Hola mis estimados lectores, como cada miércoles vengo hablarles sobre los desafíos presentes en el ciberespacio. En los últimos años, las empresas han adoptado la estrategia de fomentar varias formas de desarrollar el trabajo. El trabajo a distancia y el teletrabajo dejaron de ser una práctica pasajera, para establecerse en el mercado como una realidad necesaria. Esto fue incrementándose, a partir de la pandemia de la COVID-19, momento en que prácticamente se detuvo el mundo y nos trajo ese enemigo invisible, al cual todos llamaron Coronavirus, y que convirtió, el ser positivo en la noticia del día y la realidad de muchos.

Nuestro país atemperado a los tiempos que se avecinaban aprobó la Resolución 71/2021 del Ministerio de Trabajo y Seguridad Social, la cual estableció el Reglamento sobre el trabajo a distancia y el teletrabajo en Cuba. La norma jurídica entró en vigor a partir de su publicación en la Gaceta Oficial Extraordinaria No. 72, en ella se establece que los trabajadores que laboran con subordinación a un empleador y tienen suscrito un contrato de trabajo con una entidad, por tiempo indeterminado y por tiempo determinado, o para la ejecución de un trabajo u obra, así como aquellos cuya relación de trabajo se formaliza mediante designación o nombramiento pueden trabajar en cualquiera de estas dos modalidades. La resolución también establece que el empleador, de conjunto con el sindicato, define las áreas de trabajo y cargos en los que se puede utilizar el trabajo a distancia y el teletrabajo, siempre que la naturaleza de la actividad lo permita,

y se incluya en el Convenio Colectivo de Trabajo.

Quienes trabajan de esta forma y utilizan sus propios medios de cómputo, generalmente se encuentran más expuestos a ser víctimas de algunas de las amenazas informáticas de las que hemos conversado anteriormente. Acá en Código Seguro, hoy te ofrecemos un conjunto de recomendaciones qué puedes tener en cuenta para estar más protegido ante la ocurrencia de un determinado incidente.

1. Establecer una conexión segura

Los ataques dirigidos al protocolo de escritorio remoto (RDP) pueden llegar a tener consecuencias graves e indeseadas. Diferentes exploits de RDP han permitido a los atacantes acceder a información confidencial, realizar ataques de denegación de servicios a otras empresas, ejecutar código en máquinas vulnerables .y hasta cifrar todos los archivos para retenerlos y luego obtener dinero a cambio de un rescate (secuestro de datos).

El objetivo no es crear alarmas sin sentido, ya que existen numerosas formas de detectar y protegerse contra estos ataques, comenzando por apagar la conexión ante una determinada sospecha. Si realmente no es necesaria la utilización de este servicio, deshabilitarlo es realmente muy simple y el constituye el mejor consejo ofrecido. Y en caso de que se necesite permitir dicho acceso, hay una variedad de formas de restringirlo correctamente.

2. Actualizar sistema operativo, aplicaciones informáticas y el navegador

El trabajar de manera remota con una computadora personal provocará por lo general no tener el respaldo del departamento de Soporte Técnico o los Especialistas en Ciencias Informáticas, encargados entre otras tareas de instalar cada una de las actualizaciones en el equipo, así como de monitorear el funcionamiento de los programas de seguridad establecidos en los planes de seguridad informática existentes.

Ante este escenario, lo más recomendable es tener agendada en el Plan de Trabajo como una tarea semanal actualizar el sistema operativo, el software instalado y el navegador. Sobre todo, teniendo en cuenta que los navegadores web se han transformado en aplicaciones que se actualizan frecuentemente. Se sugiere además configurar en el caso de que sea posible las actualizaciones automáticas de estos sistemas de software y definir el momento específico en el día en que se requiere que se realicen.

3. Resguardar la información confidencial

Es un hecho que muchas personas han almacenado alguna vez información con determinada clasificación en sus equipos personales. Esto, aunque constituye una violación de lo estipulado, independientemente con el objetivo que se haga, siempre puede representar un gran riesgo, ya que esa información podría caer fácilmente en manos equivocadas.

Una muy buena alternativa es contar con un servicio de almacenamiento en la nube, en el cual poder migrar aquellos archivos de alta relevancia, a los cuales solo se pueda acceder mediante una conexión cifrada. La correcta configuración de la nube es otro factor clave.

Se recomienda además utilizar las técnicas de cifrado de unidades de disco, mediante la cual es posible proteger los datos almacenados en un disco duro o unidad de almacenamiento, en caso de pérdida o robo del dispositivo. Cuando se cifra un disco completo, se utiliza una clave de cifrado para convertir los datos en un formato ilegible. Para acceder a los datos cifrados, es necesario proporcionar la clave de cifrado correcta. Se recomienda para esto la herramienta VeraCrypt la cual es multiplataforma y de código abierto.

Tener en cuenta además que una recomendación importante a la hora de eliminar un archivo clasificado del disco duro local, es que siempre se debe sobrescribir primero el archivo: si solo se elimina, se estará liberando espacio reservado en memoria, pero los datos permanecerán y pudieran recuperarse con otras herramientas destinadas para estos fines.

4. Creciente riesgo inesperado en las videollamadas de trabajo

Los servicios de videollamadas se incrementaron exponencialmente también gracias a la pandemia: prácticamente la mayoría de las reuniones que eran presenciales hasta el momento se mudaron a un mundo virtual. Lo más serio del asunto es que hay empleados que piensan que no dejan rastro, sin embargo, recientes casos de filtraciones de datos en el ambiente laboral demuestran que hay que ser muy consciente del peligro que puede suponer esta conexión en un momento determinado. Por ello, sigue siendo clave tener en cuenta ciertas consideraciones referidas a la seguridad, para que no haya ningún tipo de sorpresas.

Por un lado, verificar las opciones de configuración y encontrar la que sea correcta a su entorno suelen ser muy convenientes y necesarias. Algunos ajustes, como las grabaciones de vídeo y audio, están activados por defecto, lo que puede poner en riesgo la privacidad de tus familiares. También es importante prestar especial atención a las comúnmente no leídas políticas de privacidad: en caso de ser gratuita, es muy probable que esté recopilando, vendiendo o compartiendo tus datos para financiar el servicio.

5. Reducir la dimensión de un posible ataque

En ocasiones resulta complicado dimensionar la cantidad de software que vamos a tener instalado en nuestros dispositivos. Pero, una muy buena práctica constituye la de dedicar algún tiempo extra para eliminar aquellas aplicaciones que ya no se vayan a utilizar. En primer lugar, puede liberar espacio de almacenamiento en el dispositivo, lo que puede mejorar el rendimiento y la velocidad del mismo. Además, eliminar aplicaciones que no se utilizan también puede mejorar la seguridad, ya que las aplicaciones que no se utilizan pueden representar una vulnerabilidad de seguridad si no se actualizan regularmente. Varios sistemas operativos tienen mecanismos para notificar a sus usuarios acerca de qué aplicaciones se utilizan y con qué frecuencia. De esta manera se estaría reduciendo la dimensión de un posible ataque y dando menos margen a los cibercriminales, que dedican gran cantidad de recursos y dinero para encontrar nuevos escenarios para su accionar.

6. Siempre estar alerta de la seguridad física del dispositivo y su interrelación con otros presentes en el entorno.

El trabajar desde casa puede conllevar riesgos invisibles, como las vulnerabilidades referidas a la Internet de las cosas (IoT). Sí hoy día, aunque esto pudiera parecer futurista, siempre se debe prestar especial atención a los dispositivos que se instalen en los hogares y más si tienen alguna interacción con el medio que se utilice para trabajar. Para evitar cualquier contratiempo innecesario es importante asegurarlos con contraseñas seguras, cambiando aquella que viene desde fábrica desde su primer uso, y actualizar el firmware y el software constantemente, siempre que las condiciones y la conectividad lo permitan.

En caso de que parte de la jornada laboral se desarrolle en lugares públicos, es fundamental cerrar la sesión para así evitar dar la oportunidad a que alguien acceda a la computadora por si la perdemos de vista (algo que no debería suceder nunca).

7. Punto clave: limpiar los registros de navegación

Es importante borrar el historial de navegación regularmente, por dos motivos: rendimiento del equipo y seguridad. El caché acumulado puede en ocasiones llegar a generar algún que otro dolor de cabeza. A su vez, es muy útil limpiar la carpeta de descargas, que suele acumular gran cantidad de archivos e información, muchos de los cuales pueden ser confidenciales y hasta peligrosos (como es el caso de los ejecutables que pueden ser posibles software malicioso). En este sentido la utilización de un buen software antivirus (pudiera ser el

de producción nacional Segurmática Antivirus) y mantenerlo actualizado constituyen una gran ayuda para la seguridad de nuestros dispositivos.

Por hoy es todo, nos volveremos a encontrar la próxima semana para seguir, acá en Código Seguro, hablando sobre el desafiante mundo de la Ciberseguridad.

Cubadebate.