INCIDENTES EN CIBERSEGURIDAD

NOTI 349 – Mayo de 2024

Recomendaciones:

- Realizar búsquedas informadas sobre el software que pretendemos instalar.
- Nunca descarguemos programas de páginas diferentes de las del propio desarrollador.
- Delegar a T.I. o quien haga sus veces, la descarga del software que se necesite.
- Antes que la instalación del software gratuito se inicie, revisar qué programas adicionales contiene.

Imagen de vecstock en Freepik

Como es sabido por la mayoría de las empresas y expertos en T.I., la seguridad cibernética se sustenta en tres pilares fundamentales: Herramientas, Procesos y Personas. Si alguno de ellos es vulnerable, se incrementa la probabilidad de ser víctima de accesos indeseados a los sistemas informáticos. Si los otros dos pilares son fuertes, podrán ayudar a disminuir el impacto o la gravedad del ataque.

Tampoco es desconocido que el eslabón más débil en todo nuestro sistema de protección es, justamente, el de las personas. De hecho, más del 70% de los ciberataques exitosos, se dan debido a fallas en este pilar. Veamos un caso típico.

En una Pyme, sector más afectado por los ciberataques, una persona a quien llamaremos Sandra Torres[1], trabajaba en la generación de contenido para su empresa, además de estar involucrada en temas de capacitación, razón por la cual, estaba autorizada para navegar con libertad en la Web y descargar los programas que considerara necesarios para el desarrollo efectivo de su labor; no sin antes, claro está, haber sido instruida sobre los riesgos existentes y las precauciones que debía tener. Ella siempre estaba pendiente de cualquier novedad, una vez hacía una descarga, independientemente de si se trataba de un programa o, un archivo; inclusive, analizaba si los sitios en los cuales podía encontrar lo que necesitaba lucían confiables. Por muchos años trabajó bajo esta forma sin que se presentaran novedades asociadas a sus actividades. Un día se le renovó su equipo de cómputo, pero no le fue instalado un programa con el cual había trabajado por varios años para hacer videos educativos, así

[1] Nombre cambiado, siguiendo lineamientos de Protección de Datos.

Imagen Propia

que tomó la decisión de descargarlo. Era un programa que ya conocía, con el que nunca había tenido inconvenientes, así que lo descargó y, en su exceso de confianza,
no leyó qué otros programas se descargarían e instalarían junto con el que deseaba. De esta forma, un malware logró ingresar al Sistema de su empresa

Al día siguiente de haber realizado la instalación, ella notó que había otro programa de antivirus, diferente al que había manejado habitualmente; por lo cual solicitó al área de Sistemas corregir dicha situación y realizar una revisión de todo su sistema. Efectivamente, encontraron virus, por lo que se procedió de inmediato a ejecutar los protocolos establecidos y se eliminaron los mismos. A las dos horas, un usuario del servidor notificó al área de Sistemas que no podía acceder al servidor; empezó un proceso de revisión y análisis, con el cual encontraron que algunas extensiones de archivos habían sido cambiadas, llegando a la conclusión que les había sido instalado un Ransomware. El equipo de Sistemas procedió a ejecutar los planes para contener la amenaza y, posteriormente, eliminarla con éxito. Durante el proceso, también pudieron identificar que Sandra mantenía abierta la VPN, facilitando la expansión del virus. A raíz de lo ocurrido, se eliminó la excepción que se tenía; y ahora, nadie puede descargar programas sin antes haber sido aprobados por T.I; así como se recordó a los usuarios de las VPN, de la importancia de mantenerlas cerradas cuando no se están utilizando. Para esta empresa, las cosas terminaron bien, debido a que tenían dos pilares fuertes y a que, si bien es cierto el factor humano falló, las capacitaciones le permitieron a Sandra identificar una situación inusual, facilitando su tratamiento temprano. Estamos seguros que ella no volverá a bajar la guardia.

Recomendaciones al momento de instalar software gratuito de internet.

A la hora de buscar herramientas que nos permitan incrementar nuestra productividad, como lo son software de capturas de pantalla, alternativas a Office, herramientas de notas, entre otros programas que podemos necesitar en nuestro día a día laboral, el mundo de Internet es al que acudiremos para buscarlas. Solo debemos ejecutar una búsqueda rápida en Google para encontrar dichas herramientas con la facilidad de un clic. Sin


Imagen de freepik

Por: Laura Castrillón y Santiago Duque
ASR S.A.S.

Medellín, Colombia
+573103923352 - 3233453366
asr@asr.com.co
http://www.asr.com.co/

embargo, esa facilidad viene asociada a unos riesgos inherentes que ya logramos describir en el caso que compartimos a lo largo de este Boletín; y es la posibilidad de que estos programas vengan contaminados con una gran cantidad de programas adicionales, que bien pueden ralentizar nuestros equipos; o, por el contrario, que se instalen virus.

Para minimizar la ocurrencia de estos resultados indeseados, proponemos las siguientes recomendaciones que nos ayudarán a protegernos de estas eventualidades:

- Siempre debemos realizar búsquedas informadas sobre el software que pretendemos instalar en nuestros equipos. Una investigación en diferentes sitios sobre el programa deseado, reseñas y calificación por parte de otros usuarios siempre será de utilidad.
- Nunca descarguemos programas de páginas diferentes de las del propio desarrollador. Es usual encontrar en diferentes sitios dichos programas, pero no podemos garantizar que el archivo que descarguemos sea el original del creador del software.
- Si en nuestra empresa tenemos un área de TI, que sea ésta la encargada de validar y certificar la idoneidad del software a instalar.
- Por regla general, una empresa no debe permitir a sus empleados descargar e instalar programas en los equipos de la empresa; por tanto, estos permisos deben ser exclusivos del área de TI o de quien cumpla dichas funciones.
- Cuando estemos instalando software gratuito, debemos estar atentos a instalaciones de programas adicionales que éstos puedan contener, como antivirus, juegos, programas de optimización de memoria, limpiezas de caché y demás extras que comúnmente se pueden encontrar en este tipo de programas.

Como hemos visto, los riesgos asociados a eventos tecnológicos por un inadecuado manejo en la instalación de un programa informático, nos puede generar muchos dolores de cabeza. Sin embargo, si aplicamos unas sencillas recomendaciones, podremos

minimizar la exposición a virus en nuestros computadores y, por ende, reducir la posibilidad comprometer la seguridad de nuestra información.

asr@asr.com.co