# Filtración de Datos

13 de agosto de 2020

Por Walter Urrea León
Walter.Urrea@Tecmanario.com

Alguien menciono que los datos son el oro negro del siglo XXI y hay que tratarlos con la precaución que le corresponde.

Otra cita que se haría celebre fue la mencionada en la película Wall Street de 1987, donde un corredor de bolsa llamado Gordon Gekko interpretado por Michael Douglas menciono: "La commodity más valiosa es la información". Lejos de la realidad no estaban.

Suele ocurrir que algunas empresas que tienen acceso a gran cantidad de información sobre los usuarios vendan los datos a terceros para distintos propósitos como realizar estudios de mercado, publicidad; Google y Faceboook son algunos ejemplos. Sin embargo ante la centralización de estos grandes volúmenes de información, se presentan filtraciones descontroladas que originan perjuicios a los usuarios y a todos los niveles, empezando por la propia seguridad de los individuos.

Recordemos algunas de las filtraciones de datos acaecidas en el último tiempo y que fueron muy repercutidas a nivel internacional:

VeriSign sufrió un ataque informático en el 2010. No se publicaron datos sobre los daños causados al acceder a sus sistemas, pero expertos en seguridad coinciden en que lo peor fue no haberle comunicado lo ocurrido a la opinión pública.

En 2011 RSA Security fue hackeada. 40 millones de registros de empleados fueron comprometidos. Un email infectado fue el anzuelo para comprometer la seguridad de la compañía.

Sony's PlayStation Network en abril de 2011 fue hackeada y unos 77 millones de cuentas se vieron comprometidas. Las pérdidas estuvieron

cerca de los 171 millones de dólares. Los hackers lograron acceder a nombres, contraseñas, correos electrónicos, direcciones y tarjetas de crédito.

En 2013 Adobe sufrió una filtración para robar los datos personales de 38 millones de usuarios. Adobe tuvo que pagar 1,1 millones de dólares en tasas legales y un millón a los usuarios.

Yahoo fue otra víctima, se comprometieron los datos de los 3.000 millones de usuarios. La empresa recibió muchas críticas por haber tardado demasiado en anunciar la filtración y su precio de mercado se redujo en 350 millones de dólares.

Finalmente, Facebook en 2018. Cuando más de 50 millones de usuarios se vieron afectados por una filtración de datos. Los ciberdelincuentes explotaron una vulnerabilidad en la función "Ver como" para robar tokens de acceso, que son unas claves que permiten iniciar la sesión de Facebook de manera automática sin digitar la clave.

Cómo podemos observar las filtraciones tienen lugar a cualquier nivel y escala. Sin importar lo sofisticados que puedan ser los controles. Un usuario desprevenido, no consciente o mal informado es suficiente para echar abajo cualquier sistema.

La concientización de los colaboradores así como la preparación y la conformación de grupos interdisciplinarios se esta volviendo un requisito en las organizaciones para hacer frente al nuevo panorama de amenazas y la complejidad digital de hoy en día. Es por ello que los equipos de seguridad deben ser tan diversos como los problemas que están enfrentando.

Las dimensiones de seguridad deben abarcar desde el software en los puntos de conexión hasta los servicios en la nube. Muchos creen que tener contratado un servicio o servidor alojado en un proveedor Cloud ya soluciona todos sus males. Nada más lejos de la realidad.

La mejor forma de prepararse para una violación a la seguridad es prevenirla.  Se deben tener protocolos sobre cómo identificar los riesgos de la ciberseguridad en los sistemas, las funcionalidades, los activos y los datos. Y en caso de detectarse una violación de seguridad, se deben adoptar acciones adecuadas tendientes a minimizar el impacto y los daños.