El popular proveedor de alojamiento web, Hostinger, resultó afectado por una violación masiva de datos, lo que dio como resultado que la compañía restablezca las contraseñas para todos sus clientes como medida de precaución.

En una publicación de blog este domingo, Hostinger reveló que *«un tercero no autorizado»* violó uno de sus servidores y obtuvo acceso a *«contraseñas hash y otros datos no financieros»* asociados con sus millones de clientes.

El incidente ocurrió el 23 de agosto, cuando hackers desconocidos encontraron un token de autorización en uno de los servidores de la compañía y lo utilizaron para obtener acceso a una API del sistema interno, sin requerir ningún nombre de usuario y contraseña.

Inmediatamente después del descubrimiento de la violación, Hostinger restringió el sistema vulnerable, haciendo que este acceso ya no esté disponible, y contactó a las autoridades respectivas.

> *«El 23 de agosto de 2019 hemos recibido alertas informativas de que un tercero no autorizado accedió a uno de nuestros servidores. Este servidor contenía un token de autorización, que se utilizó para obtener más acceso y escalar privilegios a nuestro sistema RESTful API Server*. Este API Server* se utiliza para consultar los detalles acerca de nuestros clientes y sus cuentas».*

La base de datos API aloja información personal de casi 14 millones de clientes de Hostinger, incluidos sus nombres de usuario, correos electrónicos, contraseñas hash, nombres y direcciones IP, a los que han accedido los hackers.

La violación afecta a más de la mitad de los usuarios de Hostinger

La compañía tiene más de 29 millones de usuarios, por lo que la violación de datos afectó a más de la mitad de su base de usuarios completa.

Sin embargo, se debe tener en cuenta que la compañía utilizó el algoritmo de hash SHA-1 débil para codificar las contraseñas del cliente Hostinger, lo que facilita a los piratas informáticos descifrar las contraseñas.

Como medida de precaución, la compañía restableció todas las contraseñas de inicio de sesión del Cliente Hostinger utilizando el algoritmo SHA-2 más fuerte y envió correos electrónicos de recuperación de contraseña a los consumidores afectados.

Además, la compañía actualmente no ofrece autenticación de dos factores para las cuentas de sus clientes, pero afirma que planea proporcionar esta capa adicional de seguridad en el futuro cercano.

Hostinger aseguró a sus clientes que no se cree que se haya accedido a ningún dato financiero, ya que la empresa nunca almacena ninguna tarjeta de pago u otros datos financieros confidenciales en sus servidores, y agregó que los proveedores de pagos externos manejan los pagos por sus servicios.

Por otro lado, la compañía asegura que una investigación interna exhaustiva encontró que las cuentas y los datos del cliente Hostinger almacenados en esas cuentas, incluidos sitios web, dominios y correos electrónicos alojados, permanecieron intactos y no se vieron afectados.

La investigación sobre el asunto sigue en curso, y se ha reunido un equipo de expertos forenses internos y externos y científicos de datos para descubrir el origen de la violación de datos y aumentar las medidas de seguridad de todas las operaciones de la compañía.

Después de restablecer la contraseña, la compañía también pide a sus clientes establecer una contraseña segura y única para sus cuentas de Hostinger, además de tener cuidado con los correos electrónicos sospechosos que les piden hacer clics en enlaces o descargar archivos adjuntos.

Los clientes que quieran eliminar sus datos de los servidores de Hostinger según las normas

GDPR, deberán comunicarse al correo gdpr@hostinger.com.