TOTALSEC NEWSLETTER – INFOSEC MX

BOLETIN 5

MARZO 19 – 27

Elaboración: Marzo 28, 2016

TECNOLOGÍA

En este número encontrarás noticias sobre:
- Tecnología
- Servicios Financieros
- Negocio
- Gobierno
- Redes Sociales

Protocolo cifrado de correo electrónico, el arquetipo Google, Microsoft y Yahoo

por MARZO 22, 2016 / NOTICIAS SEGURIDAD

Google, Microsoft y Yahoo, han desarrollado en conjunto un Protocolo Cifrado de Correo Electrónico, el cual fue aprobado por Comcast y LinkedIn, estas firmas buscan crear una mega estructura de seguridad especializada.

Esta propuesta nombrada como SMTP (Escritura de seguridad transparente) presentada el 18 de marzo del año en curso, está basado en un sistema de vigilancia cibernética, propuesto en 1982 como una extensión denominada STARTTLS.

Este protocolo funciona con una estructura similar a la extensión HSTS (HTTP Strict Transport Security), proporciona información sobre los intentos externos de acceder a la plataforma, permitirá establecer canales de comunicación segura en intercambios de correo electrónico.

Fuente: http://noticiasseguridad.com/seguridad-informatica/protocolo-cifrado-de-correo-electronico-el-arquetipo-google-microsoft-y-yahoo/

Robo y usurpación de identidad

MARZO 10, 2016 / CAMARA DE DIPUTADOS

NOTA No. 2266. Robo y usurpación de identidad

La diputada Gloria Himelda Félix Niebla (PRI), presentó una iniciativa en la que reforma algunas disposiciones del Código Penal Federal, con el objetivo de tipificar el delito contra la identidad de las personas y la usurpación de identidad como un delito autónomo, estableciendo sanción de tres meses a siete años de prisión y de 100 a 400 días multa.

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, informó que México ocupa el octavo lugar en este delito y según el Banco de México, 67% de los casos de robo de identidad es por pérdida de documentos. Se mandó a la Comisión de Justicia.

Fuente: http://www5.diputados.gob.mx/index.php/esl/Comunicacion/Agencia-de-Noticias/2016/03-Marzo/10/2266-Presentan-diputados-once-iniciativas-en-la-sesion-de-hoy

Ransomeware Locky, la peor amenaza (Macros Maliciosas)

MARZO 01, 2016 / REALTNET.COM

El Ransomware "Locky" se descarga de un servidor remoto, llega por medio de un correo electrónico que contiene un archivo en Word (.doc), archivo que contiene una macro, si están habilitadas las macros de Office en Word, esta macro descarga el Ransomware que Trend Micro detecta como RANSOM_LOCKY.A. Si no están habilitadas las macros, la víctima verá una instrucción de activar macro por lo que, si el usuario acepta, infectará el sistema descargando el archivo malicioso por la macro y guardándolo en la carpeta Temp para después ejecutarlo.

Una vez instalado busca unidades conectadas y cifra archivos como: documentos, imágenes, música, videos, archivos, bases de datos y archivos relacionados con las aplicaciones web utilizando el algoritmo AES. Ya cifrados serán renombrados con un hash con la extensión "locky", mostrando una nota y una imagen en los directorios donde solicita el pago del rescate de esta información, que son entre .5 y 1 Bitcoin (entre 3,600 – 7,200 pesos)

Como fondo de escritorio aparece un mensaje que contiene ciertas instrucciones que incluyen la instalación del navegador **Tor** para ingresar a la información del pago, esta información la coloca en un archivo de notas para que los enlaces puedan ser copiados, este archivo se genera en todas las carpetas donde se cifraron archivos.

Fuente: http://www.realnet.com.mx/noticias/notas/841-ransomware-locky,-la-peor-amenaza-macros-maliciosas

Apple usará servidores de Google para iCloud

por MARZO 19, 2016 / PC WORLD EN ESPAÑOL

ESET advierte acerca de una nueva estafa que Un informe de Business Insider, reveló que Apple está por firmar un acuerdo con Google para acrecentar la capacidad de iCloud, que será alojado (al menos en parte) en Google Cloud Platform, este acuerdo estaría entre los 400 y 600 millones de dólares y la migración de datos tardaría cerca de un año en concretarse.

Aunque se cree que será de manera temporal, ya que Apple se encuentra trabajando en la mejora de sus Datacenters, ampliando sus infraestructuras en Oregón y desarrollando nuevos centros de datos en Arizona, Reno, Dinamarca e Irlanda.

Por lo tanto, Apple dejaría de manera parcial los servicios de Amazon Web Services y Microsoft Azure que, junto a sus propios centros de datos, venía utilizando hasta la fecha.

Fuente: http://www.cioal.com/2016/03/14/smartphones-producen-60-de-infecciones-en-red-movil/

El cifrado es la "clave" para un futuro más seguro, dijo el CEO

por MARZO 18, 2016 / WE LIVE SUCURITY

El Dr. Andy Yen, cofundador y CEO de ProtonMail dijo que la forma más viable y segura de poder mover todos los datos en línea por medio de un correo electrónico, es manteniendo la información segura a través del cifrado de punta a punta (end-to-end encryption).

Al preguntársele sobre cuál es la posición de ProtonMail respecto al debate de lo que está pasando con Apple y el FBI, argumentó que el código de ProtonMail es de fuente abierta, por lo que pasa con ellos no es realmente posible con la empresa ProtonMail. Su postura es nunca aceptar que se introduzca un backdoor.

Así que para asegurar que los derechos al cifrado y la privacidad no sean invadidos, será dejando las herramientas en manos del público, así que la última palabra del cliente y no del gobierno.

ProtonMail, acaba de anunciar que ha abierto su servicio al registro público, ya no estará en versión beta, lanzándose de manera gratuita en iOS y Android.

Fuente: http://www.welivesecurity.com/la-es/2016/03/18/cifrado-futuro-mas-seguro-protonmail/

SERVICIOS FINANCIEROS

CONDUSEF detecta 150 casos de robo de identidad en tres semanas

por MARZO 11, 2016 / NOTIMEX

En una entrevista con el presidente de la Comisión Nacional para la Defensa de los Usuarios de Servicios Financieros (Condusef), informó que se detectaron 150 casos de robo de identidad por lo que se realizaron alrededor de 279 acciones, sobre todo por la alteración de la credencial para votar. Habrá un convenio con el Instituto Nacional Electoral (INE), para hacer un inventario de las credenciales falsas que se detectaron para que el organismo electoral levante su denuncia en la Fiscalía Especializada para la Atención de Delitos Electorales (Fepade).

Se descubrió el sitio de Internet Consulta tu buró de crédito, un formato similar al del Buró, en donde por medio de un chat se informaba a los usuarios que tenían una deuda y que ya estaba en proceso judicial, pero que si pagabas una cantidad se detenía el proceso.

Fuente:
http://www.notimex.gob.mx/acciones/verNota.php?clv=423903

NEGOCIO

El poder de la privacidad digital para las empresas

por MARZO 17, 2016 / FORBES MÉXICO

La privacidad y su importancia se remonta a inicios de la humanidad y ha adquirido mayor importancia conforme va evolucionando la tecnología. Al hablar de seguridad, se hace pensando en cuidar los dispositivos como laptops, pc's u otros de un ataque externo.

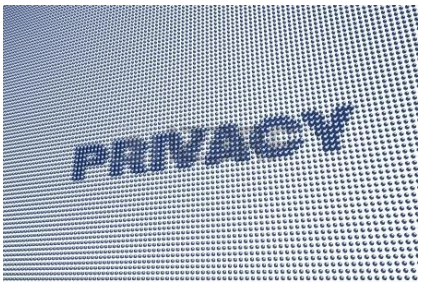
En cambio, la privacidad va ligada con tratar de proteger los datos valiosos, personales, información de empleados e información crítica, según Javier Agüera, de Silent Circle.

Se puede tener un excelente sistema de seguridad en la empresa, pero si los empleados entran a alguna red social y hacen check in, ya se está rompiendo la privacidad, por eso se debe educar al personal de la empresa en materia de privacidad y seguridad en el mundo digital.

El año pasado se perdieron cerca de 500 billones de dólares por cuestiones de privacidad, y este se ha vuelvo en un tema crítico. Una situación como esta genera un gran impacto en la imagen y credibilidad de la empresa además de causar un daño financiero en su cartera de clientes.

Los temas en materia de seguridad y privacidad a nivel corporativo se han actualizado, por lo que los responsables de las empresas deben empezar a tomar cartas en el asunto y entender que cuando se habla de cuestiones de seguridad y privacidad corporativa, se debe comprender desde la infraestructura y la red dentro de la empresa hasta los endpoints, como los dispositivos móviles que portan los empleados.

Fuente: http://www.forbes.com.mx/brand-voice/poder-la-privacidad-digital-las-empresas/



GOBIERNO

Alerta fraudes en trámites de actas de nacimiento en línea

por MARZO 17, 2016 / DIARIO DE MÉXICO

La Secretaría de Seguridad Pública de la Ciudad de México (SSP-CDMX), dio aviso sobre los fraudes sobre la venta de actas de nacimiento en línea. Los defraudadores crean sitios oficiales falsos en internet, en el cuál se gestionan trámites de actas de nacimiento a nivel nacional.

En algunas páginas falsas, se solicitan datos personales al comprador por medio de conversaciones en línea o llamadas telefónicas haciéndose pasar como "asesores". Por los que se sugiere no brindar información personal, de tarjetas bancarias o datos que puedan ser utilizados para realizar transacciones financieras.

Para estos trámites se encuentran los kioscos de la Tesorería de la Secretaría de Finanzas de la Ciudad de México, se encuentran en diversos centros y plazas comerciales, sin peligro de sufrir fraudes.

Fuente: http://www.diariodemexico.com.mx/alertan-fraudes-tramites-actas-nacimiento-en-linea/

REDES SOCIALES

Anonymous cumple su amenaza y revela información personal de Donald Trump

por MARZO 14, 2016 / UNO CERO

El grupo de hackers Anonymous, publicó en Pastebin, información personal de Trump, como el número de varios de sus domicilios, su número de seguro social, su certificado de nacimiento y sus números de teléfono.

Así mismo, información sobre la infraestructura web del magnate animando a los hackers a tomar medidas el 1 de abril.

Por medio de un video, Anonymous anunció su ataque el pasado jueves en YouTube, acusándolo de fascismo y xenofobia, así mismo de la persecución religiosa de los musulmanes a través de políticas totalitarias.

El año pasado, Trump alegó haber recibido amenazas por lo que pidió la protección del Servicio Secreto, la cuál es solo para altos funcionarios de gobierno y líderes de otras partes que visitan el país.

Fuente: https://www.unocero.com/2016/03/19/anonymous-cumple-su-amenaza-y-revela-informacion-personal-de-donald-trump/

Hackers desarrollan un Malware con la campaña Secuestro URL".om"

MARZO 17, 2016 / NOTICIAS SEGURIDAD

Un grupo de hackers ha desarrollado un tipo de campaña de Secuestro URL ".om", que lleva por nombre Typosquatting, enfocado a personas que suelen cometer errores al momento de copiar el dominio de sus páginas favoritas y por medio de un malware se apoderan de los equipos MAC o Windows.

Typosquatting permite a los atacantes llevar a cabo el Secuestro URL, esta violación se produce cuando el atacante compra el nombre de un dominio con nombres similares a los sitios más usados de Internet, con el fin de obtener más tráfico o insertando un virus en los equipos de los usuarios.

Los ciberdelincuentes se centran principalmente en el sufijo .com.

De este modo, si la víctima copia, por ejemplo, "Amazon.om" o incluso "Amazonc.om," va a ser redirigido a un sitio que sirve de malware malicioso para aquellos que no son lo suficientemente expertos como para reconocerlo.

Fuente: http://noticiasseguridad.com/malware-virus/hackers-desarrollan-un-malware-con-la-campana-secuestro-url-om/

TOTALSEC NEWSLETTER - INFOSEC

BOLETÍN No.5

19 – 27 MARZO, 2016

Elaboración: MARZO 28, 2016.