RESOURCE CENTER

Five Best Practices for Enterprise Password Management

Learn the best practices for enterprise password management in this white paper.

Get the full interactive view at https://bitwarden.com/es-la/resources/five-best-practices-for-password-management-white-paper/

bitwarden

Mientras las organizaciones siguen haciendo de la seguridad una prioridad, una parte importante de ese esfuerzo implica educar y capacitar a los usuarios en general sobre las mejores prácticas. Considere algunas de estas estadísticas del Informe sobre el estado de la autenticación de contraseñas y seguridad de Yubico 2019 Comportamientos de seguridad :

- 2 de cada 3 encuestados comparten contraseñas con sus colegas
- El 51% de los participantes afirma reutilizar sus contraseñas en cuentas personales y profesionales.
- El 57% afirma no haber cambiado sus contraseñas tras sufrir un intento de phishing.

Para introducir cambios en una empresa, los equipos de seguridad y TI deben educar a los empleados sobre las mejores prácticas. En lo que respecta a la gestión de contraseñas, una de las formas más sencillas de fomentar una buena higiene de contraseñas es implantar una solución de gestión de contraseñas en todo el lugar de trabajo. He aquí algunas buenas prácticas que conviene adoptar.

1. Utilice una solución de gestión de contraseñas

A lo largo del día, la mayoría de la gente visita muchos sitios diferentes que requieren contraseñas. Memorizar muchas contraseñas (o frases de contraseña) únicas y suficientemente seguras es prácticamente imposible. Un gestor de contraseñas simplifica el uso de contraseñas en diferentes sitios para que los usuarios estén más seguros. Existen varios gestores de contraseñas sólidos. Dé prioridad a las que funcionen en varias plataformas y ofrezcan servicios gratuitos o a muy bajo coste para particulares. La mayoría de las funciones de los gestores de contraseñas también se han ampliado con los años.

2. Elija una herramienta que pueda implantar fácilmente en toda su organización

Los gestores de contraseñas deben ser fáciles de usar para todos los niveles de usuario, desde principiantes hasta avanzados. Si se tiene en cuenta una base de empleados grande o distribuida, las aplicaciones deben ser intuitivas para el usuario y fáciles de implantar. Por ejemplo, tanto si elige Bitwarden Cloud como si despliega su propia instancia autoalojada, poner Bitwarden en marcha es fácil. Y Bitwarden Directory Connector funciona con los servicios de directorio más utilizados en la actualidad, como Azure, Active Directory, Google, Okta y otros, para mantener a sus usuarios de Bitwarden sincronizados con sus equipos y empleados.

3. Cambie las contraseñas sólo cuando puedan haber sido comprometidas

Se acabaron los días de cambiar de contraseña cada tres meses. Ahora sólo deberías cambiarlos si crees que te han puesto en peligro. El Instituto Nacional de Normas y Tecnología (NIST) no recomienda que los usuarios cambien las contraseñas con frecuencia. En realidad, esto conduce a un comportamiento que puede resultar en contraseñas más débiles con el tiempo. Puedes determinar si una contraseña se ha visto comprometida consultando pruebas tangibles, como un fraude con tarjeta de crédito, o utilizando una herramienta (como tu gestor de contraseñas) que pueda decirte si tu contraseña ha quedado expuesta en una brecha.

4. Utilice contraseñas seguras y únicas

El uso de contraseñas seguras y únicas para cada servicio que utilice en línea ayuda a minimizar el impacto de las filtraciones de datos. Una contraseña segura no significa necesariamente añadir caracteres especiales o números a una palabra o nombre común, sino aumentar la entropía o aleatoriedad de la contraseña. Una táctica sencilla para crear una contraseña segura es utilizar una frase de contraseña. Una frase de contraseña combina palabras o frases aparentemente inconexas que el usuario puede recordar fácilmente pero que, de otro modo, serían difíciles de adivinar por un atacante. Las frases de contraseña tienen un alto grado de entropía y, al mismo tiempo, son fáciles de recordar.

5. Active la autenticación de dos factores siempre que sea posible

Con la autenticación de dos factores (2FA) cada vez más común en los sitios web de consumidores y empresas, un buen gestor de contraseñas incluirá formas de ampliar esta función. El uso de 2FA aumenta la seguridad de su cuenta al exigirle que introduzca otro token además de su contraseña maestra. Aunque alguien descubriera tu contraseña maestra, no podría iniciar sesión en tu gestor de contraseñas sin acceder al token adicional. Si quieres empezar a utilizar un gestor de contraseñas, puedes registrarte para obtener una cuenta gratuita en Bitwarden aquí.