La guía esencial para compartir contraseñas de forma segura en las empresas

ManageEngine
Password Manager Pro

Regístrese para obtener una demo personalizada del producto.

ÍNDICE

1 Resumen general

Cualquier organización con una infraestructura de red decente tiene que abrirse paso a través de una multitud de contraseñas administrativas cada día para gestionar los diversos recursos de TI que sostienen su negocio. Sin embargo, el peligro acecha donde reside el verdadero poder, y las contraseñas privilegiadas resultan ser constantemente un punto de acceso favorito para los hackers y los intrusos malintencionados. A pesar de las frecuentes violaciones de datos que se producen en todo el mundo debido a una gestión descuidada de las credenciales, muchas organizaciones siguen sin tomarse en serio las contraseñas y prefieren hacer la vista gorda ante las imprudentes prácticas de compartición de contraseñas de sus empleados.

Hasta la fecha, es habitual que un equipo de administradores de TI comparta casualmente las contraseñas en texto plano a través del chat, el correo electrónico o las notas adhesivas. En efecto, la compartición inadecuada de contraseñas es una de las principales causas de las violaciones de datos y de los delitos informáticos. Según el Informe de Amenazas Internas de 2018, la exposición accidental de información sensible por parte de los empleados es la causa más común de las amenazas internas, el **44% de las cuales se debieron a malas prácticas de compartición de contraseñas.**

Este e-book identifica las prácticas de compartición de contraseñas, tanto deliberadas como accidentales, que pueden acabar comprometiendo las credenciales y abusando de los privilegios. También se incluye una lista completa de reglas básicas que todo equipo de TI debería seguir para almacenar de forma eficaz y compartir de forma segura las credenciales de cuentas privilegiadas; estas prácticas recomendadas pueden ayudar a las organizaciones a hacer frente a las fugas de contraseñas de forma eficiente.

2

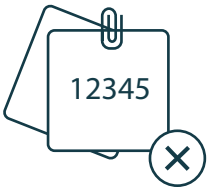
Tipos de prácticas habituales para compartir contraseñas

Tipos de prácticas habituales de compartición de contraseñas que son peligrosas y deben evitarse a toda costa

El acto de compartir contraseñas puede clasificarse a grandes rasgos como deliberado o accidental.

1. Compartir deliberadamente la contraseña

En una organización, la compartición deliberada de contraseñas suele referirse a los empleados que comparten intencionadamente las credenciales de sus cuentas con compañeros de trabajo, contratistas externos o incluso atacantes. Independientemente de la razón por la que un usuario comparte su contraseña con otros, la compartición deliberada de contraseñas es una de las mayores amenazas para las organizaciones.



Almacenar y compartir credenciales en texto plano:

Prácticas como anotar las contraseñas de la empresa en notas adhesivas siguen prevaleciendo en los lugares de trabajo. Aunque estas copias impresas son inmunes a los ataques en línea, son susceptibles de ser expuestas y robadas. Las contraseñas también se almacenan en archivos de texto y hojas de cálculo, y estos archivos suelen guardarse en Dropbox, Google Drive u otras fuentes ampliamente accesibles.

Compartir descuidadamente las credenciales entre empleados y proveedores externos:

Los empleados pueden compartir casualmente las contraseñas privilegiadas con los delegados, sin preverlo, para realizar su trabajo en su ausencia. Las credenciales también se comparten con los nuevos empleados, ya que a menudo no tienen un acceso único a las cuentas necesarias inicialmente. También hay casos en los que las contraseñas privilegiadas se comparten con proveedores externos, normalmente por requisitos empresariales, mantenimiento de la red y solución de problemas de dispositivos defectuosos.

Codificación de credenciales por parte de los técnicos:

En los entornos de DevOps, los ingenieros suelen incrustar las contraseñas de las cuentas root y otras credenciales privilegiadas, como las claves de la API, en texto plano en las configuraciones de las herramientas de DevOps, los scripts de compilación, los archivos de código, las compilaciones de prueba y las compilaciones de producción. Si bien esto puede agilizar el proceso de desarrollo de software y facilitar el proceso de comunicación entre aplicaciones, estas credenciales codificadas son objetivos atractivos para los hackers que buscan brechas. Además, la mayoría de estas credenciales no se modifican y no se someten a rotación por miedo a retrasar los programas de automatización.

Amenaza de empleados antiguos/descontentos:

Según un estudio de IS Decisions, el 36% de los empleados seguía teniendo acceso a los sistemas o datos de su anterior empresa. Los antiguos empleados rara vez encuentran una razón para cumplir con las políticas de seguridad de su antigua empresa, especialmente si tienen intenciones maliciosas, y por lo tanto podrían acceder y hacer mal uso de la información sensible si se les deja con acceso abierto a las redes de su antigua organización. Los empleados descontentos también podrían compartir deliberadamente datos sensibles accesibles con los hackers a cambio de dinero, o darles algún otro uso inmoral, como el uso de información privilegiada.

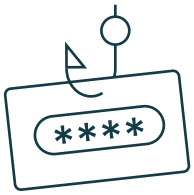
2. Exposición accidental de la contraseña

La exposición accidental, como su nombre indica, se refiere a los casos en los que los usuarios comparten sus credenciales con otra persona sin querer. Los hackers suelen llevar a empleados y usuarios desprevenidos a compartir involuntariamente contraseñas privilegiadas aprovechando tácticas de ingeniería social o llevando a cabo ataques del lado del cliente y basados en la web.

Ingeniería social

La ingeniería social es una táctica utilizada por los hackers para engañar a los usuarios para que revelen información confidencial como contraseñas, números de la seguridad social e información de contacto, con el fin de utilizar estos datos para actividades fraudulentas. Los hackers suelen ocultar sus verdaderas identidades y se presentan como entidades de confianza para manipular a los usuarios a fin de que incumplan las normas de seguridad habituales y cedan información o accesos privilegiados dentro de una organización. La ingeniería social implica la explotación del usuario a través de múltiples medios -incluyendo el phishing, los sitios web falsos, las llamadas telefónicas, las redes sociales y las falsificaciones- con la intención de convencer a los usuarios de que revelen información confidencial o se involucren en transacciones fraudulentas.

Phishing:

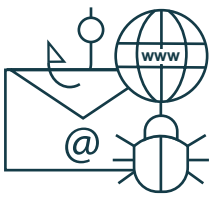


El phishing es uno de los métodos de ingeniería social más comunes utilizados por los hackers para adquirir contraseñas privilegiadas. Un correo electrónico de phishing, una publicación en las redes sociales, un sitio web, una llamada telefónica o un mensaje de voz (phishing de voz o vishing) parecen legítimos, pero en realidad pretenden engañar a los destinatarios para que hagan clic en enlaces maliciosos e introduzcan información personal u oficial.

El phishing suele consistir en crear una sensación de urgencia y pánico entre las víctimas. Por ejemplo, un hacker puede alegar que la víctima es morosa en el pago de sus impuestos o facturas, hacerse pasar por su jefe para pedirle que comparta un correo electrónico con datos confidenciales, o hacerse pasar por un colega o un familiar para recopilar información confidencial.

Los hackers envían correos electrónicos de phishing de forma masiva para dirigirse a un público general con la esperanza de que unos pocos desafortunados muerdan el anzuelo. Según una encuesta realizada en 2017 por Webroot, **cada mes se crean 1,4 millones de sitios web de phishing**; dada su popularidad, es evidente que los ataques de phishing deben tener éxito.

Spear phishing:



El spear phishing es una estafa por correo electrónico dirigida a personas, organizaciones o empresas concretas. En lugar de enviar miles de correos electrónicos para atrapar a unas pocas víctimas, el spear phishing se dirige a grupos selectivos de personas que tienen algo en común: trabajan para la

misma organización, estudian en la misma universidad, tienen intereses de compra similares (gracias a las cookies de terceros) o realizan operaciones bancarias con la misma organización financiera.

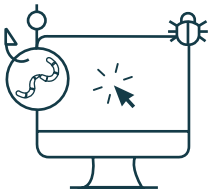
Whaling:

El whaling (o whale phishing) es un ataque de spear phishing que va un paso más allá al dirigirse a los directores generales y a los propietarios de las empresas, ya que suelen tener acceso a la información más sensible de la compañía. Una vez que el equipo de un superior está comprometido, los atacantes tienen autoridad virtual sobre toda la red de la organización. Los atacantes pasan meses investigando a sus víctimas para poder elaborar un correo electrónico que parezca lo más legítimo posible, dado que las personas de alto perfil suelen ser más cuidadosas cuando se trata de abusos en Internet.

Spoofing:

El spoofing es un tipo de estafa en línea que se utiliza para recopilar información personal de los usuarios, principalmente a través de sitios web fraudulentos que parecen legítimos. Las ventanas emergentes y los anuncios que aparecen en las ventanas de navegación de la nada son ejemplos comunes de este tipo de ataque.

Baiting:



El "baiting" se aprovecha de la codicia y la curiosidad humanas y se diferencia del "phishing" en que promete a las víctimas bienes y servicios a cambio de información sensible: contraseñas, información de identificación personal (PII), ubicaciones físicas, etc. "Haga clic aquí para reclamar sus 100 dólares", "¡Descargue cientos de películas y canciones gratis!" son ejemplos de carnada colocados para atraer a las víctimas. Una vez que el usuario haga clic en estos enlaces, se le pedirá que inicie sesión para obtener su premio; al hacerlo, compromete sus credenciales de acceso.

Watering hole attack:

Se trata de un ataque selectivo en el que los atacantes buscan vulnerabilidades en sitios web que probablemente sean visitados por sus víctimas elegidas. Una vez comprometidas las vulnerabilidades, el sitio puede ser utilizado para instalar un troyano de puerta trasera en el dispositivo del objetivo. Un troyano de puerta trasera es un software malicioso que proporciona al atacante un canal encubierto a través del cual puede acceder, enviar comandos o controlar un equipo comprometido.

Ingeniería social inversa:

Este enfoque implica tres pasos: el sabotaje inicial, el ofrecimiento de alivio y apoyo, y la penetración. En primer lugar, los hackers emplean un ataque oportunista para destruir el dispositivo del objetivo. Después, envían correos electrónicos de phishing o ejecutan un ataque DoS (un tipo de ataque en el que los atacantes intentan impedir que los

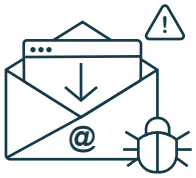
usuarios legítimos accedan a los servicios) para garantizar que el departamento de TI de la organización sepa que está en riesgo de ser comprometido. A continuación, se presentan como consultores de seguridad o una agencia de asistencia técnica, y ofrecen asistencia para solucionar el problema. Finalmente, una vez designados para resolver el problema (¡que ellos mismos provocaron!), ejecutan fácilmente la actividad maliciosa, como la instalación de malware o keyloggers, o el robo de datos confidenciales.

Ataques del lado del cliente y basados en la web

Los ataques del lado del cliente y de la web explotan la confianza entre los usuarios y los sitios web que visitan o los servidores con los que interactúan. Este tipo de ataques se dirigen a las vulnerabilidades de las aplicaciones cliente que interactúan con un servidor corrupto, y requieren interacciones del usuario como hacer clic en un enlace malicioso, rellenar un formulario con datos personales, abrir un documento o simplemente visitar un sitio web. Estos ataques son alimentados por prácticas accidentales de compartición de contraseñas dentro de una organización.

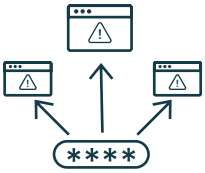
Spyware:

El spyware es un tipo de malware que se hace pasar por una aplicación legítima y se incrusta en el dispositivo de la víctima sin que ésta lo sepa, donde monitorea sus actividades en Internet y espía su información sensible. A continuación, el malware transmite estos datos sensibles a anunciantes, empresas de datos o usuarios externos. Algunos tipos de spyware pueden instalar software malicioso adicional y cambiar la configuración de los dispositivos afectados.



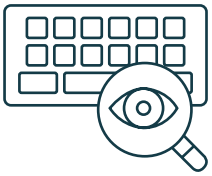
Descargas de tipo "drive-by":

Como resultado del perfeccionamiento de sus tácticas, los delincuentes informáticos han encontrado nuevas formas de propagar su software malicioso sin requerir mucha interacción del usuario. Las descargas drive-by son programas maliciosos que los usuarios instalan inadvertidamente en sus dispositivos por el simple hecho de abrir un correo electrónico o navegar por un sitio web fraudulento. Este malware se sitúa en el dispositivo de la víctima y espera a que introduzca sus credenciales o cualquier dato sensible en un formulario online aleatorio para poder capturar esa información.



Ataque de relleno de credenciales (credential stuffing):

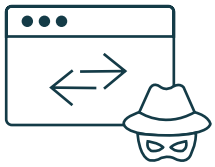
El relleno de credenciales se refiere al proceso en el que un atacante ejecuta un script automatizado que prueba una multitud de credenciales violadas que están fácilmente disponibles en línea -gracias a la Dark Web- para iniciar sesión en un sitio web o una aplicación de destino. Este tipo de ataque suele funcionar ya que la mayoría de los usuarios reutilizan las mismas credenciales en varias cuentas, y una sola violación de datos condena a varias identidades en línea.



Keyloggers:

Los keyloggers son software potentes que roban información sensible capturando las pulsaciones del teclado de un usuario. Un hacker se introduce primero en el sistema de la víctima a través del phishing u otros ataques, y luego emplea un virus troyano como herramienta de entrega para instalar un keylogger. Los keyloggers ayudan a los atacantes a interceptar

las entradas en los teclados y adquirir contraseñas, números de cuenta, códigos de seguridad y otros datos sensibles.



Secuestro de sesión:

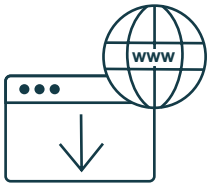
El secuestro de la sesión se refiere a cuando un atacante se apodera de una sesión activa de un usuario de la web obteniendo de forma encubierta su ID de sesión, que normalmente se almacena en las URL y las cookies de la web. Una vez que el atacante obtiene el ID de sesión, puede tomar posesión completa de la sesión y hacer todo lo que el usuario está autorizado a hacer en la web.

Ataque Man-in-the-middle:

Se trata de un tipo de secuestro de sesión en el que el atacante se inserta como proxy en una conversación para interceptar y acceder a la información transferida entre dos entidades. Por ejemplo, un hacker puede lanzar un ataque man-in-the-middle cuando los usuarios se unen sin saberlo a una red Wi-Fi maliciosa que parece ser legítima, e interceptar todos los datos que esos usuarios transfieren a la red. Esta red Wi-Fi fraudulenta que se establece para interceptar las comunicaciones inalámbricas se denomina gemelo malvado (evil twin).

Ransomware:

El ransomware es un programa malicioso que se instala secretamente en un dispositivo (a menudo a través de phishing) y ejecuta un script para cifrar todos los archivos valiosos del sistema. El programa se replica gradualmente y se extiende por la red, infectando servidores y otros endpoints. A continuación, obliga a la víctima a pagar un rescate por la clave para descifrar los archivos. Según Cybersecurity Ventures, los daños causados por el ransomware alcanzaron los 5.000 millones de dólares en 2017.



Troyanos de acceso remoto (RAT):

Los RAT son programas maliciosos que suelen descargarse silenciosamente cuando un usuario solicita un programa (como un juego o una película), o que se envían como un archivo adjunto de correo electrónico. Son casi imposibles de detectar porque normalmente no aparecen en la lista de programas o tareas en ejecución, y funcionan como programas legítimos. Los RAT pueden iniciar varias acciones desde el dispositivo de destino, como activar su cámara web y grabar sesiones; realizar capturas de pantalla; distribuir virus y software; formatear discos; o eliminar, editar o descargar archivos.

Una vez comprometido el sistema objetivo, un RAT permite al intruso tener privilegios administrativos. Al replicarse, un RAT establece un malware de tipo botnet que analiza e infecta automáticamente todos los sistemas susceptibles de la red mediante un ataque de fuerza bruta. Así, un atacante puede obtener rápidamente el control completo de todas las cuentas privilegiadas de una organización.

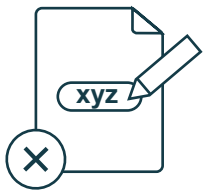
3

Directrices para compartir de forma segura las contraseñas

Aunque lo ideal es evitar por completo compartir las contraseñas administrativas para escapar de las garras de las diversas amenazas mencionadas anteriormente, los requisitos prácticos de la empresa exigen que se compartan algunas contraseñas de forma selectiva.

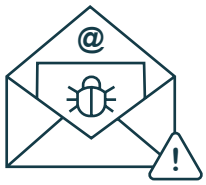
Cómo puede usted, como usuario individual, garantizar la seguridad de las contraseñas.

Es responsabilidad de todos los empleados velar por el cumplimiento de las buenas prácticas en el lugar de trabajo y contribuir a frenar los delitos informáticos. Así es como puede contribuir.



Deje de guardar las contraseñas en texto plano:

En el momento en que crea una contraseña, es suya para cuidarla. Exponer o compartir contraseñas en texto plano a través de notas adhesivas, hojas de cálculo, archivos de texto y fuentes en línea es peligroso, y puede resultar catastrófico para su organización una vez que los hackers las descubran. Si su organización utiliza un gestor de contraseñas, debería utilizar la herramienta para ocultar sus contraseñas en formatos cifrados.



Sea precavido con los correos electrónicos:

Algunos correos electrónicos van a la carpeta de spam por una razón. Preste mucha atención a los correos electrónicos sospechosos, especialmente los que le piden que abra los archivos adjuntos o que haga clic en los enlaces. No abra los archivos adjuntos potencialmente peligrosos, como los archivos PDF incluidos en mensajes de correo electrónico de remitentes desconocidos.

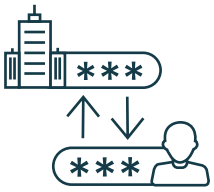
Compruebe la legitimidad de las URL de sitios web sospechosos que se proporcionan en los correos electrónicos pasando el cursor por encima del hipervínculo y comprobando el sitio web al que le llevará (se muestra en la esquina inferior izquierda de la pantalla). Asegúrese de que el sitio web que ve pertenece al remitente del correo electrónico. Si observa una dirección de sitio web con aspecto sospechoso, debe eliminar dicho correo electrónico. También puede copiar la dirección del enlace (sin abrirlo) y verificar si es auténtico utilizando un sitio web como VirusTotal.

Proteja su navegador web:

Mantenga su navegador actualizado y seguro por todos los medios. Revise lo que está marcado y desmarcado en la configuración de privacidad y seguridad de su navegador. Por ejemplo, active la opción de "Navegación segura" para proteger su dispositivo de sitios peligrosos, y garantice que su navegador bloquee las cookies de terceros, impidiendo así que los anunciantes rastreen su actividad en línea. Tenga cuidado de no descargar plug-ins y extensiones de fuentes no seguras. Evite hacer clic en las ventanas emergentes que parezcan sospechosas.

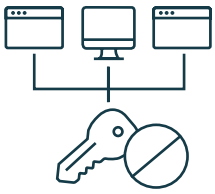
Evite conectarse a redes públicas que no estén protegidas por contraseña:

Los atacantes suelen instalar puntos de acceso Wi-Fi públicos y maliciosos para que los usuarios se conecten a ellos. No utilice las redes públicas (disponibles en parques, hoteles, aeropuertos, estaciones de tren, etc.) para realizar intercambios de datos oficiales o transacciones en línea.



No combine las contraseñas personales con las de la empresa:

Asegúrese de no utilizar las mismas credenciales para las cuentas personales y las de la empresa, ya que una cuenta comprometida podría significar el fin de otra.

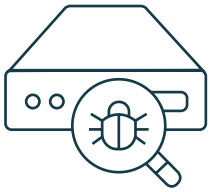


Evite encadenar contraseñas:

El encadenamiento de contraseñas se refiere al uso de una única contraseña para una multitud de cuentas en varios sitios web, aplicaciones y servicios. Aunque parezca cómodo tener una contraseña común para todas las cuentas, es uno de los factores que contribuyen a la mayoría de las violaciones. Cree contraseñas únicas para cada cuenta, de modo que compartir las credenciales de una cuenta no signifique que las credenciales de todas las demás queden expuestas.

Aléjese de las pistas sobre la contraseña:

¿Recuerda preguntas como "¿Cuál es su color favorito?", cuyas respuestas conocía de antemano? Si le ayudan a recordar una contraseña, probablemente también proporcionarán una ventaja a los atacantes que buscan comprometer sus cuentas.



Analice todos los dispositivos externos en busca de malware:

Realice un análisis adecuado al conectar dispositivos externos (pendrives, discos duros, etc.) a sus dispositivos de trabajo para garantizar que estén libres de malware y virus. Conectar un dispositivo limpio a otro infectado por malware es peligroso, ya que la infección puede transmitirse durante la conexión.

Cómo puede usted, como jefe responsable de TI, garantizar la seguridad general de las contraseñas.

He aquí algunos pasos para salvaguardar la información sensible de su organización y hacer de la gestión segura de contraseñas una prioridad en su organización.

Establezca una cultura que prohíba compartir contraseñas, a menos que sea absolutamente necesario:

Es responsabilidad de todos garantizar la seguridad en cada paso del ciclo de vida de las TI. Establezca una cultura dentro de su organización que prohíba a los usuarios compartir sus credenciales a través de cualquier medio. El miedo a enfrentarse a graves repercusiones será de gran ayuda para obligar a los empleados a cumplir las políticas de la empresa.

Implemente una política de escritorio limpio:

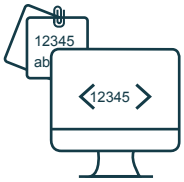
Una política de escritorio limpio garantiza que los documentos, las cartas, los libros y cualquier otra cosa que contenga datos confidenciales se guarden bajo llave. Proporcione a todos los

usuarios las herramientas necesarias (casilleros, sistemas de copia de seguridad de los documentos electrónicos, etc.) y garantice que todos los empleados sigan religiosamente la política, incluidos los altos cargos.

Establezca una política de separación de funciones:

DevOps consiste en la colaboración entre varios equipos: codificadores, desarrolladores, control de calidad, ingenieros de operaciones, equipos de seguridad, etc. Para mantener un ambiente de trabajo saludable, establezca funciones más claras para todos dentro del entorno DevOps, de modo que el acceso de los empleados no exceda el alcance de sus trabajos. Esto mantendrá a raya las prácticas negligentes, como la de un desarrollador poco riguroso que introduce una puerta trasera en el código base y la pasa al entorno de producción sin ninguna inspección.

Evite la codificación de credenciales:



Frene la práctica de codificar las credenciales y las claves de seguridad en texto plano, y haga que el proceso de revisión del código de cada ingeniero compruebe si hay información sensible directamente incrustada.

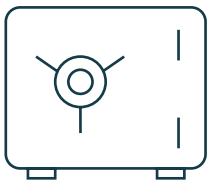
Invierta en la seguridad de la API:

Un entorno típico de DevOps exige compartir tokens de autenticidad y servicios a través de API compartidas y seguras. Utilice herramientas de seguridad de API que puedan proteger sus API, evite consecuencias no deseadas

al compartir información y garantice que los recursos sean accesibles de forma segura por grupos internos, socios, clientes y desarrolladores de terceros.

Cómo puede usted, como jefe responsable de TI, garantizar la seguridad de las contraseñas mediante una herramienta de gestión de contraseñas.

A continuación se explica cómo puede utilizar una herramienta de gestión de contraseñas segura para poner fin a las actividades peligrosas de intercambio de contraseñas en su organización.

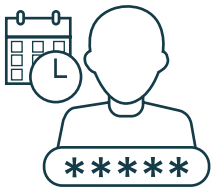


Almacene todas sus contraseñas en una bóveda centralizada y cifrada:

Opte por un gestor de contraseñas que almacene y proteja todas sus contraseñas utilizando algoritmos de cifrados seguros como el AES-256. Evite la mala gestión de las contraseñas privilegiadas consolidando las contraseñas de todos sus departamentos en un repositorio centralizado y administrando el control directo sobre ellas.

Utilice un generador de contraseñas integrado:

Su gestor de contraseñas debería ayudarle a hacer algo más que almacenar contraseñas: también debería ayudarle a generar contraseñas únicas y complejas para todas sus cuentas y quitarle de encima la tarea de recordarlas todas.

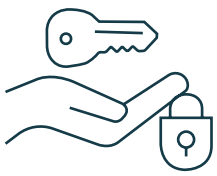


Descubra por qué los usuarios necesitan contraseñas:

Establezca una política que obligue a los usuarios a enviarle a usted o a otros administradores solicitudes de acceso siempre que necesiten acceder a determinados recursos, junto con una razón clara de por qué necesitan acceder a ese recurso en particular. Proporcióneles un acceso temporal, basado en el tiempo, a estas credenciales, y aproveche las opciones integradas para revocar el acceso cuando el tiempo estipulado haya terminado. Restablezca automáticamente las contraseñas una vez que los usuarios se registren.

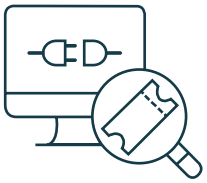
Comparta el acceso a los recursos de TI críticos sin revelar sus contraseñas en texto plano:

Proporcione a los empleados acceso a sus recursos sin revelar las credenciales en texto plano. En su lugar, utilice una herramienta de gestión de contraseñas que también les permita iniciar conexiones con un solo clic a los dispositivos de destino, sin tener que ver o introducir manualmente las credenciales.



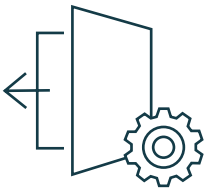
Comparta contraseñas con diferentes privilegios de acceso en función de las necesidades:

Al compartir las credenciales de los recursos, es esencial que las organizaciones impidan el acceso y los derechos de privilegio excesivos. La mayoría de las veces, proporcionar a los usuarios un acceso de sólo lectura a una contraseña es suficiente para hacer el trabajo. Dar a un usuario acceso total a una contraseña en realidad le otorga autoridad total sobre las contraseñas compartidas, incluyendo derechos de edición.



Integre su gestor de contraseñas con un sistema de generación de tickets:

Integre su gestor de contraseñas con un sistema de generación de tickets adecuado para validar automáticamente las solicitudes de servicio relacionadas con el acceso privilegiado. Esto garantizará que los usuarios sólo puedan acceder a las contraseñas privilegiadas con un ID de ticket válido.



Configure el cierre de sesión automático para las sesiones inactivas:

Puede configurar periodos de tiempo de espera para que los usuarios cierren automáticamente la sesión de la herramienta de gestión de contraseñas tras una inactividad prolongada. Esto mantendrá sus contraseñas guardadas de forma segura, incluso si un usuario se olvida de cerrar la sesión del navegador de su cuenta.

Supervise el estado de sus contraseñas y restablézcalas periódicamente:

Un gestor de contraseñas le ayuda a determinar la solidez y la antigüedad de las mismas. Habilite el restablecimiento automático de las contraseñas para deshacerse de las que no han sido modificadas o han caducado, así como para garantizar que los empleados no puedan utilizar contraseñas antiguas para acceder sin autorización.

Active la autenticación de dos factores:

Implemente la autenticación de dos factores mediante software o hardware para verificar la identidad de cualquier usuario que inicie sesión a su herramienta de gestión de contraseñas.

Maneje las cuentas de los antiguos empleados de manera responsable:

Cuando un usuario decide dejar su organización, recuerde siempre eliminar todas sus cuentas asociadas a los recursos de TI tras su salida. Los antiguos empleados que siguen teniendo un acceso descontrolado a sus cuentas privilegiadas suponen una grave amenaza para su organización. Prepare un informe de salida que contenga detalles de los recursos a los que han tenido acceso durante su estancia en la organización y garantice que las contraseñas de todas las cuentas de esos recursos se restablezcan inmediatamente.

Registre lo que un usuario hace con sus contraseñas:

Audite cada una de las operaciones de los usuarios y establezca la transparencia de todas las actividades relacionadas con las contraseñas privilegiadas integrando su herramienta de gestión de contraseñas con una herramienta interna de registro de eventos. Genere informes para obtener una visión general de quién hizo qué con una contraseña, dónde y cuándo.

4 Conclusión

La ignorancia es una bendición, pero no cuando la seguridad de la TI de su organización está en juego

A medida que los ataques cibernéticos se vuelven más sofisticados, todos los responsables de TI deben adoptar un enfoque proactivo para salvaguardar sus datos. Ya es hora de que las organizaciones protejan sus contraseñas privilegiadas utilizando una herramienta eficaz y políticas estrictas. Seguir los consejos anteriores le ayudará a abordar y mitigar los riesgos asociados a la exposición accidental y deliberada de las credenciales. Además, las organizaciones deben garantizar que todos los usuarios finales conozcan los peligros de compartir contraseñas. Cuanto mejor formados estén los empleados en cuanto a la seguridad de las contraseñas, menos probabilidades tendrán de ser objetivo de los delincuentes informáticos.

www.manageengine.com/pim

ManageEngine
Password Manager Pro

Zoho Corporation Private Limited
4141 Hacienda Drive Pleasanton, CA 94588, USA
Teléfono: +1-925-924-9500
Fax: +1-925-924-9600
Email: sales@manageengine.com
www.manageengine.com/pim