Hewlett Packard Enterprise

29 de febrero de 2020

La seguridad de las pequeñas empresas requiere la utilización de un administrador de contraseñas

Las contraseñas débiles son la clave para los atacantes que intentan hacerse con tus activos. Por ahora, las contraseñas son inevitables, pero con el software adecuado tu equipo podrá usarlas de forma segura.

Por Larry Seltzer, director editorial de Enterprise.nxt en Hewlett Packard Enterprise

Las contraseñas son, en muchos sentidos, un fracaso como medida de seguridad. Las contraseñas débiles y vulnerables son una de las principales formas en las que los usuarios, los sistemas y los datos se ponen en riesgo. Piensa en las cuentas en línea de tu pequeña o mediana empresa y en el daño que un delincuente podría hacerte si tuviese acceso a ellas. Piensa en el daño que un intruso podría causar con una cuenta de administrador en tu red antes de que te conviertas en la última víctima de **ransomware**.

Mientras tanto, las contraseñas débiles y vulnerables ponen en riesgo a los usuarios y a las empresas diariamente. Constantemente se escucha hablar sobre las vulneraciones de contraseñas. ¿Juegas a Palabras con amigos? En septiembre, un pirata informático **robó los datos de usuario de 218 millones de usuarios de Palabras con amigos** de Zynga, la empresa que ha creado el juego. Puedes comprobar si has sido uno de los afectados consultando **Have I Been Pwned? (HIBP)** («¿He sido víctima?»), un sitio web que recopila los datos de tales vulneraciones para que los usuarios puedan comprobar si les afectan. A finales de 2019, el número total de cuentas afectadas en la base de datos de HIBP era de más de 9000 millones, de las cuales 5 081 613 319 se encontraban entre las 10 vulneraciones de seguridad más graves.

Los atacantes toman las credenciales robadas de un servicio y las utilizan para intentar acceder a otros. Esto se conoce como **relleno de credenciales** y las consecuencias pueden ser muy graves. ¿Reutilizas el mismo nombre de usuario (probablemente tu dirección de correo electrónico) y contraseña en más de un sitio?

Se están adoptando medidas de seguridad mejores que las contraseñas, pero conllevan sus propios problemas y no funcionan con todos los sitios a los que los usuarios podrían necesitar acceder. Así que, desde el punto de vista práctico, la mayoría de las organizaciones, en particular las más pequeñas, se verán obligadas a seguir utilizando contraseñas durante algún tiempo. Llegados a este punto, la pregunta es la siguiente: ¿Cuál es la forma más segura

a00098971ese, abril de 2020

Hewlett Packard Enterprise

—o menos insegura, si lo prefieres— de usarlas? La respuesta es seguir las mejores prácticas, y la única forma práctica de seguirlas es utilizando un administrador de contraseñas.

Contraseñas adecuadas

- Entre las mejores prácticas, es decir, aquello que sabes que deberías hacer, pero que no harás porque resulta muy difícil, se encuentran las siguientes:
- No reutilizar contraseñas. Utilizar una contraseña diferente para cada sitio web.
- Utilizar contraseñas relativamente largas y complejas como «8&TifWT4h6jS06», en lugar de contraseñas fáciles de recordar como «vivaelfutbol».
- Asegúrate de que tus contraseñas no están en ninguna de las muchas listas de contraseñas vulnerables.

Resulta difícil hacer todas estas cosas por nuestra cuenta. Sin embargo, con la ayuda de un administrador de contraseñas, los usuarios pueden seguir las mejores prácticas más fácilmente. Un administrador de contraseñas es un programa que se ejecuta en el ordenador o en el teléfono y registra los nombres de usuario y las contraseñas que se utilizan para acceder a los diferentes sitios web. También hace otras cosas, pero esa es su función principal. En **este vídeo de YouTube** puedes acceder a una rápida demostración y explicación de cómo trabajan los administradores de contraseñas.

Puedes establecer una contraseña segura para el administrador de contraseñas, idealmente en combinación con un segundo factor como una **aplicación de contraseñas de un solo uso** o una **clave de seguridad**. Cuando tu aplicación, generalmente tu navegador, recibe un aviso de inicio de sesión de un sitio web, el administrador de contraseñas se da cuenta, busca ese sitio en su base de datos y facilita el nombre de usuario y la contraseña de ese sitio. Si tienes más de un usuario para ese sitio web, te facilitará todos ellos y te permitirá escoger.

La base de datos del administrador de contraseñas está fuertemente cifrada, tanto localmente como en el almacenamiento en la nube del proveedor. Normalmente, el proveedor no almacena las credenciales de tu administrador de contraseñas, por lo que, si pierdes las credenciales, probablemente hayas perdido toda la base de datos. El resultado de esto podría ser catastrófico, pero es fundamental para que los administradores de contraseñas sean lo suficientemente seguros.

Para más información sobre los fundamentos de los administradores de contraseñas, consulta este artículo sobre los **administradores de contraseñas en grandes empresas**.

Licencias multiusuario

Los administradores de contraseñas comenzaron y siguen consistiendo principalmente en una compra para un solo usuario, a veces en forma de versión gratuita limitada. Pero si eres el responsable de la seguridad de múltiples usuarios en una pequeña o mediana empresa, deberías buscar una opción que ofrezca cierta capacidad de gestión y un descuento por volumen. Muchos proveedores de administradores de contraseñas cuentan con versiones para equipos, familias y empresas.

Los productos verdaderamente diseñados para grandes empresas dispondrán de herramientas inadecuadas para las pequeñas empresas y su precio será más elevado. Dicho de forma general, si cuentas con una red administrada profesionalmente, estos productos pueden resultar apropiados para ti.

a00098971ese, abril de 2020

Hewlett Packard Enterprise

A continuación se presenta una lista de administradores de contraseñas dirigidos a grandes empresas, pero que no disponen de una integración empresarial completa. No esperaba que existiesen tantos productos de este tipo, y puede que me haya olvidado de alguno.

- **LastPass Teams**
- **1Password Business**
- **RoboForm for Business**
- **Dashlane Comercial**
- **Keeper Business**
- **Zoho Vault for teams**
- **Password Boss for business**
- **StickyPassword for teams**
- **Bitwarden Teams**
- **TeamsID Business Password Manager**
- **TeamPassword**

La principal función para equipos que ofrecen estos productos consiste en la posibilidad de compartir la información de acceso con otros usuarios. Probablemente también permitan que un administrador gestione los usuarios. El administrador puede incorporar nuevos usuarios, gestionar de forma centralizada los elementos compartidos y quién tiene acceso a ellos, autorizar y desautorizar dispositivos, controlar el acceso a las funciones del administrador de contraseñas y mucho más.

Puede incluir un sistema de gestión de derechos para controlar quién tiene acceso a qué, así como controlar los niveles de acceso. No voy a detallar qué productos cuentan con cada una de estas funciones porque esa información cambia con el tiempo, así que tendrás que compararlos tú mismo cuando llegue el momento de tomar una decisión.

Y estas son solo las funciones para equipos. Pueden existir diferencias significativas de precio entre los productos, y es posible que algunos sean más fáciles de usar que otros. Aunque no compara las funciones para equipos ni otras características de gestión, PCMag elabora reseñas con regularidad sobre los administradores de contraseñas, e incluye **un resumen reciente de 10 de ellos**.

Es posible que te hayas dado cuenta de que Google Chrome tiene un administrador de contraseñas incorporado. De hecho, se trata de una de las características de las cuentas de Google, que, para la mayoría de la gente, son de Gmail. Si tu organización utiliza **G Suite**, las aplicaciones de productividad basadas en la nube de Google, el administrador puede realizar **algunas tareas de gestión**, como:

- Solicitar una contraseña segura y establecer un nivel de seguridad determinado basado en la herramienta de seguridad de contraseñas de Google.
- Establecer una longitud mínima en la contraseña.

a00098971ese, abril de 2020

Hewlett Packard Enterprise

- Permitir o impedir que se reutilicen contraseñas antiguas.
- Establecer la caducidad de la contraseña, es decir, el número de días tras los cuales el usuario debe cambiar la contraseña. Como veremos más adelante, esto ya no se incluye entre las mejores prácticas.
- Cualquier administrador de contraseñas de terceros para equipos proporciona mucho más que esto.

Seguridad frente a usabilidad

Una vez que se disponga de un sistema como este, se podrán empezar a aplicar las mejores prácticas descritas anteriormente. Casi todos los productos realizarán un análisis y generarán un informe sobre las contraseñas almacenadas en el que se indicarán las contraseñas duplicadas y las poco seguras. Puedes utilizar este informe para reforzar la seguridad del uso de contraseñas en tu negocio.

Es importante valorar que existe un equilibrio general entre seguridad y usabilidad, no solo en la tecnología, sino en la vida: solo hay que intentar subir a un avión para entender esta idea. Como tal, los administradores de contraseñas no facilitan el uso de las contraseñas, sino que facilitan el uso de las contraseñas *de forma segura*.

Todos los administradores de contraseñas pueden suponer un desafío en términos de usabilidad para el usuario medio. Puede que desees comenzar el proceso migrando de uno en uno los inicios de sesión en el sistema de administración de contraseñas. También podrías mover a diferentes usuarios en diferentes momentos, permitiéndoles así acostumbrarse al sistema mientras siguen pudiendo utilizar las contraseñas a la antigua usanza. Pero si lo haces de esta forma, tendrás que posponer el objetivo principal de usar un administrador de contraseñas, es decir, hacer que tus contraseñas sean más seguras, ya que no se podrían gestionar los inicios de sesión de los usuarios que no se encuentren en el administrador de contraseñas.

¿Por qué los administradores de contraseñas suponen un reto para los usuarios? La principal razón es que no siempre funcionan. Sin embargo, no te apresures a juzgar con severidad a los administradores de contraseñas. Para cumplimentar los nombres de usuario y las contraseñas en los campos de inicio de sesión de forma automática, los administradores de contraseñas tienen que poner en marcha acciones similares a las de un software malicioso que intenta atacar al usuario. Por lo tanto, los navegadores y los sitios web adoptan medidas defensivas que, a menudo, obstaculizan al administrador de contraseñas a la par que a los ataques reales.

Me surge este problema con el sitio web de mi banco personal, un banco muy grande e importante. La opción de completar automáticamente el campo de la contraseña lleva años sin funcionar. He probado dos administradores de contraseñas diferentes para esto, y ninguno ha funcionado. La solución alternativa no está mal: hay que ir al icono del administrador de contraseñas, ya sea en el campo de entrada o en la barra de extensiones del navegador, utilizarlo para copiar la contraseña en el portapapeles y luego pegarla manualmente. No es para tanto, pero no debería ser así. Como la aplicación móvil del banco permite el uso de las huellas dactilares y el reconocimiento facial en el dispositivo, este problema no ocurre en mi teléfono.

Un documento normativo reciente del Instituto Nacional de Estándares y Tecnología recomienda específicamente que los sitios web se esfuercen en ser compatibles con los administradores de contraseñas, pero el mensaje no ha calado. (Este podría ser un buen momento para comprobar si tus sistemas de acceso a Internet permiten que tus clientes utilicen los administradores de contraseñas sin problemas).

Usar un administrador de contraseñas nunca será tan fácil como utilizar una contraseña de la forma insegura a la que estamos acostumbrados. Los administradores de contraseñas se presentan como una verdadera carga para los usuarios desmotivados. Por lo tanto, cuando les expliques el plan a tus usuarios, debes transmitirles lo importante que es para la empresa que se tomen en serio la seguridad de las contraseñas. Un cambio así resulta tan importante

a00098971ese, abril de 2020

Hewlett Packard Enterprise

como cualquier otra tecnología que puedas implementar y te ayuda a sacar el máximo provecho de tus sistemas y procedimientos de seguridad.

Administradores de contraseñas: lecciones para puestos directivos

- Insiste en llevar a cabo las mejores prácticas en contraseñas de tus sistemas internos y tus cuentas externas con proveedores y partners.
- Conseguir que la seguridad funcione correctamente es difícil si los empleados no están motivados. Asegúrate de que los empleados entiendan la importancia que supone para la empresa que se tomen en serio la seguridad.
- No se pueden usar las contraseñas de forma segura por medio únicamente de la memoria o notas. Se requiere un sistema de gestión con todas las características básicas de administración de contraseñas.

Artículos relacionados:

- **Enterprise password management: A field guide**
- **Password policy recommendations: Here's what you need to know.**
- **10 great security TED Talks**
- **How not to get ransomware**

Este artículo/contenido ha sido redactado a título individual y no refleja necesariamente el punto de vista de Hewlett Packard Enterprise Company.

Larry Seltzer es, desde hace años, un reputado experto en materia de tecnología, conocido por su trabajo de análisis del sector, así como de asesoría de seguridad y desarrollo de software. Hasta 2013 fue director editorial de BYTE, Dark Reading y Network Computing en UBM Tech. Antes de eso, dedicó más de una década a la consultoría y a escribir sobre tecnología, principalmente en el área de la seguridad. Es autor de tres libros y miles de artículos publicados, así como de muchos otros informes privados que no han sido publicados. Larry ha ejercido como director técnico en varios laboratorios de pruebas donde dirigió y realizó pruebas de productos, con un interés especial en la automatización de pruebas. Larry comenzó su carrera como ingeniero de software en la desaparecida Desktop Software Corp. de Princeton, Nueva Jersey, en el equipo que escribió el lenguaje de consulta 4GL PLN. También trabajó en departamentos de TI corporativos y en desarrollo de software en Chase Econometrics. Larry se graduó en la Universidad de Pensilvania con un título en Política Pública.

Accede a más información sobre soluciones para pymes de HPE

a00098971ese, abril de 2020

Hewlett Packard Enterprise