Microsoft confirmó esta semana que sin darse cuenta expuso información relacionada con miles de clientes después de un lapso de seguridad que dejó un punto final accesible públicamente por medio de Internet sin autenticación.

> *«Esta mala configuración resultó en el potencial de acceso no autenticado a algunos datos de transacciones comerciales correspondientes a interacciones entre Microsoft y clientes potenciales, como la planificación o posible implementación y provisión de servicios de Microsoft»,* dijo la compañía en una alerta.

Microsoft también enfatizó que la fuga B2B fue *«causada por una configuración incorrecta no intencional en un punto final que no está en uso en todo el ecosistema de Microsoft y no fue el resultado de una vulnerabilidad de seguridad».*

La configuración incorrecta de Azure Blob Storage fue detectada el 24 de septiembre de 2022 por la empresa de seguridad cibernética SOCRadar, que denominó la fuga BlueBleed. Microsoft dijo que está en proceso de notificar directamente a los clientes afectados.

Microsoft no reveló la magnitud de la fuga de datos, pero según SOCRadar, afecta a más de 65,000 entidades en 111 países. La exposición asciende a 2.4 terabytes de datos que consisten en facturas, pedidos de productos, documentos de clientes firmados, detalles del ecosistema de socios, entre otros.

«Los datos expuestos incluyen archivos con afecta de 2017 a agosto de 2022″, dijo SCORadar.

Sin embargo, Microsoft cuestionó el alcance del problema, afirmando que los datos incluían nombres, direcciones de correo electrónico, contenido de correo electrónico, nombre de la empresa y números de teléfono, además de archivos adjuntos relacionados con negocios *«entre un cliente y Microsoft o un socio autorizado de Microsoft».*

También afirmó en su divulgación que la compañía de inteligencia de amenazas *«exageró*

mucho» el alcance del problema ya que el conjunto de datos contiene *«información duplicada, con múltiples referencias a los mismos correos electrónicos, proyectos y usuarios».*

Además de eso, Redmond expresó su decepción por la decisión de SOCRadar de lanzar una herramienta de búsqueda pública que, según dijo, expone a los clientes a riesgos de seguridad innecesarios.

SOCRadar, en una publicación de seguimiento el jueves, comparó el motor de búsqueda BlueBleed con el servicio de notificación de violación de datos «*Have I Been Pwned*«, y lo describió como una forma para que las organizaciones busquen si sus datos estuvieron expuestos en una fuga de datos en la nube.

El proveedor de seguridad cibernética también dijo que suspendió temporalmente todas las consultas de BlueBleed en el módulo Threat Huntung, que ofrece a sus clientes a partir del 19 de octubre de 2022, luego de la solicitud de Microsoft.

> *«Microsoft no puede (léase: negarse) a decirles a los clientes qué datos se tomaron y aparentemente no notificar a los reguladores, un requisito legal, tiene el sello distintivo de una gran respuesta fallida»,* dijo el investigador de seguridad Kevin Beaumont«.

Beaumont dijo además que el cubo de Microsoft *«ha sido indexado públicamente durante meses»* por servicios como Grayhat Warfare y que *«incluso está en los motores de búsqueda»*.

No existe evidencia de que los atacantes accedieran indebidamente a la información antes de la divulgación, pero dichas filtraciones podrían explotarse con fines maliciosos, como extorsión, ataques de ingeniería social o una ganancia rápida.

> *«Si bien algunos de los datos a los que se puede haber accedido parecen triviales, si SOCRadar tiene razón en lo que se expuso, podría incluir información confidencial sobre la infraestructura y la configuración de la red de los clientes potenciales»,* dijo Erich Kron, defensor de la conciencia de seguridad en KnowBe4.

> *«Esta información podría ser valiosa para los atacantes potenciales que pueden estar buscando vulnerabilidades dentro de las redes de una de estas organizaciones».*