Source:
TicBeat

¿Cuántas aplicaciones o plugins diferentes ha instalado, configurado y utilizado para realizar todas estas actividades? ¿WebEx, Skype, Teams, Zoom, Jitsi, WhatsApp, Houseparty o Hangouts/Meet? ¿Cómo de seguro es tener estos productos instalados en su ordenador o móvil? ¿Y utilizarlos?

Quizá le suene esta situación, muy habitual en las últimas semanas: lleva todo el día trabajando. Desde casa, claro. Ha tenido que hablar con compañeros, con clientes, con proveedores. En algunos casos, ha bastado con una llamada telefónica; en otros ha necesitado una videollamada. Esta última permite congregar a diferentes personas casi como si se tratara de una reunión presencial.

En paralelo, sus hijos se han conectado a su cole o a su universidad. Y han tenido clases y tutorías con profesores por videoconferencia. Para terminar el día, se han conectado todos con los abuelos, con los primos o con amigos para verles las caras y saber cómo están.

Todas las aplicaciones tienen vulnerabilidades

En estos últimos días el tema está de actualidad porque han surgido multitud de noticias acerca de vulnerabilidades de seguridad descubiertas en uno de estos productos en concreto, Zoom. Estas noticias han creado tal alarma que algunos medios la han catalogado como un malware (un software malicioso) y muchas empresas e instituciones han prohibido su uso. ¿Está esta alarma justificada? ¿Son tan críticas las vulnerabilidades descubiertas? ¿Son las alternativas a este producto mucho más seguras?

Vamos a centrarnos en las vulnerabilidades de diseño, en las que se introducen cuando se desarrolla el software. Existe una base de datos que se denomina CVE (Common Vulnerabilities and Exposures) en la que se publican las vulnerabilidades que la comunidad de investigadores de seguridad va descubriendo en los diferentes productos de software.

Según esta lista, desde el año 2016, WebEx ha tenido 1 vulnerabilidad (crítica), Skype ha tenido 6 (1 de ellas, crítica), Zoom ha tenido 2 (ninguna crítica, faltan por publicar las descubiertas esta semana), WhatsApp ha tenido 8 (la mitad de criticidad moderada) y Jitsi, 1 (que no es crítica). Estas vulnerabilidades son las que los fabricantes resuelven mediante los parches y las actualizaciones de seguridad que todos tenemos que instalar en nuestros dispositivos de vez en cuando.

Estos agujeros de seguridad pueden afectarnos al ocasionar problemas como los siguientes:

Poner en riesgo la confidencialidad y la integridad de las comunicaciones que realizamos (chat, compartición de pantalla, voz, etc.). Por ejemplo, si no se utiliza cifrado o no se hace bien, un tercero malicioso podría

tener acceso a nuestras conversaciones o incluso modificarlas (eliminando o añadiendo elementos).

Dificultar o impedir la disponibilidad: puede darse una denegación de servicio, con lo que no podríamos acceder a la aplicación o a algunas de sus funcionalidades.

Provocar impactos para el control de acceso, de manera que no pudiéramos controlar quién accede a una sala o reunión privada (e incluso podría darse un secuestro de la llamada o el fenómeno que se ha llamado bombing).

Facilitar que un tercero suplante a un usuario dentro de una sala o reunión.

Suponer problemas con los permisos del micrófono o la cámara, por ejemplo, y permitir que alguien los controle por nosotros.

Pero las vulnerabilidades realmente críticas son las que permiten a un tercero tomar el control de nuestro equipo y ejecutar cualquier código en él sin nuestro permiso. Esas son las que nos deben preocupar. Y dejémoslo claro: de momento Zoom no parece tener ninguna de estas sin resolver.

Y la privacidad?
Otro aspecto muy importante es el ético. La mayor parte de estas aplicaciones de videollamada tienen, potencialmente, acceso a nuestras comunicaciones personales y profesionales, a datos personales de las personas que se conectan, a nuestro micrófono y cámara, a nuestros archivos, etc.

En privacidad nos preocupan aspectos como la minimización, la desvinculación o la transparencia y el control. Todos ellos se tratan con mucha ligereza en la mayor parte de los productos mencionados.

Si leemos con atención las condiciones de uso y las políticas de privacidad que aceptamos, nos llevaremos muchas veces las manos a la cabeza al descubrir que nuestras conversaciones pueden llegar a ser escuchadas, grabadas, compartidas con terceros. También nuestros contactos, por ejemplo. Y en principio, con nuestro consentimiento.

Muchas de las aplicaciones mencionadas, por ejemplo Zoom o Houseparty, han tenido tan mala prensa por sus políticas de privacidad que las han tenido que cambiar varias veces en las últimas semanas.

Conclusión: ¿debemos dejar de usar estas apps?
En seguridad y privacidad no suele ser buena idea demonizar a un producto o solución en concreto. Existen pocas verdades absolutas y muchos matices. En el caso de Zoom, han multiplicado por 20 el número de llamadas al día en una semana. Este aumento en el volumen de usuarios y el especial interés que ha suscitado todo lo que tenía que ver con esta herramienta han puesto de manifiesto muchos de sus problemas.

Pero no parece que la empresa esté reaccionado mal: ha sido transparente en su gestión, ha resuelto la mayor parte de las vulnerabilidades encontradas y ha bloqueado las nuevas funcionalidades durante 90 días para centrarse en mejorar todo lo posible lo que ya tienen. Por eso no parece necesario prohibir su uso en la mayor parte de los contextos en los que se utiliza.

Ahora bien, está claro que ni esta herramienta, ni la mayor parte de las que usamos en nuestro día a día, sería adecuada para compartir secretos militares (el nivel de seguridad no sería suficiente) o para utilizarla en contextos educativos donde los que se conectan son menores de edad (el nivel de privacidad tampoco sería el apropiado), por poner dos ejemplos fáciles de comprender.

En entornos empresariales donde la confidencialidad o la privacidad sean importantes, se suele contar con presupuestos que permiten desarrollar, desplegar o contratar alternativas que garantizan un cifrado robusto de extremo a extremo, la autenticación de las personas que se conectan, etc. Esto no significa que estas soluciones sean 100 % seguras; también tienen sus vulnerabilidades.

En cuanto a las instituciones educativas, como no suelen contar con tanto presupuesto, lo tienen más complicado. Casi todas están optando por usar las plataformas de Google o Microsoft mediante convenios específicos, pero no es la solución perfecta. Habrá que revisar muchos aspectos de estos convenios cuando pase esta situación excepcional porque está en juego la privacidad de menores de edad.

¿Qué podemos hacer entonces para protegernos?
El primer paso es pensar en el uso que vamos a dar a las videollamadas: ¿personal o profesional? ¿se van a compartir datos sensibles? ¿van a participar menores? La respuesta a estas preguntas nos puede ayudar a descartar algunas soluciones directamente y a buscar otras más adecuadas.

Además, no basta con instalar una solución (ya sea un software completo, un complemento o plugin, etc). Hay que invertir un tiempo en leer las condiciones de uso y la política de privacidad, hay que buscar alguna guía para saber cómo configurar lo que hemos instalado de manera segura y respetuosa con la privacidad, etc.

Tampoco basta con instalarla la primera vez y olvidarnos, hay que ir actualizándola según vayan surgiendo parches y nuevas versiones para no dejar un software con un agujero de seguridad en nuestro dispositivo. De hecho, cuando pase todo esto, ¿de verdad necesitamos seguir teniendo 20 de estas aplicaciones instaladas? A lo mejor alguna se puede desinstalar porque no la vamos a volver a utilizar.

En cuanto al uso doméstico con menores, si están bien configuradas y no se les deja solos, emplear algunas de estas apps tiene implicaciones similares a utilizar YouTube, cualquier red social, juegos online, etc. Se recopilan datos sobre ellos, pero prácticamente los mismos que todas las demás aplicaciones que usamos en el día a día. Conviene que los padres les acompañen y les conciencien sobre los riesgos que corren.

Por último, cuando tengamos que instalar cualquier nueva aplicación, debemos hacerlo siempre desde el sitio oficial, al que debemos haber llegado por nuestros propios medios. No vale pinchar en un enlace que nos han pasado por redes sociales o que hemos encontrado en una web. Porque el problema es que, en muchos casos, descargamos las aplicaciones de sitios maliciosos y vienen con sorpresa en forma de malware. Así que no tenemos un problema de seguridad por una vulnerabilidad de diseño, sino por una de ingeniería social

Disponible en:
https://www.ticbeat.com/tecnologias/son-seguras-las-aplicaciones-de-vide... [1]

Links
[1] https://www.ticbeat.com/tecnologias/son-seguras-las-aplicaciones-de-videollamada/