NEWSLETTER – INFOSEC MX

BOLETIN No. 16

JUNIO 04 - 12

Elaboración: Junio 13, 2016

EMPRESAS

En este número encontrarás noticias sobre:
- Empresas
- Finanzas
- Tecnología

La mayoría de las empresas fallará frente al riesgo digital

por JUNIO 06 2016 / SILICON

Según la consultora Gartner, 6 de cada 10 equipos de seguridad TI que están presentes en los negocios digitales, serán incapaces de gestionar el riesgo en 2020, derivando fallos importantes de sus servicios, aún y cuando el presupuesto para Seguridad de la Información, detección y respuesta rápida se haya duplicado.

Paul Proctor, vicepresidente de Gartner, dijo que las empresas aprenderán a vivir con niveles aceptables de riesgo, y las unidades de negocio innovan para descubrir qué Seguridad necesitan y qué se pueden permitir. Así mismo considera que perfeccionar el liderazgo será más importante que desarrollar nuevas herramientas y generar nuevas habilidades tecnológicas.

Fuente: http://www.silicon.es/la-mayoria-las-empresas-fallara-frente-al-riesgo-digital-2310332?utm_content=buffera5ce1&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

FINANZAS

Diversificación de pagos atrae a ciberdelincuentes

por JUNIO 05, 2016 / EL ECONOMISTA

Marcelo Hernández, Director General de AIG Seguros México, dijo que se debe estar consciente de que la diversificación de medios de pago, el creciente uso de dispositivos personales en los centros de trabajo y la actualización de los cibercriminales, son factores que pueden hacer de las compras en Internet un calvario. El estudio "Predicciones de Seguridad para 2016 y próximos años", elaborado por Trend Micro, pronostica amenazas diseñadas para robar información de tecnologías de procesamiento de pago desde tarjetas bancarias poniendo en riesgo el patrimonio personal y empresarial.

Los empleados de cualquier organización que hacen compras desde sus dispositivos personales y están conectados a la red de la empresa, ponen aún más en riesgo a la organización, por lo que es recomendable contratar un seguro que cubra pérdidas financieras por riesgo de datos personales y corporativos, responsabilidad por empresas subcontratadas y por Seguridad de los datos en su poder.

Fuente: http://eleconomista.com.mx/finanzas-personales/2016/06/05/diversificacion-pagos-atrae-ciberdelincuentes?utm_content=buffer12643&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

El monedero BitGo, sufre ataque DDoS prolongado que hace que la industria se tambalee

por JUNIO 07, 2016 / REDES ZONE

BitGo, considerada la plataforma más segura, rápida, y eficiente. Desde hace unos días se encuentra enfrascada en un ataque que ya ha repercutido en otros servicios. Expertos del sector no saben explicar qué ocurre y de quién es el interés por llevar a cabo el cierre de los servicios vinculados a las criptomonedas. El ataque de denegación de servicio también ha afectado a otros servicios que hacen uso de su API como Wirex, Bitstamp, Bitfinex, Unocoin y Kraken, teniendo una gran cantidad de horas fuera de servicio.

Gatecoin, Shapeshift, CoinWallet, BitQuick, Cryptsy y LoanBase, son servicios que en los seis últimos meses han tenido que cerrar por ataques recurrentes o por un fallo de Seguridad, en muchos casos dejó vacías las cuentas de los usuarios y no se disponía de capital para reponer el dinero robado.

Fuente: http://www.redeszone.net/2016/06/07/monedero-bitgo-sufre-ataque-ddos-prolongado-hace-la-industria-se-tambalee/?utm_content=buffer4dabb&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

TECNOLOGÍA

Solarin, uno de los celulares Android más caros y seguros del mundo

por JUNIO 08, 2016 / EL UNIVERSAL

Sirin Labs, StartUp de Israel, lanzó al mercado el modelo Solarin, que cuenta con materiales de lujo, y también un sistema de Seguridad que "es a prueba de espías". Tiene sistema operativo Android, y fue diseñado para que nadie tenga acceso al mismo.

Con una pestaña en la parte posterior que al tocarla enciende un "modo seguro", apaga los sensores que no puedan ser de utilidad, cifra llamadas y mensajes de texto utilizando software AES de 256 bits. Tiene un servicio de Seguridad que monitoriza el equipo y se pone en estado de alerta en caso de un ataque al usuario, tiene una pantalla LCD de 5.5 pulgadas con resolución Quad HD, 4GB de memoria RAM y 120GB de almacenamiento interno, una cámara con sensor de Sony de 23,8 megapixeles y una batería de 4 mil 40 mAh, con un procesador Snapdragon 810. Su precio puede llegar hasta los 14 mil dólares (257 mil 930 pesos), está a la venta en la página web del fabricante.

Fuente:
http://eluniversal.com.mx/articulo/techbit/2016/06/8/solarin-uno-de-los-celulares-android-mas-caros-y-seguros-del-mundo

Se deben prevenir ciberataques

por JUNIO 02, 2016 / NORTE DIGITAL

Jorge Miranda, experto en Seguridad, durante su participación en el Cybersecurity Summit 2016 que organiza Fortinet, comentó que, ante el aumento de ataques cibernéticos, las empresas tienen dos opciones: prevenir o corregir los errores luego de un ataque. Agregó que México pasó del séptimo al quinto lugar en ciberataques a nivel mundial, por encima de China.

Entre el primer trimestre de 2015 y el mismo periodo de 2016, el número de ataques con malware tuvo un crecimiento de 1351%, incrementándose también el ataque mediante dispositivos móviles. Por lo que el conferencista agregó que las compañías deben destinar más presupuesto para la Seguridad, ya que muchas veces este gasto queda en segundo plano. Además de afectar a la empresa, los ciberataques exponen a todos los clientes, proveedores y empleados que estén en la información que fue robada.

Fuente: http://nortedigital.mx/se-deben-prevenir-ciberataques/

Estafadores aprovechan incidentes recientes para extorsionar víctimas

por JUNIO 02, 2016 / WE LIVE SECURITY

El Internet Crime Complaint Center (IC3), emitió un anuncio advirtiendo a las personas sobre ciberdelincuentes que tratan de aprovechar la actual oleada de brechas de datos que acaba de salir a la luz como Myspace, Tumblr y LinkedIn, comprometiendo a cientos de millones de usuarios, son filtraciones de credenciales que se originaron en brechas de hace varios años.

Ha aumentado la actividad de scammers en relación a esto. Quienes reciben correos electrónicos de estos ciberdelincuentes son avisados de que, si no pagan un rescate, sus datos personales serán filtrados y exigen un monto que oscila entre 2 y 5 bitcoins (entre 21 mil 200 pesos y 53 mil 100 pesos aproximadamente).

Fuente: http://www.welivesecurity.com/la-es/2016/06/02/estafadores-aprovechan-extorsionar-victimas/?utm_content=buffer11ee9&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

575,000 millones, roba ciberdelincuencia al año

por MAYO 27, 2016 / CIOAL

Según Bank of America y Merrill Lynch, las indemnizaciones de los seguros contra ataques cibernéticos han llegado hasta los 15 millones de dólares, cada vez sale más caro asegurar los activos digitales, ayudando a que crezca más el precio global de las fugas de datos. A nivel mundial en el primer semestre de 2015, aumentó un 32% el valor medio de las primas para comerciantes, en el sector salud algunas de ellas se triplicaron.

Reuters asegura que los deducibles tienden a ser más altos, y las aseguradoras no dan pólizas de más de 100 millones de dólares a clientes en situación de riesgo. El año pasado aumentaron los indicadores de fugas de datos; se rompieron records en la cantidad de ataques, identidades robadas y "megafugas". Aseguradoras, organismos gubernamentales y las entidades sanitarias son objetivo de los delincuentes, que están buscando obtener perfiles personales más completos.

Fuente: http://www.cioal.com/2016/05/27/575-000-millones-roba-ciberdelincuencia-al-ano/

Malware Irongate afecta sistemas de control industrial

por JUNIO 03, 2016 / SEGURIDAD UNAM

La empresa FireEye, dijo que el malware Irongate, que comparte algunos de los atributos de Stuxnet, no representa de momento una amenaza, ya que fue diseñado para ejecutarse dentro de entornos Siemens simulados y ha pasado desapercibido durante años en la base de datos de VirusTotal de Google.

Algunos de sus atributos son su capacidad para perpetrar un ataque man-in-the-middle contra el proceso de entrada y salida, el ataque al software operador del proceso en simulaciones industriales. Además, puede dar a los atacantes la capacidad de alterar los controles industriales con el desconocimiento del operador del sistema. Estas técnicas se han utilizado con anterioridad para sabotear desde las redes de energía hasta los controladores lógicos en centrifugadoras nucleares.

Fuente:
http://www.seguridad.unam.mx/noticia/?noti=2897&utm_content=bufferf0bde&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

Investigadores de Data61, buscan alternativas a las contraseñas

por JUNIO 01, 2016 / SEGURIDAD UNAM

Explicaron cómo han estado probando el método patentado y llamado "la biometría del comportamiento". Proceso que pide al usuario darse de alta escogiendo dos o tres imágenes opcionales. En el inicio de sesión, recordar cuáles imágenes escogió, sumar los números del fondo de las imágenes y escribir a mano el resultado. Este sistema, usa las capacidades de una pregunta secreta (recordando una imagen), comportamiento biométrico y cognición biométrica para crear algo que espera sea más fuerte que la suma de estas partes.

Esto toma ventaja de la pantalla táctil habilitada para identificar a los usuarios por la dirección de sus golpes, la presión que estos aplican a la pantalla, aceleración y el movimiento de sus dedos, la frecuencia de pulsaciones en la pantalla, el área del dispositivo cubierto por las pulsaciones, etc.

Fuente:
http://www.seguridad.unam.mx/noticia/?noti=2893&utm_content=buffer1f88c&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

El ransomware Cerber muta cada 15 segundos para evitar las herramientas de Seguridad

por JUNIO 03, 2016 / REDES ZONE

El ransomware Cerber, es capaz de mutar su código cada 15 segundos y así evita que los softwares antivirus instalados en el equipo puedan detectar la amenaza. Se ha mostrado muy activa y se está distribuyendo por medio de correos electrónicos, lo interesante es su código, que es capaz de mutar cada 15 segundos para evitar que las herramientas de Seguridad del equipo puedan detectar su actividad.

Esto es algo frecuente desde hace varios meses, esta técnica la usan los ciberdelincuentes para complicar el trabajo del software antivirus, y en muchos casos es imposible de detectar la amenaza, o no se consigue antes de que ya se haya producido el daño, en este caso el cifrado de los archivos almacenados en el equipo. Su desventaja es la necesidad de una conexión a Internet para que dé este proceso, por lo que, si se detecta que el equipo está infectado, sólo basta desconectar el equipo para que el ransomware no pueda mutar a una nueva versión que se genera en el servidor remoto.

Fuente: http://www.redeszone.net/2016/06/07/ransomware-cerber-muta-15-segundos-evitar-las-herramientas-seguridad/

México es incierto en Seguridad cibernética

por JUNIO 03, 2016 / REDES ZONE

La ciberseguridad ha cobrado gran importancia en nuestros días, pero muchos le dan todavía poco valor en México. Miriam Padilla Espinoza, profesional certificado en protección de datos personales, comentó que el país avanza mucho en el uso de tecnología, pero está quedando atrás en el tema de protección. Es necesario hacer conscientes a quienes toman decisiones a nivel empresarial, a legisladores y a los alumnos en las escuelas sobre los riesgos que existen y que pueden atentar contra la Seguridad incluso a nivel nacional.

En México, 54.9 millones han sido víctimas de algún ciberdelito, de estos el 58% sufrieron suplantación y robo de identidad, 17% fraude y el 15% sufrieron algún hackeo, convirtiendo a México en el tercer lugar mundial en crímenes cibernéticos, después de China y Sudáfrica.

Fuente: http://www.mipatente.com/mexico-es-incierto-en-seguridad-cibernetica-experta/

Policías capitalinos se capacitan para combatir ciberdelincuencia

por JUNIO 05, 2016 / EXCELSIOR

Elementos de la Secretaría de Seguridad Pública capitalina, adscritos a la Subsecretaría de Información e Inteligencia Policial, asistieron al seminario Enfuse Conference 2016 en Estados Unidos, e intercambiaron información especializada en Forencia Digital. Patrick Denis, CEO de Guidance Software, compartió conocimientos en materia de uso y manejo de software para el análisis forense y la adquisición de información almacenada en memoria RAM.

Además, participaron junto a especialistas de más de 100 países, en un evento que tuvo una asistencia de más de mil 500 personas, en 125 sesiones de trabajo. Además, hubo ponencias sobre recopilación de información pública e ingeniería social; malware móvil para fraude financiero; mitigación de riesgos internos en organizaciones; cibercontrainteligencia y gobernanza de la Información, entre otros.

Fuente: http://www.excelsior.com.mx/comunidad/2016/06/05/1096984

TOTALSEC NEWSLETTER – INFOSEC

BOLETÍN No. 16

JUNIO 04 – 12, 2016

Elaboración: JUNIO 13, 2016

totalsec
Security Operation Center