2013-07-05

CiberNoticias

SCProgress

www.scprogress.com

ÍNDICE

Noticia # 1: ¿Cuánto cuesta a una empresa un incidente grave de seguridad?

Alrededor de 500.000 euros es el coste medio en el que incurren las grandes empresas como consecuencia de un ciberataque, según datos de la Encuesta Global sobre seguridad TI corporativa 2013 , llevada a cabo por B2B Internacional junto a Kaspersky Lab y basado en 2.895 encuestas con profesionales de IT.

Cualquier ciberataque puede causar daños a las empresa, pero ¿cómo se pueden cuantificar esos daños en términos financieros?

Los expertos de B2B Internacional han calculado los daños derivados de los ciberataques incluyendo sólo los incidentes ocurridos en los últimos 12 meses y evaluando la información de las pérdidas sufridas como resultado directo de los incidentes de seguridad.

El dato incluye dos componentes principales:

- Daños causados por el incidente en sí es decir, pérdidas derivadas de la fuga de datos críticos, continuidad de negocio y los costes asociados con la participación de especialistas para solventar el incidente. Suponen la mayor parte de las pérdidas, alrededor de 431.000 euros.
- Costos no planificados, originados para prevenir futuros ataques similares, incluyendo el personal de contratación/formación, el hardware, el software y otros cambios de infraestructura. Suponen unos 69.000 euros.

Los daños varían dependiendo de la región geográfica en la que opera la empresa en cuestión. Por ejemplo, los daños mayores se asocian con incidentes sufridos en empresas que operan en América del Norte, con un promedio de 624.000 euros, seguido de América del Sur, con 620.000 euros. Europa Occidental registró una media más baja, pero aún considerable, de las pérdidas derivadas de ciberataques, llegando a 478.000 euros.

Los costes de un ciberataque contra las pequeñas y medianas empresas son más bajos que en las grandes corporaciones. La pérdida media resultante de los incidentes de seguridad TI en las empresas de tamaño medio es de aproximadamente 38.000 euros. Alrededor de 28.000 euros derivados del incidente en sí, mientras que los restantes 10.000 provienen de otros gastos asociados.

Fuente: Segu-info.com

Noticia # 2: Alertan sobre nueva vulnerabilidad de Android.

Permite que un hacker pueda convertir cualquier aplicación en un troyano malicioso

La empresa Bluebox Security advirtió hoy y puso al descubierto una nueva vulnerabilidad para el sistema móvil Android, la cual permite que un hacker pueda convertir cualquier aplicación en un troyano malicioso.

El director de tecnología de la firma en seguridad móvil, Jeff Forristal, aseguro que lo anterior es totalmente desapercibido tanto por la tienda de aplicaciones, el teléfono, o el usuario final, y que las implicaciones que ello tiene son "enormes".

Agregó que dicha vulnerabilidad, por lo menos desde el lanzamiento de Android 1.6, podría afectar a cualquier teléfono Android lanzado en los últimos cuatro años, lo que equivale a casi 900 millones de dispositivos.

Asimismo, expuso que un hacker puede explotar la vulnerabilidad de cualquier cosa, desde el robo de datos, hasta la creación de una red de bots móviles. Pero el riesgo para el individuo y la empresa es grande, pues una aplicación maliciosa puede acceder a los datos individuales o entrar al sistema de la compañía, riesgo que se agrava si se tienen en cuenta las aplicaciones desarrolladas por los fabricantes de dispositivos o de terceros que trabajan en cooperación con el fabricante del dispositivo y que se otorgan privilegios elevados especiales dentro de Android, puntualizó.

La debilidad permite que se pueda modificar el código del paquete APK sin romper la firma cifrada de la aplicación, lo que en apariencia parecería una aplicación legítima.

La aplicación entonces no sólo tiene la capacidad de leer los datos de aplicaciones arbitrarias en el dispositivo como correo electrónico, mensajes de texto y documentos, entre otros, recupera todas las cuentas y contraseñas almacenadas.

También puede tomar básicamente en el funcionamiento normal del teléfono y controlar cualquier función del mismo, desde hacer llamadas telefónicas enviar mensajes SMS, encender la cámara y grabar las llamadas.

Por ello, Bluebox recomienda a los propietarios de dispositivos ser muy prudentes en la identificación del editor de la aplicación que desea descargar y actualizar constantemente los equipos móviles.

Fuente: informador.com.mx

Noticia # 3: Twitter refuerza seguridad tras ataques a cuentas de grandes medios.

El sistema enviará al móvil del usuario un código de verificación para ingresar a Twitter.

Twitter anunció nuevas medidas de seguridad opcionales, que permitirán a sus suscriptores instaurar un sistema de doble control antes de conectarse, después de algunos ataques de delincuentes informáticos a las cuentas de grandes medios de comunicación.

La red social afirmó que lanzará un nuevo sistema de control de identidad. "Una segunda comprobación para asegurarse de que realmente sea el usuario el que está ingresando. Cuando una persona abre su cuenta este sistema de autentificación en dos niveles será opcional", explicó Twitter.

"Usted necesitará una dirección de correo electrónico confirmada y un número de teléfono verificado. Luego de comprobar rápidamente que su teléfono puede recibir mensajes de Twitter, ya está", dijo Jim O'Leary, de la división de Seguridad del Producto de Twitter.

El nuevo sistema de seguridad enviará un mensaje al teléfono del abonado con un código de verificación que éste deberá ingresar para conectarse a Twitter, además de la contraseña tradicional.

"Por supuesto, incluso con esta nueva opción de seguridad habilitada, sigue siendo importante utilizar una contraseña fuerte y seguir los consejos de seguridad de la cuenta", aclaró O'Leary.

"El proceso de verificación parece positivo, pero"todo depende de cómo lo implemente Twitter", estimó por su parte James Gabberty, profesor de Informática de la Pace University de Nueva York.

Fuente: El tiempo.com