Un investigador de seguridad encontró en Internet una base de datos expuesta que pertenece al gigante de impresión en línea Vistaprint. El investigador Oliver Hough descubrió dicha base sin cifrar la semana pasada.

No existía contraseña en la base de datos, lo que permitía a cualquier persona acceder a los datos en su interior. La base de datos fue detectada por primera vez por el dispositivo expuesto y el motor de búsqueda de base de datos Shodan el 5 de noviembre, pero puede haber estado expuesta por más tiempo.

Hough tuiteó una advertencia a la compañía acerca del problema de seguridad, pero no ha recibido respuesta.

Vistaprint, propiedad de Cimpress, una compañía matriz con sede en los Países Bajos, desconectó de forma silenciosa la base de datos luego de que TechCrunch se comunicara con ellos, pero no realizó comentarios antes de la fecha límite.

Robert Crosland, portavoz de Vistaprint, dijo en un comunicado después de que se publicó la exposición, que resultaron afectados clientes en Estados Unidos, Reino Unido e Irlanda.

> *«Esto es inaceptable y no debería haber sucedido bajo ninguna circunstancia. Actualmente estamos llevando a cabo una investigación completa para comprender lo que sucedió y cómo prevenir cualquier recurrencia futura. En este momento, no sabemos si se ha accedido a estos datos más allá del investigador de seguridad que los encontró»*, dijo la compañía.

También mencionó que informará a los clientes de la exposición, muchos de los cuales están protegidos por las estrictas normas de protección de datos GDPR.

La base de datos contenía cinco tablas almacenadas con datos sobre más de 51 mil interacciones de servicio al cliente, como llamadas al servicio al cliente o chats con un agente de soporte en línea.

Los datos también incluían información de identificación personal, incluidos nombres e información de contacto, que podrían identificar a clientes individuales.

Una tabla llamada *«cases»* contenía consultas de clientes entrantes, incluyendo el nombre del cliente, dirección de correo electrónico, número de teléfono y la fecha y hora de su interacción con el servicio al cliente. Muchas de esas interacciones de servicio al cliente fueron tan recientes como a mediados de septiembre.

Los datos también contenían información oculta para el cliente. Cada interacción de servicio al cliente en la table de *«cases»* parecía haber calificado la consulta del cliente en función de las palabras clave elegidas de su consulta.

Esto ayudó a determinar el *«sentimiento»* del cliente, que luego describió su queja como negativa o neutral. Los datos también incluían la prioridad de la interacción de un cliente, lo que le permitía subir más alto en la fila.

Otra tabla llamada *«chat»* contenía las interacciones de chat en línea de miles de clientes con agentes de soporte, pero también contenía información sobre el navegador del cliente y la conexión de red, dónde estaban ubicados y qué sistema operativo usaban, y su Internet proveedor.

Algunos de los registros de chat grabados también contenían información confidencial, como números de pedido y números de seguimiento postal, pero no había contraseñas ni datos financieros en la base de datos expuesta.

La tabla de *«email»* contenía hilos enteros de correo electrónico con clientes que detallaban sus problemas u otros problemas con sus pedidos. La tabla de *«phone»* contenía información específica sobre cada llamada, incluida la fecha y la hora, cuánto tiempo estuvo en espera el cliente, una transcripción escrita de la llamada, que a menudo incluye detalles de los pedidos del cliente, y un enlace interno a la grabación de la llamada.

Los datos también contenían cierta información de la cuenta, incluidas las direcciones de

correo electrónico del trabajo y algunos números de teléfono pertenecientes al personal de servicio al cliente de Vistaprint.

Según Hough, la base de datos no estaba enviando o recibiendo datos en la actualidad. La base de datos se denominó «*migration*», lo que sugiere que la base se utilizó para almacenar datos temporalmente mientras se movían los registros de clientes de un servidor a otro.

Sin embargo, no está claro por qué la base de datos se expuso y se dejó en línea sin contraseña.