

La importancia de la gestión de identidad

con MFA para la ciberseguridad



intexus✧

CREANDO UN MUNDO CONFIABLE

Hay muchas maneras diferentes de autenticar a un usuario. Los métodos más comunes son nombre de usuario y contraseña, pero otras opciones realmente seguras incluyen datos biométricos, tokens de seguridad o contraseñas de un solo uso.

El nombre de usuario y la contraseña es el método de autenticación más común, pero también es el menos seguro.

Los ciberdelicuentes pueden adivinar fácilmente o usar la fuerza bruta para acceder a una cuenta si tienen las herramientas adecuadas.



Tiempo necesario para decodificar o hackear una contraseña

Diferencias entre la fortaleza de contraseñas con 5, 6, 7 u 8 caracteres. Usando números, letras con mayúsculas, combinando lo anterior y por último agregando símbolos.

38172 Al instante	manue Al instante	MaNue 4 segundos	MaN72 9 segundos	MaN7* 1 minuto
381723 Al instante	manuel 3 segundos	MaNuel 3 minuto	MaN723 9 minutos	MaN72* 2 horas
3817239 Al instante	manuela 1 minuto	MaNuelA 3 horas	MaN723e 10 horas	MaN72* 8 días
38172395 10 segundos	manuelas 35 minuto	MaNuelAB 6 días	MaN723eB 25 días	MaN72* 2 años



Uso de la biometría en la autenticación

La biometría, por otro lado, es mucho más difícil de falsificar y, por lo tanto, es el factor más seguro en una autenticación. Los tokens de seguridad también son muy confiables, pero pueden perderse, ser prestados o ser robados. Las contraseñas de un solo uso OTP por sus siglas en inglés (One-Time Password) son la forma de autenticación más segura, pero pueden ser difíciles de usar por los diferentes pasos que involucra el proceso.

Estructura del proceso de Autenticación de 2 factores:



Fuente: <https://blog.portinos.com/el-dato/como-nos-resguarda-el-segundo-factor-de-autenticacion-de-identidad>

Aunque en sectores como el financiero este tipo de autenticación es más común de lo que se piensa, para otros sectores es algo nuevo y que proporciona mayor confianza cuando se combinan estos métodos. Por ejemplo, la autenticación de dos o más factores, combina dos tipos diferentes de métodos de autenticación. Por otra parte, la biometría también se está volviendo más popular, ya que es más difícil falsificar al usar partes del cuerpo reales de la persona que se autentica.

¿Son seguros los procesos de autenticación en las empresas?

Los procesos de autenticación en las empresas son seguros si utilizan métodos de autenticación que no se pueden adivinar ni descifrar. Por ejemplo, la autenticación de dos factores es más segura porque requiere algo que sepa la persona (como una contraseña) y algo que tenga (como un token proporcionado por una app en el teléfono).

Si se desea un proceso de autenticación más seguro, entonces lo ideal es combinar más de dos factores de autenticación como lo es MFA (Multi Factor Authentication) o en castellano, autenticación multifactor.

Factores o niveles de autenticación:

Simple: Un usuario sabe algo: usuario y contraseña, pin, fecha de nacimiento, etc.

Doble: Un usuario posee algo: en un dispositivo propio tiene un Token, Smart card, pendrive, etc.

Triple: Un usuario es algo: su rostro, voz, huella dactilar, scan de retina, etc.



La autenticación robusta:

Es la capacidad de combinar al menos 3 factores de diferentes niveles de autenticación. Ejemplo:

Robusta: Reconocimiento facial + Token + contraseña, etc.

Este tipo de autenticación es usado más comúnmente en sectores como Salud, Gobierno y Financiero y generalmente es más costoso implementarlo y así mismo, se debe capacitar al usuario para que lo realice correctamente. Sin embargo, el nivel de seguridad que alcanza es mucho más alto que la autenticación simple o de doble factor. Con esto una empresa evita ser víctima de ataques cibernéticos o robo de información que podría afectar su reputación y costar mucho más dinero.



¿Cuál será el futuro de la autenticación en el mundo?

No existe una respuesta única para esta pregunta, ya que el futuro de la autenticación dependerá en gran medida de las necesidades y preferencias específicas de los usuarios individuales, las organizaciones y de los avances tecnológicos en un mundo hiperconectado.

Algunos expertos predicen que los métodos de autenticación biométrica, como el escaneo de huellas dactilares y el iris, serán cada vez más populares en los próximos años. Además, también se espera que se elimine el uso de contraseñas y aumente la implementación de autenticación de dos factores, en la que los usuarios deben proporcionar dos pruebas separadas para verificar su identidad.

Innovación y desarrollo biométrico al servicio de la autenticación segura

Emparejamiento Venoso o comparación de venas, también llamado tecnología vascular, es un nuevo método de autenticación de identidad con un simple escaneo.



Fuente:

https://www.kimaldi.com/aplicaciones/biometria_vascular/utilizar-sistemas-biometricos-para-conseguir-el-balance-perfecto-entre-seguridad-y-usabilidad/



Funciona mediante el uso de una luz led, semi infrarroja y una cámara CCD (Charge Coupled Device) monocromática para tomar una imagen de los vasos sanguíneos en los dedos de la mano de una persona. Así mismo, la circulación sanguínea de las venas permite establecer en tiempo real que la persona autenticada está viva y que es real, evitando la suplantación de identidad. Luego, esta imagen se compara con una base de datos de imágenes conocidas para verificar la identidad de la persona.

Esta tecnología aún se encuentra en sus primeras etapas, pero ya se ha mostrado prometedora como una alternativa más segura a los métodos tradicionales como las huellas dactilares y los escaneos de iris. En Intexus ayudamos a las empresas preocupadas por la seguridad de la información de sus colaboradores, clientes y datos privados corporativos. Contáctanos para recibir más información o agendar una breve asesoría en soluciones de autenticación para empresas.

intexus 
CREANDO UN MUNDO CONFIABLE



www.
intexus
.la

@Intexus  

info@intexus.la

Cel: +57 316 026 0947