CHARLAS Y TALLERES EN JUNIO

CHILE: CUATRO DÍAS DE CIBERSEGURIDAD POR *STREAMING*

Durante la primera quincena de junio, las 23 mayores comunidades de ciberseguridad de Chile se reunirán durante dos fines de semana a través de video *streaming*, siendo la primera cita virtual este sábado 6 de junio.

Llamado Convid, el encuentro será también una conferencia solidaria, ya que si bien ser espectador del evento es gratuito, se sugiere hacer una donación desde $3 mil a la Fundación Comida para Todos. El evento contempla charlas, conversatorios, talleres y desafíos de tipo Capture the Flag (CTF), que la organización señala "pueden servir de entrenamiento y selección de personal".

Sebastián Vargas, presidente de la Sociedad Chilena de Seguridad de la Información (Sochisi) y uno de los organizadores del encuentro, dice que "hace años veníamos dictando seminarios digitales y charlas de forma gratuita, pero la pandemia ha sido difícil para todos, y desde nuestra especialidad quisimos ir en ayuda de las personas que la están pasando mal y, a la vez, dar un poco de entretención y educación a los cientos de profesionales del área y entusiastas que están en cuarentena".

Se podrá acceder a las transmisiones en Convid.cl.

813

aplicaciones espía eliminó Google de su tienda virtual, las cuales son conocidas como *creepware*, término con que se denomina a los *software* que acceden a fotos o videos con fines maliciosos, como espionaje, acoso o suplantación de identidad. La medida fue tomada por el gigante tecnológico luego de recibir un informe elaborado por un grupo de académicos de la Universidad de Nueva York, Cornell Tech y la compañía NortonLifeLock.

GLOS@RIO

Exploit

Como lo dice su nombre en inglés, es un código que "explota" o "aprovecha" alguna falla o vulnerabilidad de un programa computacional, generalmente con fines maliciosos como ingresar sin autorización a un sistema, robar información, o tomar control del aparato como parte de una botnet. Como con el tiempo se suelen ir descubriendo estas vulnerabilidades y creando parches, es importante mantener el *software* actualizado.

DISCOS DUROS PUEDEN SER RECOGIDOS DE LA BASURA POR CIBERCRIMINALES:

Desde *apps* para borrar remoto a la destrucción física de memorias: cómo proteger los datos en equipos desechados

RAMÓN RIVERA NOTARIO

Con el mayor uso de aparatos electrónicos para realizar nuestra vida diaria, tanto en el ámbito personal como en el laboral, crece también la basura electrónica o *e-waste*, así como las iniciativas para reciclar y reutilizar esos equipos. Por eso es importante conocer las maneras de proteger nuestros datos o eliminarlos antes de botar o vender un celular o computador y evitar que lleguen a manos inescrupulosas.

Ya sea que los queramos desechar, vender, regalar o reciclar, todo tipo de implementos comunes a la vida de hoy como "computadores, *smartphones*, *tablets*, cámaras y grabadoras de audio, e incluso equipos más sencillos como alarmas o inesperados como automóviles, contienen información que podría caer en manos de terceros", explica Ignacio Rodríguez, director de la fundación Datos Protegidos.

Ernesto Rubio, especialista en Ciberseguridad de 3IT, advierte que "es importante saber que cuando vaciamos la papelera de reciclaje de nuestro computador, o restauramos de fábrica el *smartphone*, los archivos no se borran realmente". El peligro está en que en los computadores y memorias USB desechadas, por ejemplo, "se puede encontrar todo tipo de información muy sensible, como documentos, direcciones IP o credenciales corporativas", agrega Rubio, datos que "aunque sean difíciles de recuperar, no es imposible".

Esto también se extiende a los aparatos de uso doméstico, continúa el ejecutivo de 3IT: "Aunque la gente piense que la única información importante que hay en su teléfono u ordenador son las contraseñas, hay mucho más que eso. Alguien con acceso a cosas como el historial de navegación y las *cookies* del navegador de internet, los archivos temporales y documentos físicos con información personal de uno mismo o de otras personas, podría cometer una amplia variedad de ciberdelitos, como fraudes, *spoofing* y *phishing* dirigido".

Siempre hay que limpiar antes de reutilizar o desechar

¿Qué hacer para que los datos personales no queden a merced de futuros usuarios? "Los *smartphones* y *tablets*, tanto Android como iOS, poseen una funcionalidad incorporada que permite dejar los equipos 'como nuevos', e incluso a veces ofrecen un modo seguro que escribe ceros en la memoria para evitar que los contenidos pudieran ser extraídos con técnicas forenses", indica Rodríguez. Y añade que es sugerido también revisar cada aplicación (*app*) y cerrar sesión en ellas, y en el navegador web, cerrar sesión y eliminar el historial, el caché, las *cookies* y las claves almacenadas.

Por supuesto, antes de borrar hay que respaldar lo que se quiera conservar, complementa Juan Sanz, gerente de Servicios de Avantic: "El respaldo es el inicio de la cadena de protección contra la pérdida de información", asegura. Además, si se cuenta con un *smartphone* laboral, la idea es mantenerlo para temas de trabajo y así no perder información personal si es necesario devolver el aparato a la empresa, añade el especialista.

Para los celulares empresariales también existen los denominados Mobile Device Management —Administración de Dispositivos Móviles, o MDM—, aplicaciones que permiten borrar los datos y accesos a la red de la empresa cuando se reporta la pérdida de un teléfono inteligente, indica Sanz.

Asimismo, el experto recuerda que existen alternativas para el borrado de datos de manera remota en el caso de robo o pérdida del celular, como las aplicaciones "Buscar mi iPhone" para los dispositivos de Apple, y el "Buscar mi teléfono", en los de Android, las que lógicamente deben estar activas al momento de dejar de poseer el aparato.

La opción nuclear: destrucción física

Si se quiere más seguridad de que los datos no podrán ser leídos tras desprenderse del producto electrónico, "las dos principales recomendaciones son cifrar la unidad de almacenamiento y realizar un borrado seguro", dice Rubio, mencionando también la tercera alternativa, que es la destrucción completa del dispositivo, pero, claro, no es una opción si se quiere seguir usando el aparato. Si un disco duro está cifrado, explica, será más difícil que terceras personas puedan recuperar la información que contenía, haciendo más costosa y menos atractiva la operación.

Rubio explica que el borrado seguro supone "sellenar el espacio que ocupa un archivo que eliminamos con datos aleatorios falsos e inútiles", siendo la única forma de que el archivo sea borrado definitivamente, ya que hasta que se sobrescribe, un archivo eliminado aún puede ser recuperado. Para lograr el borrado seguro, el especialista de 3IT indica: "Siempre recomiendo utilizar las herramientas que trae el sistema operativo o las herramientas oficiales de la marca del sistema operativo para poder realizar el borrado seguro. Por ejemplo, SDelete de la suite SysInternals para Windows o la Utilidad de Discos para MacOs".

En el caso de que se busque la destrucción física de los discos duros, "debe aplicarse un procedimiento donde el oficial de seguridad de la información (CISO) asegure que los datos del disco duro sean eliminados física y lógicamente", señala César Pallavicini, miembro de la Asociación Chilena de Empresas de Tecnologías de Información (ACTI). Esto, porque "los discos duros manejan particiones y punteros, con los que un hacker puede reconstruir la información si no es eliminada con un aparato magnético específico, agrega.

LA TERCERA GRÁFICA: 3IT