NEWSLETTER – INFOSEC MX

BOLETIN No. 13

MAYO 14-22

Elaboración: Mayo 23, 2016

NEGOCIOS

En este número encontrarás noticias sobre:

- Negocios
- Tecnología
- El Mundo

Aumenta la preocupación de empresas y consumidores por la privacidad de los datos

por MAYO 10 2016 / SILICON

Deloitte en un estudio reveló que los sectores bancario y financiero, gobierno y energía, son identificados como los de mayor confianza por los consumidores en cuanto a la privacidad de los datos. Por el contrario, los medios sociales, los medios de comunicación y los bienes raíces, se han señalado como los de mayor riesgo.

Mostró que ahora los consumidores son más exigentes en la privacidad y protección de datos. Un 94% califica a la confianza, como el atributo más importante, antes que el fácil acceso a un sitio web, aplicación o dispositivo. Más del 21% quiere saber si su información se envía a terceros, y el otro 14% se informa sobre cómo proteger su información personal como de la tarjeta de crédito, claves y registros médicos.

Fuente: http://www.silicon.es/aumenta-la-preocupacion-de-empresas-y-consumidores-por-la-privacidad-de-los-datos-2308157?utm_content=buffer25b91&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

TECNOLOGÍA

La fibra óptica está en la mira de los hackers

por MAYO 17, 2016 / EL FINANCIERO

La fibra óptica también puede ser hackeada para sustraer información como cuentas y contraseñas bancarias de servicios como Netflix, Spotify o de bancos. De acuerdo con Héctor Silva, Director de Tecnología de Ciena, la vulnerabilidad comienza a partir del fácil alcance de los cables de fibra óptica. En sitios como itconference.org, se muestra cómo sustraer la información del cableado de fibra óptica.

Existen métodos y soluciones que permiten blindar la información que viaja a través de la fibra óptica. Una solución es incorporar una capacidad de cifrado directamente en el equipo óptico, lo que hacen estas herramientas es añadir un código que hace que esa información no pueda ser recuperada a menos que se tenga el código.

Fuente: http://www.elfinanciero.com.mx/tech/fibra-optica-en-la-mira-de-hackers.html

Karspersky busca participar en plan de ciberseguridad en México

por MAYO 12, 2016 / EL FINANCIERO

Roberto Martínez, analista de malware del equipo de Investigación y análisis para América Latina de Kaspersky Lab, dijo que se han tenido acercamientos con el gobierno mexicano con el objetivo de colaborar en la protección de la información medular de este gobierno, así como su infraestructura estratégica, y está en negociaciones para participar en el plan de ciberseguridad proyectado hacia 2018, en el que el país invertirá 89 millones de dólares.

Así mismo anunció que la empresa lanzó Kaspersky Industrial CyberSecurity, que combina las principales tecnologías, servicios e inteligencia de la compañía en un paquete que protege el funcionamiento de las instalaciones industriales modernas, desde centrales eléctricas, refinerías y líneas de ensamble, hasta ferrocarriles, aeropuertos y edificios inteligentes.

Fuente: http://www.elfinanciero.com.mx/empresas/kaspersky-busca-proteger-ciberseguridad-en-mexico.html

El 80% de los ciberataques tienen su origen en un fallo humano de Seguridad

por MAYO 05, 2016 / ABC

La empresa de ciberseguridad S2 Grupo, revela que de ocho de cada diez ciberataques a empresas e instituciones públicas, se producen como consecuencia de fallos humanos, por lo que es esencial hacer conciencia en los empleados sobre los riesgos y consecuencias para minimizar estas amenazas, ya que, por medio de técnicas como la Ingeniería Social, los ciberdelicuentes pueden poner en riesgo la Seguridad de cualquier persona, compañía o estado.

Algo a considerar es que se debe involucrar al empleado en la protección de la información que maneja, a través del conocimiento, normas, procedimientos y buenas prácticas en Seguridad. El empleado es quien gestiona riesgos que afectan a la Seguridad de la Información de la empresa y, por tanto, las empresas y organismos públicos deben capacitar a las personas para el manejo adecuado de la información.

Fuente: **http://www.abc.es/tecnologia/redes/abci-80-por-ciento-ciberataques-responden-fallos-humanos-seguridad-201605121355_noticia.html**

México vende Bitcoins en las tiendas de barrio

por MAYO 17, 2016 / REVISTA PAGOS

México será el primer país donde las tiendas de abarrotes vendan Bitcoins. Esta iniciativa surge del Grupo Zmart, una de las 30 empresas de negocios Forbes 2016, que tiene como objetivo abrir el comercio electrónico a personas no bancarizadas. Este servicio se realizará a través de la empresa Bitso y estará disponible con la aplicación de Max Saldo.

Según Christian Sandoval, Director General de Grupo Zmart, no se necesitará comprar unidades completas de esta moneda, bastará con comprar una cantidad en pesos para que la cartera digital haga automáticamente la conversión a Bitcoin.

Fuente: **http://www.revistapagos.com/2016/05/mexico-vende-bitcoins-las-tiendas-barrio/**

Fortium, el malware paranóico que busca la presencia de 400 virus antes de ejecutarse

por MAYO 02, 2016 / REDES ZONE

Denominado también "The paranoid malware", y teniendo como función que justo antes de instalarse y ejecutarse, analiza el sistema para comprobar si está siendo ejecutado en un espacio aislado, sandbox, o en un sistema operativo virtualizado. Si pasa con éxito, también busca la existencia alguna aplicación de análisis forense o un software antivirus de una lista de más de 400 software de Seguridad.

Además, al no detectar lo antes mencionado, modifica los DNS del sistema por los de Google y Level3 para evitar sistemas de filtrado de IPs y bloquea el acceso a más de 250 dominios de Seguridad como webs de análisis de archivos y descarga de antivirus. También desactiva las notificaciones del sistema operativo y bloquea el acceso a la línea de comandos y al administrador de tareas de Windows. Si todo es correcto, el malware empezará a enviar la información a un servidor con IP rusa pero que, termina en una dirección de Ucrania, el malware ha presentado cierta resistencia, especialmente a la hora de adivinar el servidor de control remoto real.

Fuente: **http://www.redeszone.net/2016/05/17/furtim-malware-paranoico-busca-la-presencia-400-antivirus-ejecutarse/**

Crean solución que certifica la Seguridad de las apps para automóviles

por MAYO 04, 2016 / SILICON

Appytest for Auto, aplicación hecha de la unión entre Tecnocom y el Centro Tecnológico Eurecat, la cual forma parte del proyecto Appytest, y es definido por sus autores como el "primer certificado de Seguridad" de este tipo.

Santiago Begué de Eurecat, comentó que este certificado "acredita que una aplicación móvil para el coche cumple con el estándar de la industria para la conectividad del vehículo, ya adoptada por la mayoría de los fabricantes de automóviles y de teléfonos inteligentes". Esta solución trabaja con una serie de aspectos como la compatibilidad del software, su estabilidad o su rendimiento. Appytest for Auto contó con financiación del programa AEESD del Ministerio de Industria.

Fuente: **http://www.silicon.es/crean-una-solucion-que-certifica-la-seguridad-de-las-apps-para-el-automovil-2307701?utm_content=buffer8637b&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer#dRVXgJCSolKV4ePb.99**

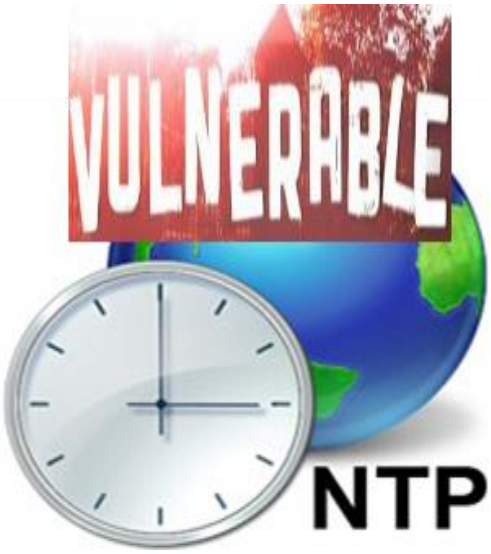
Se descubren 11 nuevas vulnerabilidades en el protocolo NTP

por MAYO 02, 2016 / NOTICIAS SEGURIDAD

Este protocolo gestiona la sincronización de los relojes en los ordenadores, servidores, routers y cualquier dispositivo que está conectado a Internet. Al no tener la hora correcta en los diferentes sistemas, se tendrían problemas incluso navegando por Internet. Entre las vulnerabilidades descubiertas se encuentran: Una relacionada con el filtrado de paquetes del rango de red 192.0.0.0/8 que podría permitir a un atacante que envíe paquetes falsificados modificar el reloj para realizar ataques Man In The Middle y descifrar el tráfico HTTPS, sin importar que las páginas web tengan habilitado HSTS ya que tienen en cuenta el tiempo.

Otra, es cambiar la fecha un año hacia atrás, para que el sistema acepte certificados de seguridad ya revocados, comprometiendo la clave privada y afectar los servicios de autenticación como Kerberos o Active Directory, ya que dependen de un reloj para su correcto funcionamiento. El equipo de desarrollo de ntpd ha lanzado el parche versión 4.2.8p7, que se encuentra disponible en su página web oficial.

Fuente: **http://noticiasseguridad.com/vulnerabilidades/se-descubren-11-nuevas-vulnerabilidades-en-el-protocolo-ntp/**



Una de las nubes más seguras llegará a México en 2017

por MAYO 11, 2016 / EXPANSIÓN

Según un estudio realizado por Business Software Alliance (BSA) sobre la adopción de la nube en América Latina, México está en el lugar 15 de 24 en la región. Los sectores de misión crítica (servicios vitales como agua, energía o petróleo), son considerados como los que están en mayor riesgo ante un ataque cibernético grave. La Organización de Estados Americanos (OEA), con la firma de Seguridad McAfee, dijeron en 2015, que México no está preparado para enfrentar un ataque por no invertir en ciberseguridad.

Rodney Rodgers, director general de Virtustream, dijo que en Estados Unidos ya están por tener completa la expansión y piensan elevar la capacidad de nodos. Están completando la expansión con Alemania y Francia, para seguir con Japón; llegando a México a inicios de 2017. Además, asegura que sus servicios son de los más sofisticados para proteger este tipo de infraestructuras, por medio de prácticas como monitoreo constante de cada set de datos por medio de sensores, por lo que el sistema notifica cuando hace falta un parche de Seguridad o similar.

Fuente: **http://expansion.mx/tecnologia/2016/05/04/una-de-las-nubes-mas-seguras-llegara-a-mexico-en-2017**

EL MUNDO

La OCDE busca delinear política digital

por MAYO 13, 2016 / EL UNIVERSAL

Los países miembros de la OCDE, buscan definir estrategias que ayuden a crear políticas públicas en materia de ciberseguridad, comercio internacional, neutralidad de la red y combate a piratería digital.

En la Reunión Ministerial, que se llevará a cabo en junio, en Cancún, México; elaborarán una declaración de ministros que servirá de base para la elaboración de políticas públicas.

En tanto, Mónica Aspe, subsecretaria de la Secretaría de Comunicaciones y Transportes (SCT), señaló que este evento es una oportunidad para dar a conocer los resultados de México en materia de economía digital, principalmente los avances de la reforma de telecomunicaciones.

Fuente:
http://www.eluniversal.com.mx/articulo/cartera/finanzas/2016/05/13/ocde-busca-delinear-politica-publica-digital

Altos funcionarios de Estados Unidos y México debaten cuestiones de Seguridad

por MAYO 13,2016 / EFE

Los pasados días 12 y 13 de mayo en la Ciudad de México, hubo un encuentro entre funcionarios norteamericanos con homólogos mexicanos para debatir cuestiones de ciberseguridad. Por parte de México participaron representantes del gobierno, académicos y del sector privado, esto según un comunicado del Departamento de Estado de Estados Unidos.

Christopher Painter, coordinador de Ciberseguridad en el Departamento de Estado, iba al frente de la comitiva estadounidense, y estuvo acompañado por otros miembros de la diplomacia de Estados Unidos, funcionarios del Departamento de Seguridad Nacional, de Justicia, de Defensa y del Consejo de Seguridad Nacional.

Fuente: http://www.efe.com/efe/america/mexico/altos-funcionarios-de-ee-uu-y-mexico-debaten-cuestiones-ciberseguridad/50000545-2925647

TOTALSEC NEWSLETTER – INFOSEC

BOLETÍN No. 13

MAYO 14-22, 2016

Elaboración: MAYO 23, 2016

totalsec
Security Operation Center