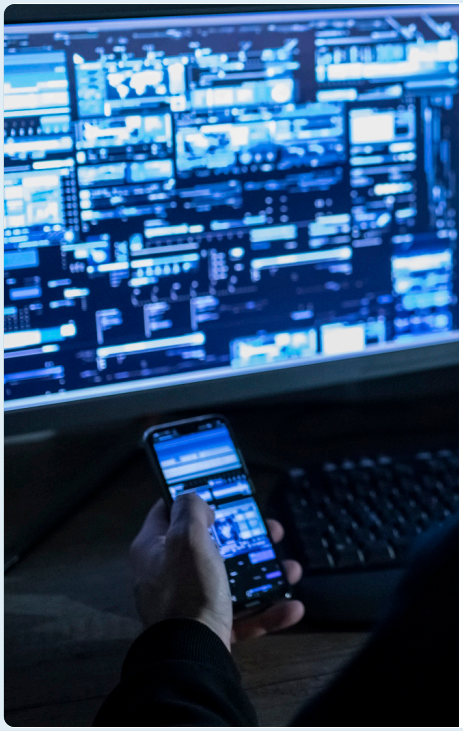
Ataque basado en software diseñado con la intención malintencionada de obtener acceso a una red o de causar daños a los datos y los sistemas.

OAuth phishing

Los hackers utilizan aplicaciones maliciosas de terceros como medio de acceso. Cuando los usuarios otorgan acceso a terceros a una cuenta, el hacker puede obtener acceso utilizando un token OAuth en lugar de una contraseña.

Intercambio de SIM

Un ataque de intercambio de SIM también se conoce como división de SIM, SIMjacking, pirateo de SIM y estafa de port-out. Es una estafa que tiene como objetivo una debilidad en algunas formas de 2FA en la que una llamada o un mensaje de texto enviado a un teléfono móvil se utiliza como segundo factor, explotando la capacidad de las tarjetas SIM para ser transferidas por los proveedores de servicios móviles de dispositivo a dispositivo con diferentes números de teléfono.



Hackers adolescentes explotaron las debilidades de la autenticación móvil en Twitter

En 2020, un pequeño grupo de adolescentes apuntó a los empleados de Twitter con un ataque de spear phishing para obtener acceso a las credenciales de los empleados y la red interna.[13] Los atacantes luego confiscaron cuentas de alto perfil, incluidas las de varias empresas de criptomonedas, y lanzaron una estafa que generó más de $ 118,000 en bitcoins.[14] Todo sin malware, exploits ni puertas traseras.

Un informe de investigación publicado por el Departamento de Servicios Financieros del Estado de Nueva York señaló que Twitter utilizó MFA basada en aplicaciones para autenticar a los empleados, la forma más común de MFA.[15] Durante el ataque, los piratas informáticos engañaron a los empleados para que ingresaran credenciales robadas en un sitio de phishing, “espejado” en tiempo real en el sitio real de Twitter, lo que activó una solicitud de autenticación en el teléfono inteligente del empleado.

Un hacker robó criptomonedas a 6.000 clientes pasando por alto el MFA basado en SMS

Una empresa de crytomoneda reveló que un pirata robó criptomonedas a 6.000 clientes después de usar una vulnerabilidad para eludir la función de seguridad de autenticación multifactor de SMS de la empresa.

En el caso de los clientes que utilizaron mensajes de texto SMS para 2FA, el pirata aprovechó una falla en el proceso de recuperación de la cuenta SMS para recibir un token de autenticación de dos factores por SMS y obtener acceso a la cuenta del cliente.[16]

Estos ataques solo demuestran lo simple que es para la ingeniería social eludir la MFA basada en autenticación móvil.

Concepto Érroneo #2:
La Autenticación en un móvil es de bajo costo

Realidad: Es más cara que lo que piensa

Las organizaciones continúan enfrentando costos crecientes asociados con ataques cibernéticos y violaciones de datos, incluida la pérdida de negocios, tiempo de inactividad del sistema, costos de recuperación, pago de ransomware, costos legales y de auditoría, así como multas regulatorias y daños a la reputación.

$1 Millón

costo anual solo para los costos de soporte relacionados con las contraseñas, para varias organizaciones grandes con sede en EE. UU. en diferentes verticales[19]

60%

de las interacciones de la mesa de servicio de TI están relacionadas con el restablecimiento de contraseñas[20]

$70

el costo promedio de mano de obra de la mesa de ayuda para un solo restablecimiento de contraseña [21]

$5.2 Millones

La cantidad que una empresa promedio pierde anualmente en productividad debido al bloqueo de cuentas[22]

Se percibe que la implementación de la autenticación móvil es relativamente económica, lo que deja a muchas organizaciones satisfechas de haber encontrado una solución rentable para la autenticación. Sin embargo, la autenticación móvil conlleva muchos costos ocultos asociados con los dispositivos, la productividad y el soporte, sin mencionar el costo de una posible violación de datos. En conjunto, se estima que el costo total de los móviles en la empresa puede llegar a $ 1.840 por cada dispositivo.[17]

Costo del Dispositivo

Si el cumplimiento normativo requiere MFA y la organización requiere que los empleados utilicen MFA basado en dispositivos móviles, entonces la organización debe asumir los costos del dispositivo, los costos de servicio recurrentes, el software de administración de dispositivos empresariales, el software de seguridad móvil, así como los costos de reemplazo de teléfonos para soportar la demanda de nuevos dispositivos. Algunas organizaciones pueden ofrecer una suma fija mensual para apoyar el uso laboral de dispositivos personales como alternativa.

Soporte y Costo de Productividad

Forrester estima que las grandes organizaciones gastan hasta $ 1 millón cada año en personal e infraestructura para manejar el restablecimiento de contraseñas de los empleados, y las contraseñas solo representan el primer factor en la autenticación 2FA o MFA.[18] De hecho, muchos de los mismos problemas basados en contraseñas persisten en la autenticación móvil, lo que aumenta los costos sin el beneficio neto para la seguridad.

AnyCualquier forma de autenticación móvil que se aplique y se haga cumplir a escala requerirá la aplicación continua de políticas, la capacitación de los usuarios y el soporte de TI. Incluso las formas más fáciles de autenticación móvil 2FA y MFA (aplicaciones OTP, TOTP, 2FA) crean una enorme carga de soporte si los códigos se retrasan, los usuarios quedan bloqueados en sus cuentas o los usuarios necesitan registrar nuevos dispositivos. Se estima que el 10% de los dispositivos se pierden, se roban o se rompen cada año en las organizaciones, otro factor que aumenta el costo de la autenticación móvil (sin mencionar el riesgo) .[23] Cada vez que un usuario tiene problemas con la autenticación móvil, no está siendo productivo. La autenticación es un servicio de misión crítica: si los empleados no pueden iniciar sesión en las aplicaciones o portales que utilizan, no pueden hacer su trabajo.

Riesgo

Desafortunadamente, es frecuente que una filtración de datos pone a las organizaciones cara a cara con el costo real de la autenticación móvil, y el mayor porcentaje de trabajadores remotos e híbridos puede aumentar el riesgo de una filtración de datos exitosa. Aproximadamente el 73% de los trabajadores de TI cree que los trabajadores remotos representan una mayor amenaza para la seguridad, son más vulnerables a los ataques de spear phishing y tienen más probabilidades de usar dispositivos inseguros.[24]

La gestión de dispositivos móviles es complicada por BYOD y las demandas de los usuarios de poseer y controlar su propio teléfono y utilizar las aplicaciones que deseen. El sesenta por ciento de las organizaciones considera que los dispositivos móviles son el mayor riesgo de seguridad, [25] incluidas las preocupaciones sobre la “TI en la sombra”, el uso no supervisado y no seguro de aplicaciones no autorizadas para el trabajo.

Dado que las credenciales son el vector principal para la violación de datos, la autenticación inadecuada podría ser un error de $ 4,37 millones de dólares, el costo promedio de una violación de datos en el último año donde las credenciales se han visto comprometidas.[26]

Concepto Érroneo #3:
La Autenticación en un móvil es fácil de usar

¿Qué sucede si un dispositivo se pierde, se daña o se apaga? ¿Hay una forma alternativa para acceder a las aplicaciones? Si la respuesta no es obvia, la respuesta con los autenticadores móviles es un "no"

Realidad: La autenticación en un móvil es compleja de utilizar y administrar

Dado que casi no hay barreras para la implementación y un gran conocimiento de los usuarios sobre los métodos de autenticación móvil, es común suponer que la autenticación móvil será fácil de usar o simple. La verdad es que si las contraseñas ya son una carga para los usuarios y para el departamento de TI, la autenticación móvil puede empeorar esa frustración debido a expectativas incorrectas y posibles disrupciones

Experiencia del usuario

El 43% de las organizaciones citan la experiencia del usuario como el principal obstáculo para el uso de MFA.[27] Los autenticadores móviles que involucran SMS o códigos push introducen pasos adicionales engorrosos, lo que aumenta la fatiga del usuario. Multiplicado en las aplicaciones y exacerbado por cierres de sesión programados, esto podría obligar a los usuarios a autenticarse cientos de veces al día. Todo este tiempo existe antes de que un usuario pueda volverse productivo.

Si un mensaje OTP se retrasa o falla, los usuarios pueden quedarse esperando. En marzo de 2021, varios millones de mensajes SMS, incluidos los códigos OTP, no se entregaron cuando se hizo cumplir una regulación comercial de bloqueo de SMS.[28] Más allá de los SMS, los autenticadores móviles requieren un dispositivo cargado y que esté conectado a Internet. ¿Qué sucede si un dispositivo se pierde, se daña o se apaga? ¿Existe una forma alternativa para acceder a las aplicaciones? Si la respuesta no es obvia, la respuesta con los autenticadores móviles es un "no".

Complejidad de TI

El 41% de las organizaciones citan la complejidad como un obstáculo para la adopción de MFA.29 Como se señaló en Concepto erróneo # 2, el soporte de contraseñas (primer factor) y autenticación móvil (segundo factor) requiere una inversión significativa de tiempo de TI. Sí, la autenticación móvil es fácil de implementar. Pero no es fácil de administrar.

Los equipos de TI enfrentan una complejidad constante con:

- Registro de nuevos dispositivos
- Entrenamiento
- Integración de MFA con nuevas aplicaciones
- Gestión de dispositivos
- Solicitudes de la mesa de ayuda, incluido el restablecimiento de contraseñas

Concepto Érroneo #4: La Autenticación en un móvil ofrece 360° de cobertura

Realidad: La autenticación móvil crea brechas en MFA

Los autenticadores móviles pueden generar brechas de seguridad en MFA cuando los usuarios no pueden, no usan o no quieren usar la autenticación basada en dispositivos móviles. Las razones incluyen baja cobertura celular en ciertas áreas geográficas, empleados que no quieren usar dispositivos personales para trabajar o no quieren permitir el acceso del administrador a sus dispositivos. También puede haber restricciones sindicales o requisitos de cumplimiento, y algunos empleados es posible que ni siquiera puedan usar un teléfono inteligente.

Si bien las organizaciones pueden priorizar o incluso exigir MFA basada en dispositivos móviles, casi siempre hay casos extremos de empleados que no pueden, no usan o no quieren usar la autenticación móvil, lo que crea brechas en MFA si la opción alternativa son los nombres de usuario y las contraseñas. Echemos un vistazo a algunos de los casos extremos en los que las organizaciones luchan por admitir la MFA basada en dispositivos móviles:

Igualdad – los usuarios que no tienen un teléfono inteligente o que viven en áreas de baja conectividad pueden tener el desafío de aceptar la autenticación móvil

Sindicatos – Las regulaciones sindicales pueden restringir a los usuarios el uso de su propio dispositivo móvil para la autenticación.

Acceso Restringido – La autenticación móvil no se puede utilizar en áreas restringidas para dispositivos móviles, como call centers, plantas de fabricación. El uso de autenticadores móviles también depende de la batería del dispositivo y la señal celular, que pueden no estar siempre disponibles.

Legal – Muchas organizaciones no pueden exigir legalmente a los empleados que instalen o utilicen aplicaciones corporativas o 2FA / MFA en dispositivos personales, por lo que es posible que deba proporcionar dispositivos corporativos para esto[30] (Vea los costos de los dispositivos, concepto erróneo # 2)

Preferencia – Los empleados pueden negarse a usar sus teléfonos personales para la autenticación móvil relacionada con el trabajo.

Obstaculos – Pérdida inesperada del dispositivo, la necesidad de registrar un nuevo dispositivo, la necesidad de registrar o configurar varios dispositivos para admitir el inicio de sesión en cada uno

Usuarios Privilegiados – Si reconocemos que la MFA basada en dispositivos móviles no es la forma más sólida de autenticación (concepto erróneo # 1), es posible que no sea adecuada para usuarios privilegiados y administradores cuyas credenciales son un objetivo principal. La advertencia aquí es que los ataques sofisticados de hoy hacen que cada usuario sea un usuario privilegiado, con una sola credencial como punto de partida para ataques laterales y escalados.

> Passwordless representa un cambio masivo en la forma en que miles de millones de usuarios, tanto empresas como consumidores, iniciarán sesión en forma segura en sus dispositivos con Windows 10 y se autenticarán en las aplicaciones y servicios basados en Azure Active Directory.
>
> **– Alex Simons, Corporate Vice President PM, Microsoft Identity Division**

¿Qué es la autenticación passwordless?

En los últimos años, el término "passwordless" ha ganado impulso y ahora lo utilizan muchos proveedores de soluciones de seguridad, autenticación e identidad.
—Cada uno con su propio matiz único. Hay muchas implementaciones diferentes de autenticación passwordless y todas tienen variantes. Algunas implementaciones passwordless, como SMS, están diseñadas específicamente para abordar problemas de usabilidad. Otras implementaciones passwordless, como las tarjetas inteligentes, están diseñadas específicamente para abordar problemas de seguridad. Una estrategia passwordless con visión de futuro se basa en FIDO2 / WebAuthn. FIDO2 es la nueva especificacion éstandar de autenticación de FIDO Alliance (presentada en 2018), y WebAuthn es una API basada en web que permite a los sitios web actualizar su flujo de inicio de sesión para agregar autenticación basada en FIDO en navegadores y plataformas compatibles. Este es un ecosistema de seguridad en evolución que facilitará la adopción de la autenticación passwordless.

Concepto Érroneo #5: La Autenticación en un móvil está probada a futuro:

Realidad: La autenticación móvil no está diseñada para el largo plazo

Las inversiones en seguridad deben proporcionar una protección adecuada que cumpla con las regulaciones cada vez más estrictas a lo largo del tiempo. Una inversión en seguridad verdaderamente considerada para el futuro debería preparar bien a una organización para flujos de inicio de sesión modernos y seguros, como passwordless, así como para el cumplimiento normativo a largo plazo. Con las actualizaciones de las regulaciones actuales y las nuevas regulaciones netas que se esperan en los próximos años, especialmente a raíz de COVID-19, la autenticación móvil, aunque se considera lo suficientemente buena hoy, puede que no cumpla con los estándares de cumplimiento futuros relacionados con MFA.

Además, el futuro de la autenticación es passwordless, es decir, cualquier forma de autenticación que no requiera que el usuario proporcione una contraseña al iniciar sesión. En la actualidad, existen muchas implementaciones diferentes de autenticación sin contraseña. Muchos se refieren a la verificación por SMS como passwordless porque no es necesario recordar una contraseña. Por lo general, se le envía un código OTP que es válido por un período corto de tiempo que el usuario puede usar para autenticarse. (Y la ironía es que "OTP" significa "contraseña de un solo uso", que es el uso común del término). Como hemos demostrado, estas formas de autenticación passwordless se consideran una forma débil de autenticación.

La autenticación con tarjeta inteligente es otra forma de passwordless. Pero las tarjetas inteligentes tradicionales pueden ser algo complejas de implementar y administrar para los administradores, e implican tener una buena estrategia para implementar a escala.

Hay formas más seguras de autenticación passwordless que no requieren verificación por SMS y que se mantienen separadas del dispositivo en sí. Separando el dispositivo del autenticador, se tiene una raíz de confianza portátil, lo que le permite demostrar que se posee el dispositivo de hardware único que contiene el material criptográfico que se registró en la cuenta de usuario. Esto, combinado con el nombre de usuario + contraseña o PIN, satisface los verdaderos requisitos de autenticación de múltiples factores al proporcionar algo que usted sabe, algo que es o algo que tiene.

La industria avanza hacia flujos de inicio de sesión passwordless que son seguros, rápidos y sencillos. FIDO2 es la especificación más reciente de la FIDO Alliance para estándares de autenticación al cubrir los flujos de inicio de sesión sin contraseña. FIDO2 ofrece autenticación de factor único o multifactor, evitando los componentes más susceptibles de suplantación de identidad de una solución 2FA como SMS y eliminando la necesidad de un nombre de usuario y contraseña como primer factor

Muchas aplicaciones que soportan OTP y otros métodos heredados aún no admiten protocolos modernos como FIDO2 y WebAuthn. Destruir y reemplazar los métodos heredados de la noche a la mañana no es pragmático y puede ser costoso. Al mismo tiempo, tampoco es deseable que los usuarios lleven varios dispositivos de autenticación. Pasar a la tecnología passwordless no es una implementación "única", sino más bien un viaje que a menudo implica admitir entornos heredados, modernos e híbridos con una autenticación sólida.

Autenticación sólida y moderna con una Yubikey

> Una opción de múltiples factores, las llaves de seguridad físicas, parece ser inmune a estas estafas sofisticadas.[31]
>
> **–Brian Krebs, Krebs on Security**

Yubico creó YubiKey, una llave de seguridad de hardware moderna construida para alta seguridad y usabilidad.

La YubiKey utiliza protocolos modernos como los estándares de autenticación abiertos FIDO U2F y FIDO2 para ayudar a eliminar los ataques basados en credenciales impulsados por phishing y soporta la necesidad de un flujo de inicio de sesión fácil de usar. Yubico también es uno de los principales contribuyente en la creación de los estándares de autenticación abierta FIDO Universal 2nd Factor (U2F) y FIDO2, y ha contribuido a las organizaciones de estándares de identidad abiertos W3C, IETF, FIDO Alliance y OpenID.

La YubiKey brinda una sólida autenticación de dos factores, varios factores y passwordless a escala, resistente al phishing, y con el autenticador de hardware protegiendo los secretos privados en un elemento seguro que no se puede extraer fácilmente. Investigaciones independientes, indican que la YubiKey es la única solución que está probada para detener el 100% de los robos de cuentas.[32]

Es el tipo de protección que podría haber detenido el ataque a Twitter:

> Durante el ataque a Twitter, los hackers superaron el MFA convenciendo a los empleados de Twitter de que autenticaran con el MFA basado en la aplicación durante el inicio de sesión. La forma más segura de MFA es una llave de seguridad física, o MFA de hardware, que incluye una llave USB que se conecta a una computadora para autenticar a los usuarios. Este tipo de hardware MFA habría detenido a los piratas informáticos, y Twitter ahora lo está implementando en lugar del MFA basado en aplicaciones.
>
> **– Departmento de Servicios Financieros de Nueva York, Informe de Investigación de Twitter[33]**

Al soportar múltiples protocolos de autenticación en la misma YubiKey, como OTP, OpenPGP y protocolos de autenticación sólida como Smart Card, FIDO U2F y FIDO2 / WebAuthn, la YubiKey ofrece a las organizaciones la flexibilidad de implementar una autenticación sólida con una sola llave en una variedad de infraestructuras heredadas y modernas para ayudar a las organizaciones sin importar dónde se encuentren. en su viaje hacia passwordless.

Tasas de robo de cuentas

> “Cualquier forma de MFA es mejor que solo un nombre de usuario y contraseña, pero la mayoría de MFA aún pueden ser atacados por phishing. No pasó mucho tiempo para darnos cuenta de que necesitábamos una autenticación más sólida para todos los empleados que no podían ser objeto de suplantación de identidad. Las YubiKeys tenían más sentido. Y cuando utilicé por primera vez una YubiKey Nano, me encantó la experiencia: lo dejé en mi computadora y simplemente lo toqué para autenticar.

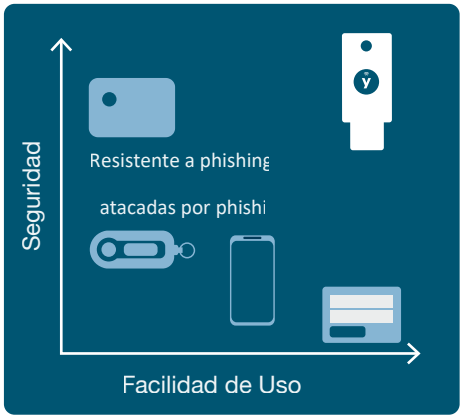
– Daniel Jacobson
Director de TI, Datadog[34]

Por su versatilidad la YubiKey no requiere instalación de software ni batería, así que para una autenticación segura, simplemente se conecta a un puerto USB y se toca el sensor, o bien se toca usando NFC . Las YubiKeys no requieren baterías, no tienen pantallas que se puedan romper, no necesitan una conexión celular y son resistentes al agua y a los golpes.

La YubiKey brinda la conveniencia necesaria para soportar los empleados internos, híbridos y remot s de hoy en día..

	Autenticación Móvil	YubiKey
Siempre Segura	X	✓
Bajo Costo	X	✓
Fácil de Usar	X	✓
360° de cobertura	X	✓
Probada a Futuro	X	✓

Resumen



Durante muchos años, elegir un enfoque de MFA y passwordless requirió un intercambio entre seguridad y productividad / facilidad de uso del usuario. Las tarjetas inteligentes ofrecen alta seguridad y almacenan el secreto en la tarjeta, pero la implementación es costosa y no es práctica en todos los dispositivos a los que un empleado pueda tener acceso. Por otro lado, la ubicuidad de los dispositivos móviles introdujo el concepto de conveniencia y facilidad de uso en MFA, pero ¿la autenticación móvil entregó todo lo que esperábamos (y creíamos) que haría?

En este documento técnico, aprendimos que la seguridad de la autenticación móvil es un espectro, y que algunas formas funcionan mucho mejor que otras. Hemos visto que existen muchos costos ocultos para la autenticación en un móvil, y algunos costos no tan ocultos que ninguna organización quiere enfrentar. Hemos visto que fácil de implementar no siempre significa fácil de usar o fácil de administrar. Y que la industria se está moviendo hacia la autenticación passwordless, mientras que la autenticación móvil está estancada en el pasado.

Afortunadamente hay un camino a seguir. YubiKey es una solución MFA más segura y fácil de usar diseñada para llegar a las organizaciones independientemente del punto en el que encuentran y ser un verdadero puente hacia la tecnología passwordless, que admite sin problemas las infraestructuras heredadas, así como los sistemas modernos basados en la nube que aprovechan los últimos estándares como WebAuthn y FIDO2.

Fuentes

[1] Kurt Thomas, Angelika Moscicki, New research: How effective is basic account hygiene at preventing hijacking, (May 17, 2019), https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

[2] Amber Steel, LastPass Reveals 8 Truths about Passwords in the New Password Exposé, (November 1, 2017), https://blog.lastpass.com/2017/11/lastpass-reveals-8-truths-about-passwords-in-the-new-password-expose/

[3] IBM, 2021 Cost of Data Breach Report, (Accessed September 14, 2021), https://www.ibm.com/security/data-breach

[4] IBM, 2021 Cost of Data Breach Report, (Accessed September 14, 2021), https://www.ibm.com/security/data-breach

[5] Red Canary, The State of Incident Response 20201, (Accessed September 16, 2021), https://redcanary.com/resources/guides/the-state-of-incident-response-2021/

[6] Verizon, 2021 Data Breach Investigations Report, (Accessed May 18, 2021), https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/

[7] 451 Research, 2021 Yubico and 451 Research Study, (April 2021), https://pages.yubico.com/work-from-home-policies-driving-mfa-adoption [8]

Rob Lemos, The state of two-factor authentication by text: What security pros need to know, (Accessed Sept 14, 2021), https://techbeacon.com/security/state-two-factor-authentication-text-what-security-pros-need-know

[9] Joseph Cox, A Hacker Got All My Texts for $16, VICE, (March 16, 2021), https://www.vice.com/en/article/y3g8wb/hacker-got-my-texts-16-dollars-sakari-netnumber

[10] Euronews, SIM swapping: 10 arrested in Europe over €82.4m scam to hijack celebrities' phones, (February 10, 2021), https://www.euronews.com/2021/02/10/sim-swapping-10-arrested-in-europe-over-82-4m-scam-to-hijack-celebrities-phones

[11] WhiteHouse.gov, Federal Zero Trust Strategy (EO 14028), Accessed Sept 16, 2021, https://zerotrust.cyber.gov/federal-zero-trust-strategy

[12] 451 Research, 2021 Yubico and 451 Research Study, (April 2021), https://pages.yubico.com/work-from-home-policies-driving-mfa-adoption

[13] Twitter, An update on our security incident, (July 18, 2020), https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident

[14] New York State Department of Financial Services, Twitter Investigation Report, (Accessed Sept 14, 2021)

[15] Department of Financial Services Twitter Investigation Report, Oct 14, 2020, https://www.dfs.ny.gov/Twitter_Report

[16] Hackers rob thousands of Coinbase customers using MFA flaw, https://www.bleepingcomputer.com/news/security/hackers-rob-thousands-of-coinbase-customers-using-mfa-flaw/

[17] Wandera, Uncovering the True Costs of Enterprise Mobility, (Accessed September 14, 2021), https://www.clevermobile.it/risorse/file/wandera/tcowhitepaper.pdf

[18] LastPass, New Forrester Report: The Real Cost of Password Risks, (May 18, 2018), https://blog.lastpass.com/2018/05/new-forrester-report-real-cost-password-risks/

[19] Forrester Report: Best Practices: Selecting, Deploying, And Managing Enterprise Password Managers, (January 8, 2018)

[20] Gartner, 3 Simple Ways IT Service Desks Should Handle Incidents and Requests, (Aug 2019)

[21] Forrester Research, Best Practices: Selecting, Deploying, and Managing Enterprise Password Managers, (January 8, 2018)

[22] Ponemon Institute, 2019 State of Password and Authentication Security Behaviors Report, (Accessed September 14, 2021), https://pages.yubico.com/2019-password-and-authentication-report

[23] LocknCharge, The True Cost of Lost or Missing Mobile Devices, (Accessed September 12, 2021), https://www.locknCharge.com/cost-of-lost-devices/

[24] OpenVPN, Remote Work is the New Future - But Is Your Organization Ready for It? (Accessed September 13, 2021), https://openvpn.net/blog/remote-workforce-cybersecurity-quick-poll/

[25] Verizon, Mobile Security Index 2021 Report, (Accessed September 14, 2021), https://www.verizon.com/business/resources/reports/mobile-security-index.html/

[26] IBM, 2021 Cost of Data Breach Report, (Accessed September 14, 2021), https://www.ibm.com/security/data-breach

[27] 451 Research, 2021 Yubico and 451 Research Study, (April 2021), https://pages.yubico.com/work-from-home-policies-driving-mfa-adoption

[28] FE Online, OTP messages not coming through? You are not alone, here's why this is happening, (March 9, 2021), https://www.financialexpress.com/industry/technology/otp-messages-not-coming-through-you-are-not-alone-heres-why-this-is-happening/2209041/

[29] 451 Research, 2021 Yubico and 451 Research Study, (April 2021), https://pages.yubico.com/work-from-home-policies-driving-mfa-adoption

[30] https://www.shouselaw.com/ca/blog/do-i-get-reimbursed-for-business-use-of-my-personal-cell-phone/

[31] Brian Krebs, Voice Phishers Targeting Corporate VPNs, Krebs on Security, (August 19, 2021) https://krebsonsecurity.com/2020/08/voice-phishers-targeting-corporate-vpns/

[32] Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (May 17, 2019), https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

[33] New York State Department of Financial Services, Twitter Investigation Report, (Accessed September 14, 2021)

[34] Yubico, Datadog leads in authentication best practices, deploys YubiKeys to all employees enterprise-wide https://www.yubico.com/resources/reference-customers/datadog-leads-in-authentication-best-practices-deploys-yubikeys-to-all-employees-enterprise-wide/

yubico

Acerca de Yubico

Yubico establece nuevos estándares globales para el acceso simple y seguro a computadoras, dispositivos móviles, servidores y cuentas de Internet.

El invento principal de la empresa, la YubiKey, ofrece una sólida protección de hardware, con un simple toque, en cualquier cantidad de sistemas de TI y servicios en línea. El YubiHSM, el módulo de seguridad de hardware ultraportátil de Yubico, protege los datos confidenciales almacenados en los servidores.

Yubico es uno de los principales contribuyentes a los estándares de autenticación abierta FIDO2, WebAuthn y FIDO Universal 2nd Factor, y la tecnología de la empresa es implementada y apreciada por 9 de las 10 principales marcas de Internet y por millones de usuarios en 160 países.

Fundada en 2007, Yubico es una empresa privada, con oficinas en Suecia, Reino Unido, Alemania, Estados Unidos, Australia y Singapur. Para más información: www.yubico.com.