Noticia: Los fallos de seguridad informática se incrementan un 36% en el primer semestre de 2010

Madrid, 7 de septiembre de 2010:

En el primer semestre de 2010 se han incrementado muy significativamente las vulnerabilidades en la seguridad de las aplicaciones (36%), al tiempo que ha aumentado la complejidad de los ataques encubiertos en ficheros pdf y código JavaScript. Asimismo, se han reducido en un 82% los ataques de phising que buscan robar datos privados de los usuarios a través de correos fraudulentos. Estas son algunas de las conclusiones del último informe sobre seguridad -IBM X-Force ® 20010 Mid-Year Trend and Risk Report- que también identifica la seguridad en entornos virtualizados y cloud computing como dos aspectos relevantes a abordar en los próximos meses.

Primer semestre

La detección de las vulnerabilidades -defectos en la programación o el diseño de las aplicaciones de software que hacen que estos programas estén expuestos a incidencias de seguridad- se está incrementando muy significativamente en 2010. De hecho, en el primer semestre se descubrieron 4.396 vulnerabilidades nuevas, lo que representa un incremento del 36% respecto al mismo período de 2010. El 55% de estas vulnerabilidades no disponían de un parche de seguridad al final del semestre. Si analizamos el tipo de vulnerabilidades detectadas, el informe indica que el 55% de ellas estaban relacionadas con aplicaciones Web.

Puesto que las organizaciones son cada vez más eficaces a la hora de combatir los ataques que tienen lugar en sus redes, los atacantes están utilizando cada vez más técnicas encubiertas para introducirse en las redes sin ser detectados. En el primer semestre se ha incrementado la frecuencia y complejidad de los ataques encubiertos en un 52%, especialmente aquellos introducidos en código JavaScript. El estudio desvela también que, en este período, también proliferaron los ficheros en formato pdf infectados, especialmente en abril, con un incremento del 37%.

Phising

En los primeros 6 meses de 2010, las emisiones de phising cayeron un 82%. Las instituciones financieras siguen siendo el principal objetivo de este tipo de ataques (el 49%), seguidas por las empresas emisoras de tarjetas de crédito (27%), las organizaciones públicas, así como las instituciones de pagos on line y subastas. España continúa figurando en la lista de los 10 primeros países (puesto número 8) dónde están ubicados los servidores que alojan las direcciones Web contenidas en estos correos fraudulentos. Esto indica que un 3,2% de los ataques remiten a servidores ubicados en nuestro país, aunque dichos envíos sean generados en otros países. De hecho, Brasil es el primer país en emisión de phising.

Cloud computing y virtualización

Las empresas y organizaciones cada vez están más interesadas en los aspectos de seguridad relacionados con cloud computing, un modelo de prestación de servicios que se encuentra en fase de expansión. IBM recomienda a las organizaciones que están planteándose la transición a cloud computing comenzar analizando los aspectos de seguridad relacionados con cada una de las cargas de trabajo que quieren trasladar a estos entornos. Y en función de este primer

análisis tomar las decisiones posteriores de cuál puede ser el tipo de cloud a utilizar, el proveedor, etc.

La seguridad también está cobrando relevancia a medida que las empresas están apostando por la virtualización. El informe indica que el 35% de las vulnerabilidades que impactan a los sistemas virtualizados afectan a la hipervisora (el software que controla todas las máquinas virtuales) lo que pone de manifiesto la necesidad de tener en cuenta también la seguridad a la hora de abordar los proyectos de virtualización.

“Las amenazas a la seguridad no dejan de multiplicarse y evolucionan a un ritmo vertiginoso, por lo que, ahora más que nunca, es importante analizar las diferentes amenazas que puedan existir para ayudar a nuestros clientes a anticiparse a ellas", afirma Steve Robinson, director de las Soluciones de Seguridad de IBM. "Este año, el informe revela que, a pesar de las amenazas van en aumento, la industria en su conjunto se está volviendo mucho más activa a la hora de identificar vulnerabilidades, lo cuál es muy positivo ya que esta colaboración permite identificar y hacer frente antes a las vulnerabilidades”.

El equipo de investigación X-Force trabaja desde 1997 en la investigación, análisis y catalogación de vulnerabilidades. Su objetivo es detectar las amenazas y ponerlas al descubierto. Para ello, IBM recopila información de diferentes fuentes, entre las que figura una base de datos propia con más de 50.000 vulnerabilidades de seguridad catalogadas o los más de 10.000 sensores ubicados en las redes de los clientes de IBM en todo el mundo.

La oferta de soluciones de seguridad de IBM incluye tanto hardware, como software, así como servicios que cubren todos los riesgos de seguridad de negocio y tecnología. El objetivo de IBM es ayudar a sus clientes a innovar desarrollando su negocio en plataformas con un nivel de seguridad muy alto.

Informe completo en www.ibm.com/security/x-force