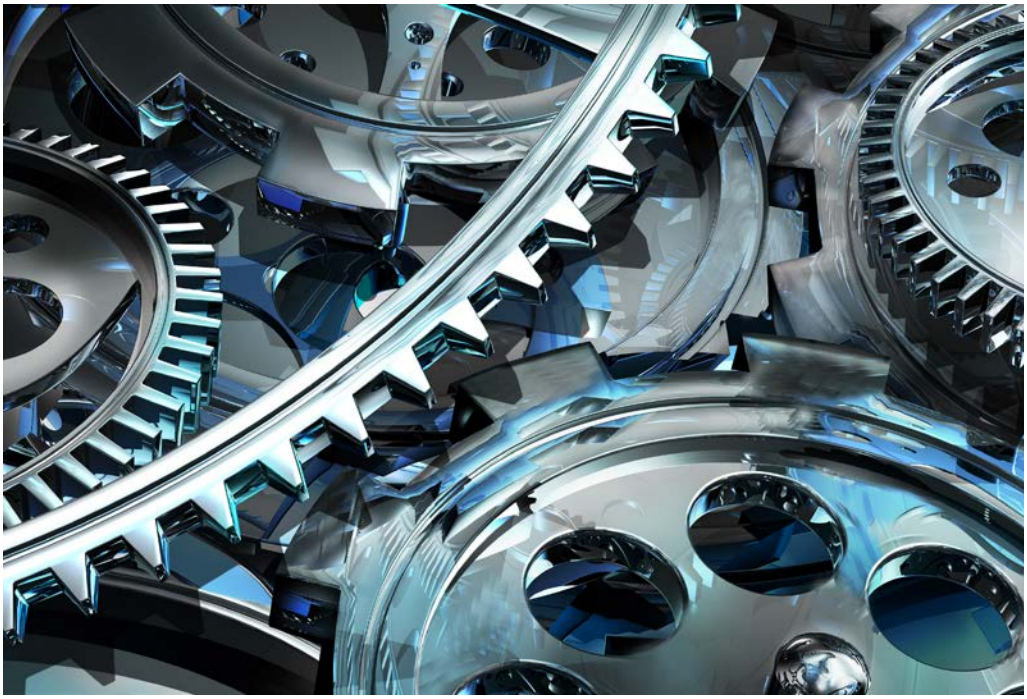

NEWSLETTER – INFOSEC MX

BOLETIN No. 19

JUNIO 25 - JULIO 03

Elaboración: Julio 04, 2016

Para entrar a Estados Unidos habrá que informar cuentas de Twitter y Facebook

por JUNIO 26, 2016 / SIN EMBARGO

A raíz de las amenazas y atentados terroristas, los cuerpos de seguridad de Estados Unidos van incorporando nuevos filtros en sus aduanas para impedir la entrada de posibles delincuentes peligrosos. Una de las áreas que más se va a reforzar es el registro de todas las cuentas en redes sociales de quienes quieran tener acceso a ese país; por lo que extranjeros deberán notificar su presencia en Internet para que las autoridades puedan comprobar si representa algún peligro.

Esto fue propuesto por el organismo de aduanas y patrullas fronterizas de EU al Registro Federal, sugiriendo la creación de un nuevo campo en el impreso para solicitar un visado –también en las solicitudes del Sistema Electrónico de Autorización de Viaje (ESTA), el documento que permite viajar a EU sin visado– en el que se deban declarar las distintas cuentas en redes sociales con los correspondientes nombres de usuario

Fuente: **http://www.ticbeat.com/socialmedia/para-entrar-en-estados-unidos-habra-que-informar-de-nuestras-cuentas-en-twitter-y-facebook/**

Google enseñará a los mexicanos a desarrollar apps

por JUNIO 21, 2016 / EXCELSIOR

El pasado 21 de junio, se realizó por primera vez en México el encuentro Google Play Apps & Juegos, reuniendo a socios y desarrolladores. Regina Chamma, de Google Play Apps y Juegos para América Latina, dijo que el potencial del país se refleja en que la penetración de teléfonos inteligentes apenas es de 35%, la descarga mensual de aplicaciones nacionales creció 100% en 2015. Se enseñó a los desarrolladores las formas que existen para monetizar su aplicación y nuevas herramientas para crear aplicaciones en Android, entre otras cosas.

Google Play hace investigación sobre desarrollo de herramientas y programación que sean más fáciles para construir aplicaciones en Android; como Firebase, una plataforma con muchas "librerías". El reto no es programar, sino desarrollar ideas, entender al cliente y saber sus necesidades. Google lanzará con su nuevo sistema operativo Android N, la herramienta Instant Apps, con la que no es necesario descargar una aplicación.

Fuente:
http://www.excelsior.com.mx/hacker/2016/06/21/1100135

El backup como plan B para enfrentar el ransomware

por JUNIO 23, 2016 / COMPUTER WORLD MEXICO

El ransomware se ha disfrazado de diferentes maneras, aumentando la posibilidad de que este pueda ser activado al momento de caer al buzón del correo electrónico de la víctima. Se recomienda usar software adicional de backup y recuperación utilizado para recuperar el sistema. La empresa Paragon ofrece la solución Hard Disk Manager, que establece copias de seguridad incrementales, el proceso se realiza constantemente y ocupando poco espacio, consumiendo escasos recursos del sistema. Cuando el problema es detectado, se puede determinar fecha y hora de actuación de este y restaurar los datos a un punto anterior.

Para las empresas, se encuentra la solución profesional Paragon Protect & Restore, con una única consola de gestión centralizada con la que es posible recuperar servidores físicos, máquinas virtuales, y estaciones de trabajo. Haciendo posible solventar cualquier inconveniente relacionado con el puesto de red de un usuario, con los archivos individuales del mismo, con las bases de datos de Exchange, con los buzones de correo de los empleados, así como con la copia de seguridad y restauración de todo el sistema.

Fuente:
http://www.seguridad.unam.mx/noticia/?noti=2894&utm_content=buffera6a13&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

Evita caer en falsas ofertas de verano

por JUNIO 20, 2016 / PC WORLD MEXICO

La firma G Data comparte unos pasos para evitar caer en las redes de los cibercriminales como: Usar una solución de seguridad que proteja contra el malware y bloquee ataques de phising, incluya un filtro antispam y protección de banca y compras online. Instalar periódicamente las actualizaciones del sistema operativo y programas. Mandar correo no deseado a la papelera. Tener cuidado con correos que ofrecen artículos a precios muy bajos, no hacer clic en los enlaces, no reenviar el correo, y mucho menos responderlo.

Borrar continuamente el historial del navegador, así como eliminar las cookies para dificultar el seguimiento por parte de otros. Comprobar si los sitios favoritos en el navegador son originales. No aceptar peticiones de amistad de desconocidos. Tener una contraseña fuerte en plataformas sociales. Eliminar etiquetados no deseados en fotos y comentarios de Facebook y revisar el contenido donde se encuentre etiquetado por terceros.

Fuente: http://www.pcworld.com.mx/Articulos/36184.htm#

Preocupa a Banco de México "hackeo" en sistemas financieros

por JUNIO 29, 2016 / EL FINANCIERO

En la ponencia "Amenazas y tendencias en las infraestructuras de mercado" que se realizó durante la Conferencia Regional para América Latina 2016 de SWIFT, Miguel Díaz, director de Sistema de Pagos de Banco de México, afirmó que a esa institución le preocupa mucho los ciberataques y el que el público quiera operaciones en tiempo real, el reto es hacer eficiente esta facilidad sin que los hackers tomen beneficios de ello.

Durante la ponencia, Roberto González, CEO de Post-Trade en el Indeval de la Bolsa Mexicana de Valores (BMV), comentó que, en la parte del mercado bursátil, al igual que en la banca, los ciberataques se están convirtiendo en una prioridad. La tecnología ayuda a reducir costos y ser competitivos al estar bien implantada. El directivo del Indeval reveló que el Grupo BMV está proyectando una nueva tecnología en post-trade: Blockchain, estimado en una inversión de 500 y 600 millones de dólares en soluciones utilizando DLT (distributed ledger technology).

Fuente: http://www.welivesecurity.com/la-es/2016/06/20/cuantos-usuarios-ransomware-en-latinoamerica/?utm_content=buffer09ddd&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

HTML5 tampoco es capaz de prevenir los ataques del malvertising

por JUNIO 27, 2016 / SILICON

HTML5 es la tecnología que se está defendiendo como sustituta ideal para Flash, tanto por sus características como desde el punto de vista de la seguridad. Sin embargo, HTML5 acaba de ser retirado por GeoEdge, y publicó en el informe "Security Aspects of Flash, HTML5 and Video in the Ad Tech Industry" que al menos en cuestión de anuncios, seguridad y malvertising, las vulnerabilidades de Flash no serían peores a las que podrían tumbar a HTML5 ya que este también permitiría la inserción de código malicioso.

GeoEdge indica que el contenido HTML5, incluyendo los vídeos, es vulnerable a inserción de malware, ya sea en la publicidad o por parámetros VAST. Dice que no hay nada que evite a un atacante inyectar una URL maliciosa utilizando código de terceros en VAST o XML, o por inyección directa de un bloque de anuncios maliciosos. El insertar código JavaScript se usa mucho en ciberataques y actúa de base para HTML5, abriendo puertas al código malicioso en HTLM5 sín mucha dificultad.

Fuente: http://www.silicon.es/html5-tampoco-previene-malvertising-2312410

Un fallo de Chrome permite piratear y descargar películas de Netflix o Amazon

por JUNIO 24, 2016 / ADSL ZONE

Se hizo público la existencia de un fallo en el navegador Google Chrome que permite piratear y descargar copias de las películas colgadas en portales como Netflix o Amazon. David Livshits del Cyber Security Research Center en la Universidad Ben-Gurion de Israel junto con Alexandra Mikityuk con Telekom Innovation Laboratories en Berlín, alertaron a Google el pasado 24 de mayo de este fallo en su navegador. Pero no se ha lanzado ningún tipo de parche para corregirlo.

Al parecer el problema está en cómo implementa Google la tecnología Widevine EME/CDM. Pero la empresa ya declaró que están estudiándolo afirmando que no es algo suyo únicamente, ya que cualquier navegador basado en Chromium estaría afectado.

Fuente: http://www.adslzone.net/2016/06/24/fallo-chrome-permite-piratear-descargar-peliculas-netflix-amazon

Estos son los efectos negativos del phishing para las empresas

por JUNIO 24. 2016 / SILICON

Un informe de Return Path analizó los efectos del phishing sobre las empresas, revelando que estos ataques tienen costos directos reales para cada empresa que los sufre de 3,7 millones de dólares (69 millones de pesos aprox.) al año. Estos ataques traen perdidas de productividad para esas compañías, afectando su servicio de atención al cliente y pueden ser multadas. Agregando que reduce la confianza de los clientes que están suscritos a los newsletters y mailings de la empresa afectada.

Estelle Derouet, Vicepresidenta de Marketing y Prevención de Fraude en Emails para Return Path, señala que, si la reputación de una marca se ha visto afectada por un fraude a través del correo electrónico, los clientes dejarán de abrir sus emails y los proveedores de servicios de mail puede que no muestren esos mensajes en la bandeja de entrada, situaciones que hacen perder a las empresas oportunidades de generar ingresos.

Fuente: http://www.silicon.es/2312363-2312363?utm_content=buffer6ae50&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer#93fXmJLhpv2W1khH.99

Las víctimas del criptoransomware se han quintuplicado

por JUNIO 23, 2016 / SILICON

Según Kaspersky Lab, el número de usuarios que han sufrido los efectos del criptoransomware en primera persona se ha disparado de 131.111 a 718.536 en un solo año. El avance del ransomware en los últimos 24 meses ha sido notable, el número de usuarios que se han topado con esta amenaza ha pasado de 1.967.784 entre abril de 2014 y marzo de 2015 a 2.315.931 entre abril de 2015 y marzo de 2016, lo que implica un incremento del 17,7 %.

La mayoría de las víctimas están en Alemania, Italia y Estados Unidos. Sinitsyn, de Kaspersky comenta que las empresas y los usuarios pueden protegerse con la aplicación de copias de seguridad periódicas, utilizando una solución de seguridad probada y manteniéndose informados sobre los riesgos de seguridad cibernética actuales. Así que, aunque el ransomware parece ser rentable y seguro para los criminales todavía hay esperanza, esto se puede mediante la aplicación de estas medidas básicas.

Fuente: http://www.silicon.es/victimas-criptoransomware-quintuplicado-2312204?utm_content=buffere668c&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

Nueva estafa se hace pasar por empresa de telecomunicaciones

por JUNIO 23, 2016 / SEGURIDAD UNAM

Usuarios han informado recibir mensajes realistas de los ISP, diciendo que se ha detectado malware en sus equipos y que deben llamar al número de "ayuda inmediata". Estos incidentes están aumentando, Symantec registró un crecimiento de 200% en estafas de soporte técnico este año. Los estafadores pueden conocer los ISP de los usuarios con la colocación de anuncios en sitios web maliciosos que infectan la computadora de los usuarios, los redirige a un sitio web oculto y descubren su dirección IP.

El supuesto soporte técnico engaña a las víctimas de dos formas, una mediante el acceso remoto a la computadora de la víctima con los permisos que adquieren por teléfono y sín que los usuarios lo sepan, instalan software malicioso en su computadora para analizar información financiera. Y la otra, convenciendo los estafadores a las víctimas para hacer un pago de 200 dólares (3 mil 700 pesos aprox.) por el soporte técnico falso.

Fuente:
http://www.seguridad.unam.mx/noticia/?noti=2922&utm_content=buffer98b46&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

En México hasta 40 mil dólares exigen los ciberextorsionadores para liberar datos: expertos

por JUNIO 28, 2016 / NOTICIAS MVS

En México, ciberdelincuentes exigen a hasta 40 mil dólares (735 mil pesos aprox.) para liberar información encriptada, para después ser vendida como base de datos o en el mercado negro. Eduardo Ellerbraker, director de TrustPort México, señaló que es cada vez más común el acceso a información de alta prioridad mediante virus casi indetectables. Hasta 60% de los usuarios de antivirus lo adquieren de manera ilícita o gratuita, programas que incluso ya traen virus o alentan demasiado los equipos.

Además, informó que esta firma, originaria de la República Checa, signó una alianza con la Universidad Autónoma Metropolitana (UAM) para ocupar las herramientas tecnológicas y proteger su información, así como para cumplir sus objetivos en seguridad. Esto también abrirá las puertas de la UAM con el gobierno de la República Checa, a través de su embajada en México, la cual está interesada en que exista intercambio de profesores entre instituciones de educación superior de ambos países.

Fuente: http://www.noticiasmvs.com/#!/noticias/hasta-40-mil-dolares-exigen-ciberextorsionadores-para-liberar-datos-expertos-966

TOTALSEC NEWSLETTER – INFOSEC

BOLETÍN No. 19

JUNIO 25 – JULIO 03, 2016

Elaboración: JULIO 04, 2016

totalsec
Security Operation Center