Sáenz & Ius Confidence

Abogados / Consultores

Seguridad en la red para video llamadas

A lo largo de esta última década, es cada vez más común, la proliferación de aplicaciones y plataformas de mensajería rápida, que ha terminado derivándose en la utilización de las mismas para realizar video llamadas debido sobre todo a su comodidad y rapidez, más aún acentuada debido a la situación que vivimos en estos momentos, tanto a nivel profesional como su uso particular.

Todas las compañías punteras dentro de las redes sociales tales como Facebook, Instagram o nuevas startups creadas, **deben garantizar al usuario** que la aplicación o plataforma **es inexpugnable**.

Objetivos como eliminar las brechas de seguridad, evitar la pérdida de datos, la cesión de datos sin consentimiento entre otros, evitar el acceso a datos de carácter personal no autorizados por el usuario, es el santo grial de las empresas, actualmente no hay ninguna mensajería rápida en este caso que estamos hablando las dedicadas a videollamadas que garantice el 100% de seguridad, con lo cual estamos a expensas de que se realice un seguimiento a las mismas y una rápida respuesta en caso de fallos de seguridad algo de lo que, por ejemplo, Facebook no puede presumir, pero como todo, a medida que van surgiendo los problemas se van encontrando soluciones, que puede que sea la segunda premisa que valoramos los usuarios en estas empresas, ya que muchas veces no es posible ser proactivo porque en muchos casos es imposible atender a todas las fisuras que pueden darse, pues ser reactivo y dar soluciones rápidas. Para lo cual las aplicaciones para empezar en sus políticas ya van avisando de los datos a los que acceden y a los que no, pues es obligatorio darlo a conocer.

En cuanto a las plataformas más utilizadas, en el ámbito empresarial, aparte de “Teams” de Windows, se están utilizando otras recientes como Zoom, relativamente nueva y Skype que es la pionera de las plataformas en realización de video llamadas, “Slack” o “Whereby” también consideradas unas plataformas seguras para uso empresarial, muchas de ellas, incluyen opciones para configurar la seguridad, prevenir accesos fraudulentos, bloquear reuniones una vez sus participantes ya estén en ella y así evitar el acceso de intrusos, la configuración de seguridad predeterminada, herramientas para identificar dispositivos de los participantes entre otros.

No obstante, se nos hace necesario puntualizar lo siguiente, los diversos organismos de seguridad nacional e internacional en los distintos países, y desde las propias empresa propietarias de dichas plataformas se incide en dos puntos fundamentales, en primer lugar, es imprescindible tener actualizadas las aplicaciones o plataformas ya que en ellas se recogen las soluciones a los distintos fallos que contengan las versiones anteriores, y tener activado un antivirus que nos proteja de estos ataques.

Por otro lado, aparte de plataformas cada vez surgen más aplicaciones que permiten video llamadas y que se utilizan principalmente en los dispositivos móviles y que pueden conllevar quizás más dudas sobre la seguridad, Party home, WhatsApp, jitsimeet, hangout, en cuanto a éstas, se debe extremar el uso y el contenido de las conversaciones que se mantienen en las mismas, muchas utilizan mensajes cifrados, algunas se caracterizan por ser seguras de extremo a extremo, donde hay un candado en la que solo emisor y receptor/es pueden acceder a su contenido.

Desde los organismos oficiales se aconseja que el contenido de temas tratados en estas conversaciones sea básico y se restrinja los datos de carácter personal, los accesos que se realicen a través de enlaces a url, códigos de invitación o de SMS, en estos casos también se aconsejan que las aplicaciones estén actualizadas sus versiones para garantizar que sean lo más seguras posibles.

Por último, exponemos una serie de **medidas de seguridad a tener en cuenta para preservar la seguridad durante las llamadas**:
– la aplicación debe tener cifrado de extremo a extremo, que garantice que solo emisor y receptor acceden a la comunicación y los datos estén encriptados.

– Configurar las medidas de seguridad en la aplicación, no vienen por defecto impuestas.

– Actualizar las versiones del dispositivo y la aplicación.

– Evitar las contraseñas fáciles con el fin de dificultar la posible suplantación.

– Activar un bloqueo de pantalla por inactividad.

Nuestras sugerencias:

– Leer atentamente las condiciones de la aplicación para saber a qué datos acceden y lo que estamos contratando en el momento del alta.

– Informar a los propietarios de la aplicación en caso de detectar alguna incidencia.

– Tener precaución con el tipo de datos compartidos, no compartir datos sensibles.

– Deshabilitar la función de micrófono y cámara cuando no se utilice la aplicación.

– Utilizar aplicaciones recomendadas por las autoridades.

Cierto es que la piratería ha crecido con la situación actual, tendremos que enfrentarnos a muchas amenazas ya que los hackers buscan sacar rédito de las situaciones, toda precaución es necesaria, así como estar informado de tendencias y herramientas con las que trabajamos para sacarles el mayor rendimiento y protegernos de las continuas amenazas.

Santiago Sáenz — Abogado Lawyer
Martín Rosa — Abogado - Economista

COMPLIANCE l AUDITORÍA | PRIVACIDAD DATOS PERSONALES | CORPORATE l | TAX & LEGAL SERVICES LITIGATION & ARBITRATION l DERECHO Tics | CONCURSAL l REAL ESTATE & INVESTMENTS

C / Suárez Guerra, 19
38003 S/C de TENERIFE
Fax 922 531 613
Tel.902 050 170

C/ Luis Doreste Silva 25
35004 Las Palmas de GRAN CANARIA
Fax 928 296 324
Tel. 902 050 170

Paseo de La Castellana, 216 Torres Kio
28046 MADRID
Fax 91 130 42 40
Tel. 902 050 170

Av./ Ernesto Sarti nº 10, Edif. Parque Royale, L-61, Torviscas ADEJE, 38660, TENERIFE, Tel 922716905 & 669720333

No imprimas si no es necesario. Protejamos el Medio Ambiente.