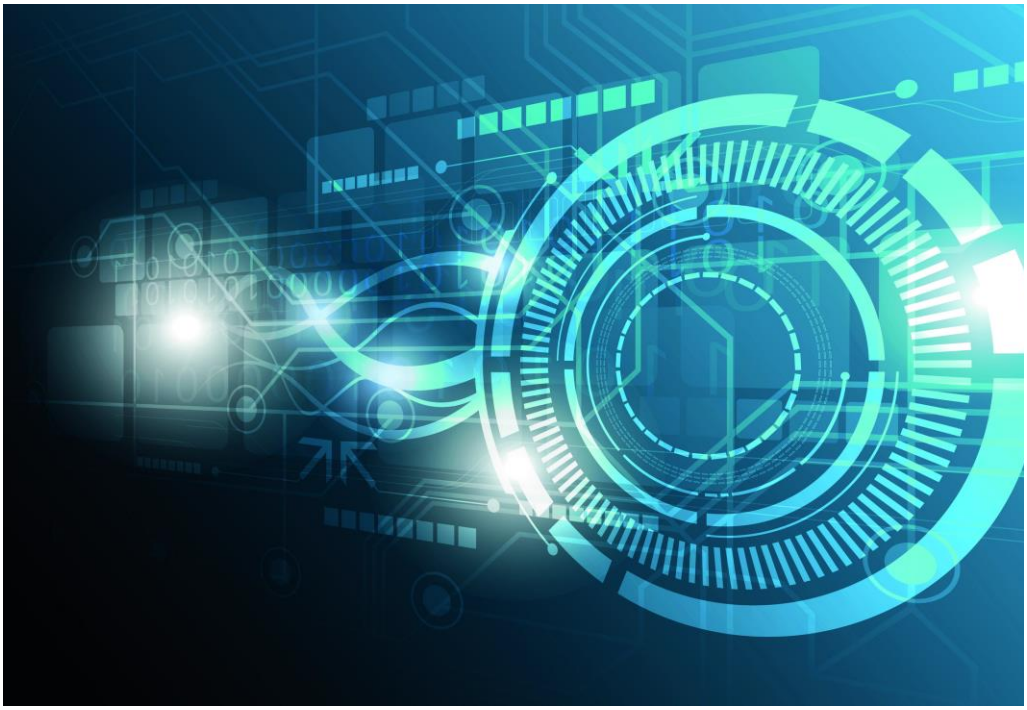

NEWSLETTER – INFOSEC MX

BOLETIN No. 17

JUNIO 11 - 19

Elaboración: Junio 20, 2016

MUNDO

En este número encontrarás noticias sobre:

- Mundo
- Gobierno
- Empresas
- Tecnología

Garantizada la Seguridad cibernética de los Juegos Olímpicos de Río 2016

por JUNIO 08 2016 / TICBEAT

Terminaron las pruebas y evaluaciones de los componentes de TIC relacionados con sistemas de comunicaciones, medios informativos, deportes y seguridad tecnológica de los Juegos Olímpicos de Rio 2016, estos probablemente sean los próximos 9, 10 y 12 de agosto. Fueron más de 200 mil horas de actividad de TI realizadas por Atos con la ayuda del comité organizador de los juegos y otros asociados tecnológicos. Donde también se puso a prueba sistemas como los portales de acreditación de personal voluntario, que por primera vez en unos Juegos Olímpicos se gestionan en la nube.

Durante el ensayo técnico final, el equipo técnico afrontó casi 1.000 escenarios como inundaciones, desconexión de redes, cortes de suministro eléctrico, cambios de programación de competencias y ataques contra la Seguridad en las 22 sedes olímpicas.

Fuente: **http://www.ticbeat.com/seguridad/garantizada-la-seguridad-cibernetica-de-los-juegos-olimpicos-de-rio-2016/?utm_content=buffer09143&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**

GOBIERNO

Falsos sitios electrónicos envían correos de SAT y Afores para robar datos

por JUNIO 13, 2016 / LA JORNADA

El Servicio de Administración Tributaria (SAT), reportó 228 correos electrónicos donde se envía material falso para supuestamente citar al destinatario para que aclare su estado tributario, siendo este un fraude para instalar malware en las computadoras y obtener información personal, alertó el Consejo Ciudadano de la Ciudad de México, señalando además que en las últimas dos semanas recibió 120 denuncias por estos correos.

Con esta manera de operar se han detectado correos supuestamente recibidos de administradoras de fondos para el retiro (Afores). Una forma de detectar el fraude es ver la dirección del remitente del mensaje, este no es oficial.

Fuente:
http://www.jornada.unam.mx/2016/06/13/capital/034n2cap

La plataforma web del SAT es vulnerable a ataques: experto

por JUNIO 13, 2016 / CRONICA

En el 2005, el Servicio de Administración Tributaria (SAT), implementó esta plataforma para declaraciones de impuestos, pagos, facturación, descarga de certificados digitales o corrección de datos. Pero este sistema es altamente vulnerable a ciberataques, ya que expertos explicaron que el algoritmo RSA-1024, utilizado para registrar la firma del contribuyente, así como el SHA-1 (algoritmo del cual se elabora otro mensaje codificado) están clasificados como obsoletos desde el año 2010 por organismos de Seguridad.

Aunque el SAT ya está emigrando a una versión más poderosa como RSA-2048, los certificados digitales que fueron generados con la versión vulnerable RSA-1024 van a continuar hasta el año 2020. Además, la Clave Electrónica de Identificación Confidencial (CIEC) para acceder al sistema en línea del SAT, es un blanco potencial para un ataque, ya que sólo son de 8 caracteres, cuando lo recomendable es que la contraseña tenga una longitud de al menos 12 caracteres.

Fuente: **http://www.cronica.com.mx/notas/2016/966545.html**

EMPRESAS

La mayoría de las empresas NO sabe dónde está su información confidencial

por JUNIO 15, 2016 / CHANNEL BIZ

Un estudio hecho por Ponemon Institute, arrojó que el 72% de las empresas no confían en su habilidad para gestionar y controlar el acceso de los empleados a información confidencial. 60% no sabría decir qué información confidencial están compartiendo los empleados, quienes se han convertido en uno de los primeros responsables (60%) de las brechas de Seguridad, seguido por el robo o pérdida de los dispositivos (37%).

La mayoría de las organizaciones no tienen la tecnología para impedir que los empleados compartan información confidencial. Sólo un 36% dicen que sus empresas evitaron el intercambio de documentos confidenciales con terceros, y sólo un 27% impidieron que la información se compartiera entre los empleados. Según el estudio, titulado Risky Business: How Company Insiders Put High Value Information at Risk, el 73% de los encuestados dicen que sus empresas han perdido información confidencial en los últimos doce meses. Un 56% de las compañías no educan a los empleados acerca de proteger la información confidencial, y sólo un 44% utilizan herramientas para la prevención de la pérdida de datos.

Fuente: **http://www.channelbiz.es/2016/06/15/la-mayoria-de-las-empresas-no-sabe-donde-esta-su-informacion-confidencial/?utm_content=buffer478d5&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**

Robaron 178 millones de archivos a empresas en 2015

por JUNIO 14, 2016 / LA JORNADA

En 2015, cibercriminales robaron cerca de 178 millones de archivos de empresas, por lo que es necesario que el país implemente una estrategia nacional integral de ciberseguridad que permita ofrecer protección y certidumbre en sus operaciones al gobierno, las empresas y a usuarios de internet, señaló la Cámara Nacional de la Industria Electrónica de Telecomunicaciones y Tecnologías de la Información (Canieti).

Además, detalló que cerca del 89% de los ciberataques son financieros o de espionaje. El año pasado las campañas de spear-phishing orientadas a empleados de instituciones para el robo de datos personales y de archivos de las empresas aumentaron un 55%.

Fuente:
http://www.jornada.unam.mx/ultimas/2016/06/13/ciberdelincuentes-roban-178-millones-de-archivos-en-2015

CANIETI
www.canieti.org

TECNOLOGIA

Foro de ciberseguridad busca estrategia de protección para usuarios

por JUNIO 14, 2016 / EL UNIVERSAL

La Cámara de la Industria Electrónica de Telecomunicaciones y Tecnologías de Información (Canieti), realizará un foro nacional sobre ciberseguridad. Detalló que en 2020 el país contará con 84 millones de usuarios de Internet, un crecimiento de 31%, y de acuerdo con estudios recientes, cerca de 89% de los ciberataques son con objetivos financieros o de espionaje. El año pasado, las campañas de spear-phishing que buscan el robo de datos personales y de archivos de las empresas se incrementaron 55%.

Este foro buscará que México cuente con una estrategia integral contra los ciberdelincuentes, se busca que la estrategia obtenida en este encuentro ofrezca protección y certidumbre a los usuarios que realicen sus operaciones en la red.

Fuente: **http://eluniversal.com.mx/articulo/techbit/2016/06/14/foro-de-ciberseguridad-busca-estrategia-de-proteccion-para-usuarios**

Caen ventas de software "pirata" en México, señala Microsoft

por JUNIO 12, 2016 / LA JORNADA

Microsoft señaló que desde el año 2005, en México se vio una reducción de software "no original", estimando que, si en los dos próximos años esa tendencia continúa, la recaudación fiscal del país podría incrementarse en 500 millones de dólares.

Agregó que el 53% de los consumidores comentaron usar software pirata de forma "ocasional" o "rara vez", mientras el 35% dijo no usarlo nunca. El 83% de los empresarios tuvieron incidentes de virus informáticos asociados a software "no original". Microsoft señaló que el uso de software pirata aumenta el riesgo de ataques por malware, robo de identidad, robo de tarjeta de crédito y exposición de información personal.

Fuente: **http://www.jornada.unam.mx/ultimas/2016/06/12/caen-ventas-de-software-pirata-en-mexico-senala-microsoft**

Revolucionan la Seguridad con datos biométricos

por JUNIO 11, 2016 / EXCELSIOR

Las empresas y el propio gobierno están adoptando esta tecnología para luchar contra el creciente robo de identidad y tener un mayor control. Danilo Ochoa, director de ventas de comercio electrónico y e-banking de Gelmato, comentó que este cambio tendrá un impacto en la vida diaria de las personas y aceptó el temor de algunos usuarios a que les corten un dedo, les tomen una foto o los cibercriminales traten de burlar la biometría, pero hay diversas capas de Seguridad para evitar esto.

Dijo que existen sistemas que validan si una huella digital proviene de un dedo de una persona viva, analiza si hay rastros de sangre o si se intenta acceder con una fotografía al hacer reconocimiento de rostro. Las instituciones requerirán capturar los datos biométricos cada cierto tiempo, ya que el rostro cambia conforme pasa el tiempo y si la persona sube o baja de peso, las huellas se van desgastando con el tiempo, hasta la voz llega a cambiar.

Fuente: **http://www.excelsior.com.mx/hacker/2016/06/11/1098039**

México entre los más afectados por xDedic, el mercado de servidores hackeados

por JUNIO 15, 2016 / COMPUTER WORLD MEXICO

Kaspersky Lab, ha investigado un foro global donde hackers pueden comprar y vender acceso a servidores comprometidos en 6 dólares cada uno (113 pesos aproximadamente). El mercado xDedic, cuenta con 70,624 servidores de Protocolo de Escritorio Remoto (RDP) hackeados a la venta, este grupo parece ser ruso y no tiene vínculos o afiliaciones con los vendedores. Muchos alojan o proporcionan acceso a sitios web y servicios populares, algunos con software instalado para correo directo, contabilidad financiera y procesamiento de Punto de Venta (PoS).

Se pueden usar para atacar infraestructuras de los propietarios o como plataforma de lanzamiento para ataques más amplios, los propietarios, entre ellos el mismo gobierno, corporaciones y universidades, muchas veces desconocen de lo que está pasando. Últimos datos informan que, en mayo de 2016, este grupo tenía una lista de 70,624 servidores de 173 países a la venta, publicados en los nombres de 416 vendedores diferentes. México se encuentra en el doceavo lugar de los países afectados de América Latina.

Fuente: **http://computerworldmexico.com.mx/xdedic-mercado-servidores-hackeados-mexico-los-afectados/**

Nuevo hackeo masivo, esta vez en VerticalScopoe: 45 millones de registros de 1,100 webs

por JUNIO 15, 2016 / GENBETA

Hay indicios de que las páginas y comunidades que han utilizado la plataforma VerticalScope, han visto comprometidos los datos de sus usuarios, la empresa ya confirmó la violación de sus datos. LeakedSource asegura que VerticalScope y sus dominios fueron hackeados en febrero de este 2016. Tras obtener acceso a los datos, ha visto que estos contienen 45 millones de registros pertenecientes a 1,100 webs y comunidades como Techsupportforum, MobileCampsites, Pbnation o Motorcycle.com.

En los registros se encontraron datos como correos electrónicos, nombres de usuarios, direcciones IPs y contraseñas. LeakedSource teoriza que la única explicación para una filtración tan masiva es que VerticalScope almacenase todos sus datos en los mismos servidores, o en servidores interconectados entre sí. También han comprobado que, aunque las claves estaban cifradas, menos del 10% de ellas utilizaban métodos difíciles de descifrar.

Fuente: **http://www.genbeta.com/seguridad/nuevo-hackeo-masivo-esta-vez-de-verticalscope-45-millones-de-registros-de-1100-webs**

El ataque a LinkedIn está expandiendo malware bancario

por JUNIO 10, 2016 / TICBEAT

Hace días, 32 millones de cuentas y contraseñas de Twitter fueron robadas a consecuencia del ataque a LinkedIn. Al parecer, ciberdelincuentes están empleando los datos robados para expandir malware bancario a través de correos electrónicos usando técnicas de phishing. Siendo los más afectados los usuarios alemanes y holandeses, pero sin saber hasta dónde puede expandirse, pero se empieza a ver un aumento en los casos de robo de identidad y ataques de phishing, así como suplantación de identidad.

Los hackers están utilizando los datos asociados a los perfiles de LinkedIn para identificar a las víctimas, ponerles nombre y saber qué hacen o dónde viven. La unidad de respuesta para emergencia electrónicas de Alemania (CERT), avisó que haber detectado técnicas de phishing a través de correos electrónicos que contenían factura falsas y documentos, dirigidos a usuarios con su nombre completo, cargo profesional e incluso la compañía para la que trabajan, emplean macros incrustadas en los documentos adjuntos distribuyendo el troyano bancario Panda, especializado en el robo de credenciales de banca online.

Fuente: **http://www.ticbeat.com/seguridad/el-ataque-a-linkedin-esta-expandiendo-malware-bancario/?utm_content=buffer222a2&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**

Mexicanos dispuestos a cambiar de operador móvil en caso de falla de Seguridad

por JUNIO 08, 2016 / SEGURIDAD UNAM

A nivel global México ocupó el lugar más alto con un 73%, esto debido a que los consumidores tienen diferentes actitudes hacia la relación entre ellos, sus teléfonos y sus operadores. Según Giuseppe Targia, de Nokia, en algunos mercados, la gente piensa que son dueños del dispositivo, y el operador es sólo la conexión, mientras en otros mercados, el teléfono móvil es una extensión de su servicio telefónico.

Agregó que la cantidad de malware que detectan en el espacio móvil en los mercados de transición y los mercados emergentes, es mayor que en los mercados maduros. Así mismo, los clientes acostumbran a usar tiendas de aplicaciones no oficiales en los mercados emergentes, por lo que son más propensas a tener aplicaciones maliciosas. El 91% de los consumidores a nivel mundial están preocupados por lo menos de un problema de seguridad, pero en una lista de razones al elegir un operador.

Fuente:
http://www.seguridad.unam.mx/noticia/?noti=2904&utm_content=bufferf753b&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

TOTALSEC NEWSLETTER – INFOSEC

BOLETÍN No. 17

JUNIO 11 – 20, 2016

Elaboración: JUNIO 20, 2016

totalsec
Security Operation Center