Fuente:
ABC

Gobiernos, tarjetas de crédito, datos médicos y aparatos propios de la llamada «Internet de las Cosas» serán los principales focos de actuación por los ciberdelincuentes a lo largo del presente año. Las organizaciones han visto la necesidad de utilizar la inteligencia para gestionar sus riesgos informáticos, con el fin de proteger sus activos de los ciberataques, predecir y prevenir cualquier incidente y defender sus sistemas y datos críticos. La rápida evolución de la tecnología y **la creciente sofisticación de los atacantes** son un reto continuo para las bases sobre las cuales hoy en día se construyen los programas de ciberseguridad.

Según las previsiones de la firma española Vector ITC Group [1], las ciberamenazas más importantes que se darán en los próximos meses irán hacia el robo de credenciales para operar operaciones financieras y los ataques dirigidos a instituciones públicas volverá a ser, al igual que en 2014, otro de los riesgos.

Buscar nuevos métodos de contraseñas

Mientras diversas marcas exploran nuevas funciones y sistemas más seguros que las contraseñas tradicionales, **tales como sensores biométricos**, habrá varios sectores afectados por los ciberataques. En ese sentido, ya se aprecian ciertos movimientos en las empresas de cara a fortalecer sus accesos informáticos. Por ejemplo, MasterCard ha anunciado recientemente sus planes para poner fin al uso de las contraseñas en los pagos online a través de un nuevo estándar desarrollado junto con Visa. «Lo esencial de estos datos es que compañías tan importantes están viendo las contraseñas como algo vulnerable y obsoleto», afirma **Francisco José Mateo Ballesteros**, Consultor de Seguridad Informática de Vector.

El reto de seguridad -adelantan los expertos- al que se enfrentan las firmas tecnológicas es que la utilización de datos biométricos está en que los datos biométricos no se pueden cambiar. «Esto implica que si nos roban nuestra huella dactilar nos robarán esa "contraseña" para siempre hasta el fin de nuestros días».

Otro de los sectores que más interés cobrará será el de la salud, objetivo cada vez mayor para los criminales. «Probablemente, 2015 sea el año en el que veamos ataques dirigidos a compañías de salud y compañías y **aplicaciones que registran datos de salud médicos de los propietarios**», aseguran los expertos.

Y es que los historiales médicos contienen una gran cantidad de información personal que puede ser utilizada en una multitud de ataques y varios tipos de fraude. «En un entorno en el que millones de registros de pacientes se están pasando aún del papel a formato digital, muchas organizaciones **están tratando todavía de ponerse al día en relación a la seguridad y la protección de datos personales**. Por este motivo, esperamos un mayor número de ciberataques contra esta industria», explica **Bruce Goslin**, director ejecutivo de la firma de investigación K2 Intelligence [2].

Esfuerzo en ampliar técnicas de Big Data

También, en materia de análisis de grandes datos (Big Data), los ciberdelincuentes han desarrollado nuevas capacidades para intentar robar material sensible. Así, se espera que las empresas tiendan a utilizar el análisis cognitivo y el procesamiento del lenguaje natural para responder a las preguntas de negocio, cambiar a través de cantidades masivas de datos en diferentes fuentes y responder con un alto nivel de precisión.

Es una prioridad para las empresas mantener esos datos a salvo», concretan. Según estudios realizados por las principales empresas y analistas de seguridad, este 2015 se vivirá una escalada de ataques en esta «guerra informática»que ya mueve más dinero que el narcotráfico [3].

Ataques patrocinados

De hecho, se registrará un aumento de ataques patrocinados por estados junto con un aumento en la guerra digital y el ciberespionaje. «Como resultado, **otros países querrán desarrollar sus propios programas de ciberespionaje**, particularmente en países con altas previsiones de crecimiento económico», según este experto.

«Vamos a ver un aumento en células vagamente afiliadas que llevan a cabo iniciativas de ciberterrorismo o ciberguerra **independientes pero con el apoyo de causas de los gobiernos**. Además, un ciberataque en instalaciones industriales puede causar estragos en un país y originar daños extremos. Por ejemplo, la interrupción del servicio eléctrico; esto no sólo afecta a la vida cotidiana, sino que también ocasiona una gran cantidad de pérdidas económicas a muchos niveles», vaticina.

Ataques a la nube

Otra de las previsiones que manejan los expertos es un aumento de las violaciones de seguridad en cuanto a nombres de usuario y contraseñas almacenadas en la nube, ya que cada vez **más datos de las organizaciones se están llevando a los servidores externos**. «Los nombres de usuario y contraseñas de cuentas con privilegios y de administrador son, básicamente, las llaves del castillo como se pudo probar en los grandes ataques a bases de datos como el que sufrió la cadena de supermercados Target, con alto valor en el mercado negro. Además, los dispositivos móviles serán cada vez más objeto de ataques de robo de credenciales o autenticación que se utilizarán en una fecha posterior. Estos ataques usarán el teléfono como un punto de entrada a las aplicaciones y datos empresariales basados en la nube a los que los dispositivos acceden libremente», agrega Goslin.

Disponible en:

http://www.abc.es/tecnologia/informatica-software/20150108/abci-tendencias-tecnologicas-201501081845.html [4]

Links

[1] http://www.vector-itcgroup.com/
[2] http://www.k2intelligence.com/es/
[3] http://www.abc.es/espana/20141207/abci-ciberdelincuencia-dinero-201412062106.html
[4] http://www.abc.es/tecnologia/informatica-software/20150108/abci-tendencias-tecnologicas-201501081845.html