Comunicado 231
Ciudad de México, 9 de diciembre de 2020

# ENCUENTRA CIBERDELINCUENCIA NUEVO FLANCO DE ATAQUE EN VIDEOCONFERENCIAS: EXPERTO DEL IPN

- ***"Se han convertido en un objetivo más de estos grupos por la alta probabilidad de obtener algún beneficio": Eleazar Aguirre Anaya, especialista del IPN***
- ***"En el futuro convivirán el modelo de educación presencial y a distancia, por lo que el uso de las Tecnologías de la Información y la Comunicación serán de vital importancia": Esteban Moctezuma Barragán***
- ***Por la pandemia, la mayor parte de las instituciones, empresas u organizaciones utilizaron plataformas virtuales para dar continuidad a sus labores, pero no previeron fortalecer la ciberseguridad***

La ciberdelincuencia encontró un nuevo flanco de ataque para el robo de información mediante las plataformas para videoconferencias, cuya utilización se intensificó de manera exponencial en todo el mundo ante el confinamiento por la pandemia de COVID-19 y, por ello, es necesario que instituciones y empresas generen políticas y procedimientos de seguridad, a efecto de que sean más seguras y menos vulnerables, afirmó Eleazar Aguirre Anaya, especialista del Instituto Politécnico Nacional (IPN).

El Secretario de Educación Pública, Esteban Moctezuma Barragán, ha insistido en diversos foros que en el futuro convivirán el modelo de educación presencial y a distancia, por lo que el uso de las Tecnologías de la Información y la Comunicación dentro de los procesos educativos, será de vital importancia ante esta nueva realidad.

En este sentido, el Jefe del Laboratorio de Ciberseguridad del Centro de Investigación en Computación (CIC), Eleazar Aguirre Anaya, reconoció que en el pasado las videoconferencias tenían la atención de la ciberdelincuencia, pero no en la misma proporción de la que ha puesto a partir del incremento del universo de usuarios de estas plataformas. "Se han convertido en un objetivo más de estos grupos por la alta probabilidad de obtener algún beneficio".

Explicó que por la forma acelerada en la que se propagó el COVID-19 en todo el mundo, la mayor parte de las instituciones, empresas u organizaciones se vieron obligadas a utilizar plataformas de videoconferencias para dar continuidad a sus labores, pero no previeron conformar o fortalecer sus políticas de seguridad que permitieran blindar con procedimientos específicos el uso de estas aplicaciones.

Manifestó que hay diferentes errores de seguridad en el uso de algunas plataformas, uno de los más comunes y críticos es cuando se roban información de la nube, pero también es posible que hurten las bases de datos de los usuarios y que esa información sea vendida en el mercado negro de la ciberdelincuencia. "Los aspectos importantes a cuidar son los datos personales, ubicación geográfica, fotografías y los objetos que se observan mientras se realizan las videoconferencias".

Sostuvo que los responsables de que una videoconferencia no sea vulnerada son tres actores: Las empresas responsables de desarrollar software seguro, el equipo de seguridad de la empresa que define las políticas de seguridad y, por último, los usuarios de los productos, quienes deben obedecer las políticas y procedimientos de seguridad. En varias plataformas para videoconferencias, dijo, existe la posibilidad de que se pueda compartir información del escritorio de la computadora o dispositivo móvil que se utiliza. “Esto sucede cuando tenemos información relevante y algunas aplicaciones están abiertas durante la sesión”.

Finalmente, Aguirre Anaya expresó que para la selección de una plataforma se debe considerar que se garantice que las actualizaciones de seguridad, creadas por los desarrolladores de software, no tengan retrasos. “Se requiere personal capacitado para controlar las cuentas de los usuarios, contraseñas, políticas de seguridad y el tipo de acceso para administración remota de los equipos. Además, se debe exigir a los usuarios apegarse a las políticas de seguridad. La tecnología es muy útil, nos ayuda y facilita la vida, pero un uso no racional, nos lleva a cometer errores que pueden ser aprovechados por la ciberdelincuencia”.

**--o0o--**