20211110, Nota Informativa, ciberseguridad sobre aplicaciones.

En virtud de mis compromisos contractuales, seguidamente os traslado una serie de principios y recomendaciones sobre el uso de aplicaciones.

El **CCN-CERT (Centro Criptológico Nacional)** en el documento titulado “principios y recomendaciones sobre ciberseguridad”, dedica un apartado a la aplicaciones que considero puede ser de mucho interés. A ello pues.

La instalación de programas puede afectar al rendimiento y la seguridad de los dispositivos/equipos. Debe mantenerse la integridad de los mismos y siempre hay que instalar software autorizado y proporcionado directamente por el fabricante.

- El empleo de software legal ofrece garantía y soporte, con independencia de las implicaciones legales de utilizar software no legítimo.
- Certificación del programa para su compatibilidad con el sistema operativo y las demás aplicaciones.
- Instalación y mantenimiento de parches y actualizaciones de seguridad, con especial atención a aquellas de carácter crítico (en los últimos meses la no actualización de los programas ha provocado numerosas brechas de seguridad).
- Considerar la superficie de exposición asociada a los sistemas heredados (legacy), especialmente aquellos que tienen más de una década de antigüedad por su extremada vulnerabilidad.

Los usuarios deben ser conscientes de que la introducción de software no autorizado puede causar la infección del sistema más protegido. Como buenas prácticas se indica lo siguiente:

- Trabajar habitualmente en el sistema como usuario sin privilegios, no como “Administrador”.
- No ejecutar nunca programas de origen dudoso o desconocido.
- Si se emplea un paquete de software ofimático capaz de ejecutar macros, hay que asegurarse de que esté desactivada su ejecución automática.

En cuanto a la impresión de documentos, hay que ser conscientes de que los documentos y transacciones impresas son susceptibles de violaciones de la seguridad. Por lo tanto, resulta fundamental emplear buenas prácticas para cumplir la normativa existente en cada entidad y que la información impresa sea segura y no accesible por personal no autorizado.

1. CIFRADO DE DATOS

Cifrar los datos significa convertir texto plano en texto ilegible, denominado texto cifrado, evitando que la información sea accesible por terceros no autorizados. Para lo cual, se necesita de un algoritmo de cifrado y la existencia de una clave, que permite realizar el proceso de transformación de los datos y que debe mantenerse en secreto.

Existen múltiples soluciones comerciales4 para cifrar los equipos informáticos, clasificables en tres (3) tipos atendiendo al nivel en el que actúan en el sistema de archivos:

- Cifrado de disco

Es una tecnología que cifra el disco por completo, de esta manera el sistema operativo se encarga de descifrar la información cuando el usuario la solicita.

- Cifrado de carpetas

El cifrado se realiza a nivel de carpeta. El sistema de cifrado se encargará de cifrar y descifrar la información cuando se utiliza la carpeta protegida.

- Cifrado de documentos

El sistema se encarga de mostrar y permitir el acceso al documento solo para los usuarios autorizados, haciendo ilegible el contenido a los no autorizados.

2. CORTAFUEGOS PERSONALES

Los cortafuegos personales o firewalls son programas que monitorizan las conexiones entrantes y salientes del equipo. Están diseñados para bloquear el acceso no autorizado al mismo, pero permitiendo al mismo tiempo las comunicaciones autorizadas. Lo más complicado de un cortafuegos es configurarlo correctamente, de modo que no se bloqueen las conexiones legítimas (navegación web, actualizaciones, correo electrónico, etc.).

Como criterio genérico, no se deben permitir las conexiones de fuentes desconocidas. Por tanto, deben bloquear todas las conexiones entrantes y sólo permitir aquellas que se indiquen expresamente sobre la base de un conjunto de normas y criterios establecidos. Un cortafuegos correctamente configurado añade una protección necesaria que dificulta los movimientos laterales no autorizados por la red, pero que en ningún caso debe considerarse como suficiente.

3. APLICACIONES ANTIMALWARE

Entre las acciones que puede provocar un código malicioso o malware se encuentran: borrado o alteración de archivos, consumo de recursos del equipo, acceso no autorizado a archivos, infección remota de los equipos, etc.

Las funciones mínimas que se pueden esperar en una buena herramienta antimalware6 (más conocidas por antivirus) son las de filtrado entrante y saliente de contenidos maliciosos, protección en el correo electrónico, en la navegación y en las conexiones de todo tipo en redes profesionales o domésticas. También deben ser capaces de analizar los ficheros en dispositivos removibles como discos externos o memorias USB y permitir programar análisis exhaustivos cada cierto tiempo.

Las aplicaciones antimalware deben disponer de actualizaciones regulares (últimas definiciones y motores de búsqueda) y ser productos de casas comerciales de confianza que permitan una combinación de los siguientes métodos:

- Escáner de acceso: permite examinar los archivos cuando son abiertos.
- Escáner a demanda: análisis en base a un calendario establecido.
- Escáner de correos electrónicos: en dispositivos de protección de perímetro o servidores de correo.
- Control de firmas: permite detectar cambios no legítimos en el contenido de un archivo.
- Métodos heurísticos: búsqueda de anomalías en los archivos y procesos en base a experiencias previas de comportamiento del malware.

Pero, una aplicación antimalware sola no es suficiente; hay que proporcionar un enfoque centralizado (cliente-servidor) para proteger todos los puntos finales (servidores, sobremesas, portátiles, teléfonos inteligentes, etc.) conectados a la red. Algunos proveedores ofrecen sistemas de Endpoint Security que incluyen antivirus, cortafuegos y otro software de seguridad.

4. BORRADO SEGURO DE DATOS

Se puede pensar que un simple formateo del disco duro impedirá que los datos almacenados en el mismo puedan ser recuperados. Sin embargo, hay aplicaciones que permiten deshacer el formateo de una unidad existiendo incluso métodos para recuperar los datos de los discos, aunque estos hayan sido sobrescritos.

Si se quiere garantizar que no se está distribuyendo información sensible, se deben sobrescribir los datos siguiendo un método (patrón de borrado) que no permita su recuperación de modo alguno.

Para tal fin, es necesario realizar diversas pasadas de escritura sobre cada uno de los sectores donde se almacena la información. Para simplificar la tarea, lo más sencillo es utilizar alguna aplicación especializada que permita eliminar la información de forma sencilla.

En el caso de fotografías digitales, archivos de audio o vídeo y documentos ofimáticos existen metadatos que pueden almacenar información oculta y no visible usando la configuración estándar de las aplicaciones, necesitando de una configuración específica o incluso un software concreto para revelar esos datos.

Estos metadatos son útiles ya que facilitan la búsqueda de información, posibilitan la interoperabilidad entre organizaciones, proveen la identificación digital y dan soporte a la gestión del ciclo de vida de los documentos.

Sin embargo, el borrado de metadatos o datos ocultos mediante procedimientos y herramientas de revisión y limpieza de documentos/archivos es fundamental para minimizar el riesgo de que se revele información sensible en el almacenamiento e intercambio de información.

En todo caso, y como siempre, quedo a vuestra disposición para aclarar cualquier duda sobre la cuestión comentada.

Hecho conforme a mi leal saber y entender, en Manilva a 10 de noviembre de 2021,

ZOTANO SANCHEZ SALVADOR - 32028277H

Firmado digitalmente por ZOTANO SANCHEZ SALVADOR - 32028277H
Fecha: 2021.11.10 08:41:45 +01'00'

Salvador Zotano Sánchez

(Delegado de Protección de Datos Certificado 19-ADK0101 conforme al Esquema AEPD-DPD)