2013-05-15

Boletín de Noticias de Seguridad Informática

SC Progress

http://www.scprogress.com

ÍNDICE

NOTICIA 1: Estudio de INTEL: Cada minuto se roban 20 identidades en Internet

En la actualidad las cuentas de facebook están siendo hackeadas recibiendo una invitación con otra cuenta de facebook, tal cual como la propia cuenta personal. Es por ello que a continuación les contaremos de un caso con la Estratega Digital de una empresa de seguros Irma Toro que ha estado en facebook desde el año 2006. Hace un par de semanas, sus amigos en esta red social le reportaron que estaban recibiendo una invitación con su foto, aunque tenía un nombre distinto. Ella les pidió que denunciaran en la propia red el perfil falso y fue dado de baja.

Sin embargo, fue una alerta para aumentar los niveles de privacidad aunque se queja de las pobres opciones de redes como Facebook, que además permite la interconexión automática con otros servicios, como Instagram, Twitter que a fin de cuenta allí está toda tu vida.

"La violación de la privacidad y la suplantación de la identidad están en ascenso por la cantidad de transacciones en la red mundial de información y la exposición de información en redes sociales".

Según un estudio de Intel, en un minuto 20 personas son víctimas del robo de identidad en la red y se disparan 135 virus letales para su computadora.

Hay quienes cogen cierta información de su biografía de facebook. Con ello pueden adivinar gustos, afinidades, parentescos y llegar hasta la clave del correo, que, en la mayoría de los casos, es la contraseña de todos los servicios.

La debilidad de las contraseñas es tan solo una de las maneras de robar la identidad, una de las cyberplagas de la era de internet que lleva a defraudaciones millonarias y violación de la privacidad.

El abogado Andrés Guzmán Caballero hizo una encuesta entre cien clientes empresariales y encontró que 45 por ciento de las personas han experimentado la intrusión en redes sociales y la suplantación de su identidad. "Los motivos van desde envidia, fanatismo, diferencias personales, intereses propios con fines delictivos, o simple curiosidad", argumenta.

Para ello es recomendable guardar pruebas porque a medida que crece el robo de identidad, también aumenta la cultura por recoger evidencia con el fin de rastrear a los atacantes y recuperar la identidad.

Hay que salvaguardar las pruebas que para esto es preciso acudir a un ingeniero especializado en informática forense, con el fin de guardar la página o perfil falso. La idea es que no se baje de la red y se pierda la evidencia.

Lo que sigue es iniciar acciones directas en cada red social. "Ellos tienen fáciles sistemas de denuncia, pero un poco lentos".

Fuente: www.seguinfo.com

Noticia 2: Los retos de seguridad para las Pymes

"Las Pymes ubican candado al negocio después de que se metieron los ladrones".

Las empresas no invierten en seguridad sino que reaccionan a un ataque, es decir

La tendencia de atacar a las Pymes empezó con un incremento de amenazas sofisticadas en 2012, está dirigida a vulnerar las bases de datos y los sistemas productivos de gestión empresarial.

La ingeniería social será más prominente: Esta consiste en extraer información del sistema por medio de las redes sociales y el correo electrónico, por ejemplo. Los ataques de phising son una forma de ingeniería social muy popular por estos días.

Avira asegura que las amenazas internas tendrán que ser contrarrestadas ya que cada día son más frecuentes los casos donde el robo de la información se da desde el interior de las pymes explicó la compañía de seguridad.

La tecnología tiene que proponer soluciones para que los mismos empleados no puedan extraer información confidencial de la empresa.

Cabe recalcar que con el ingreso de diferentes sistemas operativos y miles de aplicaciones cada día es más complicado mantener altos niveles de seguridad.

La situación de las Pymes es complicada.

Obviamente tienen recursos limitados y la seguridad en TI no está entre las prioridades. Sin embargo, las empresas deberían entender que la realidad es diferente. Los piratas informáticos son lo suficientemente inteligentes para saber dónde hay menos resistencia, y por ahí atacan.

El Phishing es un delito informático en el que se pretende recabar datos confidenciales, como contraseñas e información bancaria, de forma fraudulenta.

Fuente: www.enter.com

Noticia 3: **Avira revela que las pymes españolas son el colectivo más vulnerable ante las amenazas de seguridad.**

Un nuevo estudio de Avira revela, que las pymes son el perfil más vulnerable ante las amenazas de seguridad por diversos motivos.

Entre los motivos que predominan: El desconocimiento de las bases fundamentales en seguridad informática, la ausencia de un departamento de IT y la baja inversión en esta estructura de seguridad. Un 43% de los encuestados lo cree así.

Destaca también como foco de riesgo de las pymes, el uso personal que algunos trabajadores puedan hacer de los equipos informáticos y que acaban siendo una entrada de virus o un foco de fuga de información.

El estudio sitúa al consumidor final como el segundo gran grupo vulnerable, con un 26,4%.

Con un 14,7% le siguen los autónomos, las grandes empresas o corporaciones, con un 11,7% y los organismos oficiales o instituciones, con apenas un 4,4%.

La falta de inversión y el desconocimiento son una combinación peligrosa para las Pymes españolas, cuyos riesgos se traducen, según apunta en este estudio la red de ventas de Avira en España, en robo de datos por parte de empleados, malware y contagios vía memorias USB.

Avira, con un 92% de su base de clientes finales mundiales procedentes de empresas pequeñas y micro, estima que el mercado de la seguridad en este colectivo aumentará en España entre un 4% y 5% este año. La compañía destaca que los productos más solicitados por las pymes en España son los relacionados con la protección al PC y al servidor.

Fuente: www.muyinformacion.com