NEWSLETTER – INFOSEC MX

BOLETIN No. 37

Octubre 29- Noviembre 06

Elaboración: Noviembre 07, 2016

Gobernación desmiente presunto hackeo por parte de la Agencia de Seguridad de Estados Unidos

por NOVIEMBRE 01, 2016 / ANIMAL POLITICO

La Secretaría de Gobernación (SEGOB), indicó que los servicios electrónicos de la dependencia se encuentran seguros, no están comprometidos y operan de manera ordinaria. Esto después de que el grupo de hackers The Shadow Brokers dio a conocer que la NSA espió los servidores de gobiernos y universidades de distintos países, entre los que se encontraban los de ambas dependencias mexicanas, junto con los de la Universidad Nacional Autónoma de México (UNAM). De acuerdo con Motherboard, la información revelada por The Shadow Brokers incluye 306 dominios y 352 direcciones IP de 49 países, entre ellos México, Rusia, China, India y Suecia.

En agosto pasado, este grupo hackeo los servidores de la NSA y filtró una serie de documentos, por lo que fue detenido Harold T. Martin III, un ex contratista de la agencia, acusado de espionaje. El 20 de octubre pasado, los fiscales federales que llevan el caso señalaron en un documento presentado ante la corte que el robo de información a la NSA fue impresionante por su longevidad y alcance. En respuesta, la Secretaría de Gobernación precisó que "el direccionamiento electrónico al que se hace referencia no coincide con los registros que en esta dependencia se tiene desde el 2012 a la fecha".

Fuente: **http://www.animalpolitico.com/2016/11/hackers-agencia-seguridad-espio/**

Malware fantasma, troyano malicioso que amenaza la seguridad móvil

por NOVIEMBRE 01, 2016 / EL UNIVERSAL

Aun habiendo sido descubierto hace dos años, sigue afectando a los usuarios de dispositivos Android, debido a que los usuarios no han actualizado los sistemas que borran la infección del denominado "Ghost Push", ya que usa varios disfraces para poder acceder a los dispositivos y sus datos. El malware inicia su ataque haciéndose pasar por una aplicación o plug-in, y se disfraza como Google Play, pidiendo al usuario revelar información de su tarjeta de crédito. Una vez en el dispositivo móvil, una segunda superposición de phishing pide a la víctima su teléfono y fecha de nacimiento.

La empresa advierte que los hackers son esnobs totales de las marcas, por lo que podemos darles "Me gusta" a sus páginas, las 'seguimos', y descargamos sus aplicaciones, estando al tanto los ciberdelincuentes. Por ello, se debe ser cuidadoso al descargar la aplicación móvil de una marca, pues a veces un gran nombre es la validación para confiar en una aplicación para obtener ofertas especiales, nuevo contenido o servicio al cliente. También en YouTube, los ciberdelincuentes actúan con comandos de voz escondidos. Para evitarlos se aconseja apagar el modo "siempre activado" del micrófono. Al incorporar una voz manipulada que diga "Ok Google", los delincuentes pueden alertar a su dispositivo y controlarlo, sin su conocimiento.

Fuente:
http://eluniversal.com.mx/articulo/techbit/2016/11/1/malware-fantasma-troyano-malicioso-que-amenaza-la-seguridad-movil

Preparan diputados castigos por ciberdelitos

por OCTUBRE 31, 2016 / MILENIO

Diputados locales del PRI y de Movimiento Ciudadano revelaron que preparan estrategias para castigar los ciberdelitos. Héctor García, presidente de la Comisión de Legislación, mencionó que se buscaría revisar la ley para que se puedan evitar delitos como el robo de datos por internet. A su vez, el diputado de Movimiento Ciudadano, Samuel García, mencionó que su fracción prepara una iniciativa para tipificar delitos como acoso o difamación que se cometen en la web, y para esto se estudia una legislación de California a fin de evitar casos como de sexting y otros en las redes sociales.

Arturo Salinas Garza, coordinador de la bancada del PAN, mencionó que es necesario que la Procuraduría General de Justicia de Nuevo León invierta en capacitación de los elementos para poder detener los ciberataques o ciberdelitos. El presidente de la Comisión de Legislación, Héctor García García, mencionó que buscarían promover una iniciativa para agravar y tipificar el robo de identidad en Nuevo León. Mencionó que, aunque actualmente en la entidad el Código Penal establece la suplantación de entidad, no hay una sanción grave.

Fuente: **http://www.milenio.com/politica/cyberdelitos_castigos-preparan_diputados-milenio_noticias_0_839316395.html**

Robo de identidad, el mayor temor de los millennials mexicanos

por OCTUBRE 31, 2016 / EXPANSION

Según un estudio de LexisNexis Risk Solutions, empresa dedicada al manejo de solución de riesgos, cerca del 74% de los mexicanos pertenecientes a esta generación le teme al robo de identidad a través de sus actividades en línea, esto a pesar de ser la más adepta a las compras en líneas, ya que el 60% realiza transacciones en línea, y utilizan en promedio 3.9 dispositivos móviles, solo 29% de ellos confía plenamente en las instituciones financieras sobre el manejo de su información personal.

Esta generación se muestra renuente al dar información a las instituciones, ya que, con los datos suficientes, estas instituciones podrán detectar delitos financieros y malos actores dentro del sistema. De acuerdo con el estudio, 77% de los millennials mexicanos está preocupado porque su información sea robada, mientras que 67% está de acuerdo en que la información que las empresas solicitan es necesaria para la prevención de fraude y otros delitos financieros.

Fuente: **http://expansion.mx/tecnologia/2016/10/31/robo-de-identidad-el-gran-temor-de-los-millennials-mexicanos**

Escuderías se "ciberblindan" durante el Gran Premio de México

por OCTUBRE 28, 2016 / EXPANSION

El 50% del desempeño del auto tiene que ver con la forma en la que los ingenieros le sacan provecho a los datos generados por el auto. Escuderías como Toro Rosso, Ferrari, Mercedes y otras, se han aliado con firmas de tecnología y ciberseguridad para proteger el manejo de esos datos. La firma Acronis dio a conocer que utilizarán un sistema de protección y manejo de datos en la nube, cuya seguridad se nada en Blockchain, que se basa en la autenticación compartida de varias partes de una cadena de datos, a los cuales solo se puede acceder si toda la cadena lo aprueba, evitando una manipulación de datos.

Al usar esta tecnología, se puede dar una mayor protección a los datos que se monitorean del coche durante las pruebas, que puede llegar hasta cinco terabytes. Durante el Gran Premio de México, la información de Toro Rosso y sus pilotos deberá ir también a Italia y Londres. La información debe ir segura y muy rápida, por lo que en cada sede de carrera se deben hacer adaptaciones para tener los datos disponibles y se utilizan conexiones móviles en lugar de satelitales. Si la conectividad de datos no está optimizada se pueden perder 0.01 décimos de segundo, perdiendo uno o dos lugares en la competencia y un impacto económico por lugar de hasta dos millones de dólares menos.

Fuente:
http://expansion.mx/tecnologia/2016/10/28/escuderias-se-ciberblindan-durante-el-gran-premio-de-mexico

¡Cuidado! Hay un sitio falso del Buró de Crédito, advierte Condusef

por OCTUBRE 28, 2016 / EL DIARIO DE CHIHUAHUA

La Condusef alerta sobre la existencia del sitio web www.burodecredito-consulta.mx, que busca engañar a los usuarios ofreciendo eliminar sus deudas, actualizar su Reporte de Buró de Crédito, e incluso borrar su historial negativo en cuestión de minutos, a cambio de una cantidad monetaria. En donde el presunto asesor, detalla las dos opciones para "salir" del Buró de Crédito.

La primera opción es para saber quién está "afectando" tu Buró de Crédito, quién te reportó, desde cuándo y por cuánto dinero por la cantidad de 999 pesos. La segunda opción, por un costo de 1,999 pesos, ofrece sacarte del Buró de Crédito, obtener nuevos créditos. El pago de uno de estos servicios es mediante una tienda de conveniencia, a una cuenta bancaria. Condusef recordó a los usuarios que ninguna entidad financiera puede borrar la información de quien se encuentra en el Buró de Crédito. El crédito o el historial de pagos pueden eliminarse 72 meses contados a partir de la fecha de liquidación, siempre y cuando el Otorgante de Crédito haya reportado la fecha de cierre.

Fuente:
http://eldiariodechihuahua.mx/Economia/2016/10/28/cuidado-hay-un-sitio-falso-del-buro-de-credito-advierte-condusef/

Incrementan ciberataques financieros: Banorte

por OCTUBRE 21, 2016 / EL UNIVERSAL

El director general de Grupo Financiero Banorte, Marcos Ramírez, dijo que el número de ataques cibernéticos que sufre el sistema financiero mexicano es creciente ante lo cual se han reforzado las medidas de seguridad para evitar daños a las instituciones y usuarios. Agregó que la cifra es impresionante, alarmante y depende a qué se le llame ataque, ya sí alguien desde algún lado manda un chat a ver si caen o si puede bloquearte algo no es nada pero es un pequeño ataque.

O los que vienen un poco más formalizados que te llenan la red de datos para bloquearte un poco el tiempo y te tiran durante unos segundos la red. Al igual que otras instituciones financieras, Banorte enfrenta ataques constantes los cuales no han vulnerado sus sistemas.

Fuente
http://www.eluniversal.com.mx/articulo/cartera/finanzas/2016/10/21/incrementan-ciberataques-financieros-banorte

Analizarán expertos la ciberseguridad en México

por NOVIEMBRE 03, 2016 / MI AMBIENTE

Según la Asociación Mexicana de Internet (Amipci), 65 millones de mexicanos son usuarios de internet, representando casi el 60% de la población del país. 36% de estos utiliza el servicio para realizar compras en línea y 26% realiza operaciones de banca en línea. Por lo que ALAPSI (Asociación Latinoamericana de Profesionales en Seguridad Informática), analizará los temas de ciberseguridad, en el foro nacional "Ciberseguridad, el lado humano: ¿Estás seguro?", los próximos 29 y 30 de noviembre en Ciudad de México.

Esto con la intención de analizar los avances de la seguridad cibernética, su entorno e impacto en el mercado, los resultados de las mejores prácticas en seguridad lógica y establecer objetivos y planes de seguridad, así como integrar a profesionales y empresas dedicados al tema. Una de las metas principales es proponer políticas, normas y legislación en la materia, promoviendo prácticas que aseguren la confidencialidad, integridad y disponibilidad de los recursos informáticos de las organizaciones cuyo enfoque se centre en la importancia de la cultura a los usuarios respecto a la Seguridad Informática.

Fuente: **http://www.miambiente.com.mx/notas/analizaran-expertos-la-ciberseguridad-en-mexico**

México, uno de los países "hackeados" por la NSA

por NOVIEMBRE 02, 2016 / LA PANCARTA DE QUINTANA ROO

El grupo de hackers The Shadow Brokers filtró una lista de servidores a los que supuestamente el Grupo Equation, ligado a la Agencia de Seguridad Nacional (NSA) había comprometido. Según el sitio Hacker House, las direcciones de IP y dominios que fueron objeto del ciberataque se encuentran alrededor del mundo y los 10 países más atacados fueron: China, Japón, Corea, España, Alemania, India, Taiwán, México, Italia y Rusia. De confirmarse esta lista, significaría que la NSA, indirectamente, estuvo atacando o vigilando diferentes servidores de diferentes instituciones a nivel mundial.

La lista de las más de 300 direcciones de IP y 300 dominios diferentes que fueron atacados por la NSA, se encuentra disponible en una publicación dentro del blog del grupo de hackers, y en donde explican que esta filtración busca llamar la atención del ciberespionaje que se realiza en Estados Unidos, además de pedir a los ciudadanos americanos boicotear las elecciones. El investigador en seguridad Mustafa Al-Bassam aseguró que los archivos filtrados por el grupo de hackers son de entre 2000 y 2010, por lo que es muy probable que el spyware ya haya caducado. Según el sitio especializado TechCrunch, estas filtraciones podrían haber contado con la ayuda del ex contratista de la NSA, Harold Martin, quien actualmente enfrenta una investigación por haber extraído información clasificada de la Agencia de Seguridad Nacional de los Estados Unidos.

Fuente: **http://lapancartadequintanaroo.com.mx/ciencia-y-tecnologia/mexico-uno-de-los-paises-hackeados-por-la-nsa/**

Agentes de la SSP – CDMX recibirán capacitación de Corea del Sur

por NOVIEMBRE 01, 2016 / AZTECA NOTICIAS

El Secretario de Seguridad Pública de la Ciudad de México, Hiram Almeida Estrada, aseguró que hoy en día el fenómeno delictivo no es menor y existen nuevas formas de realizarlo, por lo que destacó la importancia de trabajar coordinadamente con países expertos en el tema para combatir la delincuencia. Al inaugurar el curso de "Estudios de Ciberdelincuencia e Investigación", donde 40 agentes de la secretaría recibirán una capacitación de 40 horas abarcando los temas de ciberterrorismo, redes sociales, abuso sexual infantil, suplantación de identidad, extorsiones y fraude cibernético por parte de elementos de la Policía Nacional de Corea del Sur.

El subsecretario de Información e Inteligencia Policial de la secretaria, José Gil informó que diariamente en la Ciudad de México se reciben 10 llamadas de denuncia al día en torno a este tipo de delitos. "Hoy en cada uno de los delitos que se cometen en la Ciudad de México por lo menos la tecnología se encuentra presente en 9 de ellos de cada 10 de estos delitos en 9 hay un teléfono celular, hay una computadora, hay una conversación por Whatsapp por internet entonces en todos estos delitos interviene la Policía Cibernética.

Fuente:
http://www.aztecanoticias.com.mx/notas/seguridad/264111/agentes-de-la-ssp-cdmx-recibiran-capacitacion-de-corea-del-sur

Malware aumenta 35% durante el tercer trimestre del año

por OCTUBRE 25, 2016 / SEGURIDAD UNAM

AppRiver encontró tráfico de malware ampliado durante el cuarto trimestre, los analistas pusieron en cuarentena 5,7 millones de correos electrónicos con malware, siendo más del triple de los observados durante todo el 2015. Los formatos de archivo con los que ha llegado el malware son JScript (.js), Windows Script Archivos (.wsf), y documentos con las macros habilitadas (.doc y .xls). El malware para Denegación de Servicio Distribuida (DDoS) está en aumento, con distorsiones provocadas por botnets conformadas principalmente por dispositivos IoT (Internet of Things), como Mirai.

A medida que más dispositivos IoT se conecten de manera insegura, esta tendencia empeorará a corto plazo. Después de la actualización de seguridad de Apple, un exploit muy avanzado de malware fue descubierto usando múltiples ataques de día cero que podrían acceder al sistema operativo de un dispositivo iOS9 (jailbreak), Apple ha corregido el fallo. El ransomware sigue siendo popular habiendo versiones con objetivos específicos vistos en los últimos meses. Locky y Zepto siguen siendo algunos de los primeros en cuanto a volumen aumenta, pero están de cerca EduCrypt, ransomware para IoT y MarsJoke. El tráfico de spam estuvo constante, AppRiver puso en cuarentena 2,34 mil millones de mensajes de spam. Siendo PayPal el tema de mensaje de phishing que también aumentó.

Fuente:
http://www.seguridad.unam.mx/noticia/?noti=3076&utm_content=buffer08ac1&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

TOTALSEC NEWSLETTER – INFOSEC

BOLETÍN No. 37

Octubre 29- Noviembre 06, 2016

Elaboración: Noviembre 07, 2016

totalsec