Si alguna vez has visto el mensaje *«Advertencia: hacer público su calendario hará que todos los eventos sean visibles para el mundo, incluso a través de la búsqueda de Google. ¿Está seguro?»*, deberías revisar tu configuración de Google para verificar que tu información no esté expuesta al público.

Hasta ahora, existen más de 8000 calendarios de Google de acceso público, que se pueden buscar utilizando el motor de búsqueda de la compañía, permitiendo a cualquier persona acceder no solo a los datos confidenciales guardados, sino también agregar nuevos eventos con información o enlaces creados maliciosamente, según informó el investigador Avinash Jain.

Avinash Jain es un investigador de seguridad de la India que trabaja en una empresa de comercio electrónico, Grofers, que anteriormente encontró vulnerabilidades en otras plataformas como la NASA, Google, Jira y Yahoo.

> *«Pude acceder a calendarios públicos de varias organizaciones que filtraban detalles confidenciales como sus identificadores de correo electrónico, su nombre de evento, detalles de evento, ubicación, enlaces de reunión, enlaces de zoom, enlaces de hangout de Google, enlaces de presentación interna y mucho más»,* dijo Avinash.

Debido a que el comportamiento previsto del Servicio de Calendario es una característica útil para colaborar con las personas al hacer público un calendario, no se puede culpar directamente a Google por los datos expuestos.

> *«Si bien esto es más una configuración prevista por los usuarios y el comportamiento previsto del servicio, pero el problema principal aquí es que cualquiera puede ver cualquier calendario público, agregar cualquier cosa en él, simplemente con una sola consulta de búsqueda sin compartir en enlace del calendario»,* agregó el investigador.

Además, el problema realmente no es nuevo, ya que se planteó por primera vez hace 12 años, cuando Google agregó esta función de *«hacer público»* a su servicio de calendario basado en la web como una forma genial para que los usuarios descubran eventos interesantes por medio de los motores de búsqueda, pero algunas búsquedas rápidas revelaron información corporativa confidencial que se hizo pública inadvertidamente por medio de Google Calendar.

De acuerdo con el investigador, ya que Google no notifica al creador de un calendario público cuando alguien accede a él o le agrega un evento, la función dificulta que los usuarios sepan si están exponiendo información involuntariamente o si están abiertos a spammers y phishers también.

Además, tampoco existe una indicación gráfica en la interfaz del calendario desde donde los usuarios puedan obtener una pista de que hicieron público el calendario y deberían dejar de agregar eventos personales.

Al utilizar la consulta de búsqueda avanzada de Google (Google Dork), se puede enumerar todos los calendarios disponibles públicamente en segundos y acceder a toda su información, incluyendo datos corporativos confidenciales que pertenecen a organizaciones.

> *«Varios calendarios pertenecían también a muchos de los 500 empleados principales de la compañía Alexa, que intencionalmente o sin intención, fueron hechos públicos por los propios empleados»,* dijo Avinash.

Hace unos meses, la firma de seguridad Kaspersky también descubrió que los estafadores abusaron del servicio de Google Calendar para atacar a los usuarios con ataques de robo de credenciales, donde los phishers enviaban a las víctimas un correo electrónico que contenía una invitación a eventos elaborada con enlaces maliciosos.

En caso de que un usuario quiera compartir un calendario con alguien en privado, Google también permite a los usuarios invitar a usuarios específicos agregando sus direcciones de

correo electrónico en la configuración del calendario, en lugar de hacerlos accesibles al público.