20200408, Nota Informativa, sobre las cinco medidas técnicas básicas que se deben tener en cuenta para evitar brechas de seguridad.

En virtud de mis compromisos contractuales, seguidamente paso a informar de una publicación realizada esta misma semana por la AEPD al objeto de prevenir las brechas de seguridad. En concreto, se proponen cinco medidas técnicas.

Dado que la privacidad se puede ver afectada por incidentes de confidencialidad, integridad y disponibilidad debemos usar una combinación de medidas de seguridad básicas para hacer frente a estos desafíos.

El RGPD establece en su artículo 32 la obligación de notificar a la autoridad de control cualquier violación de seguridad de datos personales en las primeras 72 horas desde que se ha producido; por eso es muy importante que, en cuanto se produzca una violación de seguridad de datos personales, lo ponga en mi conocimiento.

Desde que se estableció la obligación de notificar las brechas de seguridad que afectan a datos personales, la AEPD, a través de su Sede Electrónica ha registrado ya más de 2.400 brechas de seguridad, más de 400 en los últimos tres meses, lo que representa un 48 % más que en el mismo periodo del año pasado. En las estadísticas que se publican periódicamente pueden verse las tipologías más comunes y sus víctimas. La mayoría de los incidentes de seguridad no corresponden a ciberataques sofisticados y en muchos casos se podrían haber evitado o minimizado sus consecuencias llevando a cabo un razonable análisis de riesgos y aplicando unas medidas de seguridad básicas como las que se describen a continuación, y que son válidas para cualquier tipo de organización independientemente de su tamaño o ámbito.

Se proponen las siguientes cinco medidas técnicas:

Primera. Uso de contraseñas seguras y segundo factor de autenticación.

Se debe establecer una buena política de contraseñas para el acceso a los sistemas. Esta política puede empezar por no almacenar las contraseñas en los sistemas sin cifrar, obligar a actualizarlas de forma periódica y no reutilizarlas para distintos servicios.

A la vista de los incidentes de robos masivos de contraseñas, contar con un segundo factor de autenticación se hace necesario para los sistemas más críticos, y recomendable para el resto. El uso de un segundo factor implica que aparte de facilitar el usuario y contraseña sea preciso una prueba adicional para realizar la identificación, como pueda ser un elemento biométrico, un código pseudoaleatorio, o el envío de un código de un solo uso establecido para cada usuario.

Segunda. Copias de seguridad.

Actualmente, las amenazas de tipo *ransonware* o secuestro de la información están más extendidos y son más dañinos, causando la indisponibilidad temporal o permanente de datos y servicios.

En este caso, las herramientas de copias de seguridad son fundamentales para recuperarse del incidente (artículo 32.c delo RGPD). Se debe establecer de forma minuciosa una política de cómo se realizarán las copias de seguridad, en la organización.

Tercera. Sistemas actualizados.

Una de las medidas más efectivas es contar con los sistemas actualizados en todo momento, puesto que los fabricantes están continuamente aplicando parches y mejoras de seguridad según se detectan los problemas. Esta actualización no sólo se refiere al sistema

operativo de nuestros equipos de trabajo y servidores, sino también a los programas que utilizamos en nuestros dispositivos, y que deben ser la última versión disponible por el fabricante. Se debe establecer una rutina de actualizaciones periódicas documentada y trazable.

No hay que olvidar que, por ejemplo, para el famosos ataque *WannaCry*, que afectó a millones de equipos en todo el mundo, existía una actualización de seguridad por parte de *Microsoft* desde tres meses antes de que tuviera lugar el ataque.

Cuarta. Exposición de servicios en internet.

En ocasiones, para llevar a cabo una tarea de mantenimiento, realizar pruebas o permitir un acceso puntual se aplican configuraciones en los sistemas que pueden llegar a comprometer la seguridad. Muchas veces, estas 'soluciones de un día' no se vigilan y terminan convirtiéndose en definitivas, dejando un posible agujero de seguridad abierto. Por ejemplo, acciones como permitir un acceso libre desde Internet a una base de datos o acceder al escritorio remoto de un servidor se dan muy a menudo.

Es importante que las organizaciones definan una estricta política de servicios expuestos en Internet. Asimismo, los accesos remotos siempre deben realizarse a través de sistemas de VPN, proxy inverso o medidas igualmente eficaces.

Quinta. Cifrados de dispositivos.

Una medida básica para asegurar la confidencialidad de la información consiste obligar a que al menos los dispositivos portátiles que se puedan extraviar fácilmente o ser objeto de robo estén cifrados. Esta recomendación aplica no sólo a los ordenadores portátiles, sino también a teléfonos móviles, tabletas, memorias USB, discos duros externos y copias de seguridad que se depositan en otros lugares. Una

contraseña de acceso al sistema no asegura la confidencialidad del contenido en caso de robo o extravío, por lo que es necesario complementar con el cifrado. Esta medida es una de las que menciona el RGPD en su artículo 32.

Otra aproximación al RGPD es aplicar la minimización de datos en los dispositivos. Esto implica tener la menor cantidad de datos personales y el menor tiempo posible en un dispositivo, y solamente cuando se vayan a tratar.

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

Hecho conforme a mi leal saber y entender, en Manilva a 8 de abril de 2020,

ZOTANO SANCHEZ SALVADOR - 32028277H

Firmado digitalmente por ZOTANO SANCHEZ SALVADOR - 32028277H
Fecha: 2020.04.08 08:18:50 +02'00'

Salvador Zotano Sánchez

(Delegado de Protección de Datos Conforme al Esquema de Certificación AEPD-DPD v. 1.4 nº 19-ADK0101).