White Paper

No más contraseñas

781.276.4000 | sales@aware.com | www.aware.com

Aware es el principal proveedor mundial de productos y soluciones biométricas. Las soluciones de gestión y verificación de identidad de Aware son utilizados en servicios financieros, seguridad empresarial, atención médica, recursos humanos, identificación de ciudadanos, control de fronteras, cumplimento de la ley, defensa e inteligencia. La tecnología Aware líder en la industria ayuda a las organizaciones a recopilar, administrar, procesar y comparar imágenes y datos biométricos para la ayuda de identificación y autenticación.

La pandemia de COVID-19 presentó nuevos desafíos a los negocios ya que se vieron obligados a adaptarse a un modelo operativo donde trabajar desde el hogar era la nueva normalidad. Estas condiciones de trabajo en casa produjeron una mayor dependencia en la tecnología y, sin la protección que ofrece la infraestructura de la oficina, muchos empleados quedaron expuestos a numerosos riesgos de ataques cibernéticos. Además, los empleados están experimentando un aumento de fatiga de contraseña como resultado de la necesidad de actualizar constantemente las mismas. A la luz de esta condición de cambio, los métodos actuales de autenticación son apenas suficientes para proteger los datos de la empresa y los trabajadores. La necesidad de autenticación bien protegida es más importante que nunca.

Métodos actuales de autenticación

Con el aumento de amenazas a la seguridad cibernética, muchas compañías han recurrido a la autenticación de dos factores. La autenticación de dos factores es un método de autenticación electrónica en la cual se otorga a un usuario acceso a una página web o aplicación solamente después de presentar de manera satisfactoria dos elementos de evidencia a un mecanismo de autenticación. Los factores que conceden el acceso incluyen algo que usted conoce, como una contraseña, frase secreta o número de identificación personal, y algo que usted tiene, como un dispositivo móvil o un dispositivo USB fiable.

Este nivel de autenticación se ha convertido en lo normal ya que establece que las organizaciones continúen utilizando contraseñas. Sin embargo, el método no es del todo perfecto. Muchos usuarios reportan[1] que las barreras adicionales de la autenticación de dos factores son excesivamente inconvenientes, lo que puede causar que usuarios enfadados busquen la salida fácil y tomen atajos que hacen más vulnerable al sistema. Aunque requerir un identificador más no disuade a algunos atacantes de asaltar los sistemas defendidos con autenticación de múltiples factores, muchos otros están dispuestos a encargarse del obstáculo adicional si creen que la información almacenada dentro de su organización objetivo vale la pena el esfuerzo. Además, la autenticación de dos factores no proporciona autenticación de identidad sino más bien autenticación del dispositivo. La prueba de posesión del dispositivo se conduce bajo el supuesto de que el propietario del dispositivo específico será la única persona que lo utilice, sin tomar en cuenta las ocasiones de fraude.

El problema de las contraseñas

Conforme el mundo sigue aumentando la dependencia en las soluciones digitales, la sociedad continúa dependiendo en gran medida de contraseñas y números de identificación personal (NIP). Por desgracia, las contraseñas tienen problemas. De hecho, casi todos los profesionales de TI (~95%) están de acuerdo en que las contraseñas representan auténticos riesgos de seguridad a su organización. Esto se debe a que las personas han estado utilizando contraseñas vulnerables, descuidando las contraseñas (las escriben en post-its) y reutilizando las que hacen sentir cómodos a los usuarios, entre otros malos hábitos. De acuerdo con Gartner[2], el State of Password and Authentication Security Behaviors Report 2020[3] y Verizon[4]:

- **20-50% de todas las llamadas de asistencia técnica se relacionan con el cambio de contraseñas**
- **39-50% de las personas reutilizan las contraseñas personales o comerciales para las cuentas de la oficina**
- **80% de las transgresiones evidenciaron contraseñas vulnerables o robadas**

Entre las frustraciones[5] principales de los empleados está el cambio de contraseñas, recordar las 100 contraseñas anteriores y no poderlas reutilizar. Esto hace que la gestión de contraseñas sea una parte tediosa del trabajo y que seguro no agrega nada de seguridad si se hace incorrectamente. Como resultado, muchos trabajadores sufren de fatiga de contraseña, que puede definirse como la dificultad de los trabajadores por recordar todas sus contraseñas. Se calcula que el empleado de empresa promedio mantiene un registro de 191 contraseñas[6]. Esto es un fastidio evidente. Los empleados se cansan de tener que recordar un montón de contraseñas, por lo que empiezan a repetir contraseñas y a reducir la complejidad en un esfuerzo por atenuar la carga mental de cómo iniciar sesión. Por desgracia para muchos, el temor de olvidar una contraseña es más poderoso que el temor de una posible filtración de datos. De hecho, 91% de las personas[6] entienden el riesgo de reutilizar las contraseñas, y no obstante el 59% admite que lo hace de todos modos[6]. En síntesis, las contraseñas son la entrada a los datos confidenciales, las operaciones financieras electrónicas, y más, y aun así no las tratamos como el riesgo de seguridad más decisivo que enfrenta una organización.

La fatiga de contraseña, entonces, no impacta solamente a los empleados sino a la seguridad de la organización también.

Queda claro que la empresa corre más riesgo si sus empleados están batallando con la fatiga de contraseña. De acuerdo con una encuesta conducida por el Ponemon Institute, 51% de las personas[7] alternan las mismas cinco contraseñas entre sus cuentas de trabajo y personales. Además de compartir las contraseñas entre sus propias cuentas, los empleados con frecuencia se comparten entre sí las contraseñas; 69% de las personas admiten que comparten credenciales para el acceso a la cuenta de trabajo. Otro riesgo de seguridad en potencia relacionado con la fatiga de contraseña es la susceptibilidad a la suplantación de identidad (phishing) ya que la mayoría de las solicitudes de recuperación de contraseñas se entregan por correo electrónico. La suplantación de identidad (phishing) es el vector de ataque más común y presente en 36%[4] de las filtraciones de datos. Si se suplanta con éxito la identidad de un empleado que sufre fatiga de contraseña, quien además tiene cinco contraseñas en rotación que comparte con otro compañero, la situación podría escalar con facilidad a una filtración de datos grave. Como resultado, muchas de las peores filtraciones de datos corporativos se han originado a través de transgresiones de contraseña.

Impacto del COVID-19 en la tecnología del lugar de trabajo

La actual pandemia de COVID-19 ha puesto de relieve la vulnerabilidad de los métodos de autenticación actuales, haciendo que la ciberseguridad sea una prioridad fundamental conforme millones de trabajadores y negocios en todo el mundo dependen de la infraestructura digital y la internet. De acuerdo con el Informe sobre Riesgos Mundial de 20208, los líderes empresariales dicen que sus riesgos de ciberseguridad están aumentando, encontrándose los ciberataques y el robo de datos entre los 10 riesgos principales que los CEO muy posiblemente enfrenten tanto a corto como largo plazo. Tan solo en los primeros seis meses de 2019, las filtraciones de datos expusieron 4.1 mil millones de registros[9], revelando muchas veces millones de credenciales en una sola filtración a la web pública y la dark web. El costo promedio de una filtración se calcula en $3.92 millones[10], y en 2021 la pérdida económica global asociada con la delincuencia informática fue de $6 billones.

La dependencia en la tecnología y la internet, combinada con el temor permanente causado por la pandemia, creó el ambiente perfecto para que los delincuentes informáticos prosperen. Los trabajadores cambiaron los estilos y comportamientos de trabajo. Por ejemplo, HP Inc.[12] reporta que 70% de los oficinistas encuestados admiten que usan sus aparatos de trabajo para tareas personales, mientras que el 69% está usando las computadoras portátiles o impresoras personales para actividades laborales. Como resultado de estos factores, los trabajadores a distancia se volvieron el objetivo cada vez mayor de los atacantes. Los ciberdelincuentes podían pedir rescate de millones de dólares de los negocios utilizando tácticas de eficacia comprobada como la suplantación de identidad (phishing), ingeniería social y otras herramientas de atacantes de la industria. Para las compañías, el costo promedio de una filtración de datos se disparó a $21,659 por incidente durante la pandemia, escenario en que la mayoría de los incidentes fluctuaba desde tan poco como $800 hasta más de $650,000, de acuerdo con un informe nuevo de Verizon[4]. Aunque 5% de los ataques con éxito costaron a los negocios $1 millón o más. KuppingerCole[13] reporta que durante la pandemia ha habido un aumento del 238% en el volumen de ciberataques a nivel mundial.

Reducción de índices alarmantes de delitos cibernéticos con autenticación biométrica

Las contraseñas se inventaron en la década de los 60 y el objetivo nunca fue proteger las cuentas bancarias, los registros de salud, correos electrónicos y una larga lista de otros usos que se les ha adjudicado. En realidad fueron inventadas para tiempo compartido de computadora y en su momento funcionaron con la suficiente eficacia para ese caso de aplicación. El aumento de amenazas a la ciberseguridad y la identificación falsa han causado que muchas compañías adopten un método rígido como la autenticación de dos factores para combatir estos problemas. Sin embargo, resolver los problemas de identidad y seguridad puede facilitarse con la biometría. Esto se debe a que la biometría se puede ajustar en los métodos de autenticación por múltiples factores o permite que los usuarios renuncien totalmente a las contraseñas.

La autenticación biométrica por múltiples factores[14] funciona igual que los métodos de autenticación de dos factores aunque requiere un factor adicional en la secuencia del inicio de sesión. Uno de los factores que el usuario final tiene que dar es un parámetro biométrico (e.g., cara o huella digital). La tecnología biométrica se ha vuelto el patrón de referencia para seguridad y prueba de identidad debido a sus altos porcentajes de exactitud. La adición de la biometría a la autenticación por múltiples factores podría hacer finalmente que las contraseñas se hicieran obsoletas, reforzando la infraestructura de TI de los negocios a nivel mundial. Como mínimo, la biometría podría fortalecer la autenticación por múltiples factores en general.

Para finales de 2022, Gartner[15] predice que 60% de las empresas grandes y globales, y 90% de las empresas medianas, implementarán métodos sin contraseñas en más del 50% de los casos de aplicación — superando el 5% de 2018. La autenticación sin contraseña[14], por su naturaleza, elimina el problema de usar contraseñas vulnerables. También ofrece beneficios a los usuarios y organizaciones. Para los usuarios, causa que el problema creciente de la fatiga de contraseña quede en el olvido.

Para las organizaciones, deja de existir la necesidad de guardar contraseñas, y como resultado las empresas tendrán:

Mejor protección:

Aunque las contraseñas son vulnerable a los intentos de suplantación de identidad (phishing), los parámetros biométricos y los autentificadores de hardware no lo son. La autenticación sin contraseña quita el problema de duplicar contraseñas y prácticas de gestión de contraseñas inferiores como escribir códigos en notas adhesivas.

Menos filtraciones:

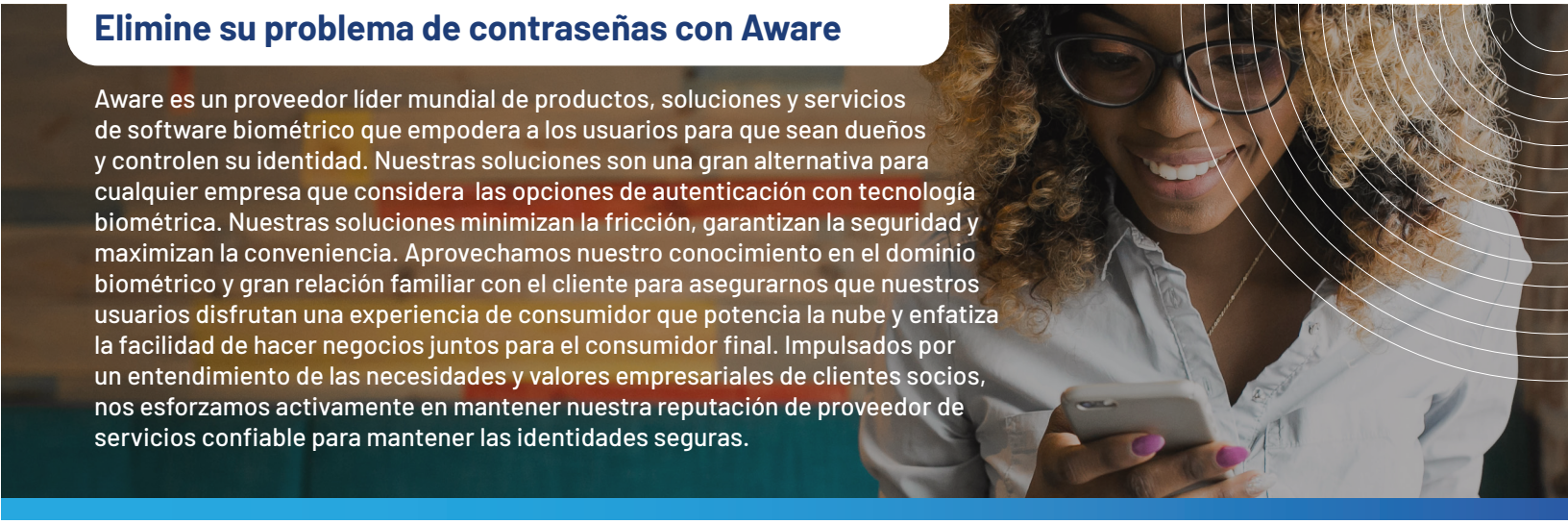
Cuando las compañías hagan la transición a las soluciones sin uso de contraseñas para autenticar, reducen de manera considerable su exposición a las filtraciones de datos. Al usar soluciones sin contraseñas para autenticar, dejan de existir las contraseñas que los ciberatacantes puedan robar de un servidor de plataformas.

Costos de soporte inferiores:

La autenticación sin contraseñas es más barata a la larga. Las contraseñas requieren que las organizaciones mantengan sistemas de gestión de contraseñas de modo que los usuarios realicen actualizaciones periódicas de contraseñas y la ocasional restauración de contraseña. Cambiar la autenticación a biometría, reduce la carga de los servicios de asistencia técnica permitiendo que las organizaciones ahorren en los costos asociados con la sustitución de contraseñas.

Con el aumento de la dependencia en la tecnología, las nuevas condiciones laborales y una intensificación cada vez mayor de ciberataques maliciosos, ahora es el momento ideal para que las empresas consideren modernizar sus productos y procedimientos de seguridad. La biometría aporta conveniencia y seguridad, permitiendo a las compañías que protejan sus datos. – su activo más importante.

Elimine su problema de contraseñas con Aware



Aware es un proveedor líder mundial de productos, soluciones y servicios de software biométrico que empodera a los usuarios para que sean dueños y controlen su identidad. Nuestras soluciones son una gran alternativa para cualquier empresa que considera las opciones de autenticación con tecnología biométrica. Nuestras soluciones minimizan la fricción, garantizan la seguridad y maximizan la conveniencia. Aprovechamos nuestro conocimiento en el dominio biométrico y gran relación familiar con el cliente para asegurarnos que nuestros usuarios disfrutan una experiencia de consumidor que potencia la nube y enfatiza la facilidad de hacer negocios juntos para el consumidor final. Impulsados por un entendimiento de las necesidades y valores empresariales de clientes socios, nos esforzamos activamente en mantener nuestra reputación de proveedor de servicios confiable para mantener las identidades seguras.

Integración móvil: Nuestras soluciones proporcionan verificación de identidad para respaldar la integración móvil. Las comprobaciones de seguridad avanzada pueden autenticar las licencias de conductor y pasaportes y asegurar la correspondencia facial biométrica invulnerable a suplantación entre las imágenes vivas e impresas. La integración incluye correspondencia biométrica facial a los documentos de identificación, y la verificación para más de 9,000 documentos a nivel mundial. La detección de usuarios reales también descubre a los impostores, evitando que tengan acceso a las cuentas y la información confidenciales

Autenticación por dispositivo móvil: Nuestra solución Brinda autenticación por múltiples factores sin contraseña utilizando el reconocimiento biométrico facial y de voz y detección de usuario real y se basa en los algoritmos de correspondencia de cara y voz probados de NIST. Con nuestras capacidades biométricas multimodales, los usuarios pueden ser verificados con sus caras, voces o una combinación de las dos para lograr una seguridad incluso mayor.

Detección de usuarios reales: Nuestros algoritmos para detección de ataques de presentación avanzados no solamente detectan la suplantación de la víctima, sino además el encubrimiento de identidad, proporcionando a bancos y compañías financieras la paz y tranquilidad de que sus clientes son quienes dicen ser. Nuestra detección de usuarios reales también es pasiva para nuestros usuarios, no requiriendo medidas adicionales (como movimientos de cabeza indicados) para ser eficaz. Nuestra detección de usuarios reales funciona para integración y autenticación.

Configuraciones flexibles: Además de dar soporte a toda una gama de sistemas operativos móviles y de servidor, nuestras soluciones se pueden configurar para estar disponibles solamente en el dispositivo, el servidor o en el navegador. Las configuraciones solamente de dispositivo colocan la funcionalidad biométrica en el dispositivo de una persona y son ideales para situaciones en las cuales no se garantiza la disponibilidad de la red. Sin embargo, las configuraciones basadas solamente en servidor, ponen la funcionalidad biométrica en el servidor; una solución perfecta para cuando la disponibilidad de la red es potente. Nuestras configuraciones solamente de navegador sirven como una tercera alternativa, realizando la captura biométrica directamente a través de un navegador, y poniendo funcionalidad adicional en el servidor. Independientemente de la elección, nuestras soluciones continuarán proporcionando el mismo nivel de seguridad y conveniencia.

Para mayor información acerca de nuestra cartera biométrica, comuníquese con nosotros.

AWARE

Fuentes:

1 https://medium.com/@rezaduty/2fa-security-issue-675a6dec825a
2 https://www.gartner.com/en/documents/3773163
3 https://www.yubico.com/blog/yubico-releases-2020-state-of-password-and-authentication-security-behaviors-report/
4 https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf
5 https://www.comparitech.com/blog/information-security/password-statistics/
6 https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/en/LastPass-Enterprise-The-Password-Expose-Ebook-v2.pdf
7 https://www.yubico.com/wp-content/uploads/2019/01/Ponemon-Report-Infographic.pdf
8 https://www.weforum.org/reports/the-global-risks-report-2020
9 https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/?sh=4e662ce4bd54
10 https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years
11 https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
12 https://threatresearch.ext.hp.com/hp-wolf-security-blurred-lines-blindspots-report-risky-remote-working/
13 https://www.kuppingercole.com/research/lc80127/fraud-reduction-intelligence-platforms
14 https://www.aware.com/blog-enhance-multifactor-authentication-enterprise/
15 https://www.gartner.com/smarterwithgartner/embrace-a-passwordless-approach-to-improve-security
16 https://www.aware.com/blog-going-passwordless/

Copyright © 2022 Aware, Inc. Todos los derechos reservados. Este documento es exclusivamente para fines de información y está sujeto a cambios sin previo aviso. Aware, Inc no asume responsabilidad alguna por la exactitud de la información. "Aware" es una marca registrada de Aware, Inc.. "AwareABIS" es una marca registrada de Aware, Inc.. Otros nombres de empresas y marcas, productos y servicios son marcas comerciales, marcas de servicio, marcas comerciales registradas o marcas de servicio registradas de sus respectivos propietarios. Going-Passwordless-SPanish_0622