

Análisis de negocios en la frontera

En los últimos años, la Seguridad Informática es testigo de grandes cambios tecnológicos que permiten establecer un nivel adecuado de protección y prevención para el mantenimiento y

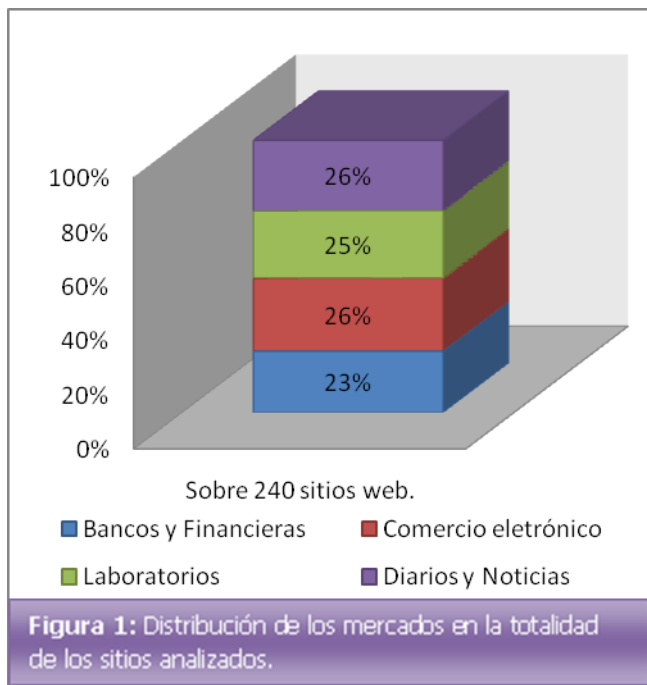


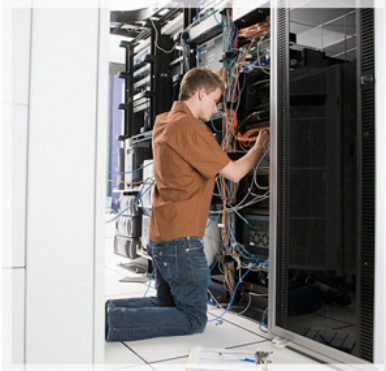
desarrollo del negocio de las empresas. La evolución se observa claramente en el plano normativo cuyos aspectos conceptuales son adoptados por directivos de la seguridad

informática en Argentina, no obstante su implementación tecnológica y operativa sigue siendo lenta, desordenada y hasta en algunos casos impracticable. Aspectos fundamentales y directrices del negocio como los servicios provistos en los portales Web, mantienen un nivel de vulnerabilidad muy superior al mínimo necesario para desarrollar el negocio en forma adecuada y confiable en un mercado exigente en esta era de la información digital.

Por otra parte, mientras compañías y gobiernos se enfrentan por intereses de algunos pequeños grupos privados producto de la fuerte contracción financiera sufrida por los mercados desde fines del 2008, la llamada “crisis económica” influye negativamente en las empresas en temas de tecnología y servicios profesionales de TI, ampliando aún más la brecha entre los niveles establecidos por el marco normativo y las soluciones técnicas de seguridad aplicadas.

En este contexto, la “Seguridad Informática” como parte de las denominadas Nuevas Tecnologías sufrió el embate de un mercado exigido por normas que no pueden ser implementadas en su totalidad y en la forma debida, donde la crisis sigue sosteniendo –y agravando- una situación de Status Quo que en la mayoría de los casos no permite la implementación tecnológica de mejoras, exige mayores controles operativos -con mayores explicaciones- y hasta con menos gente.



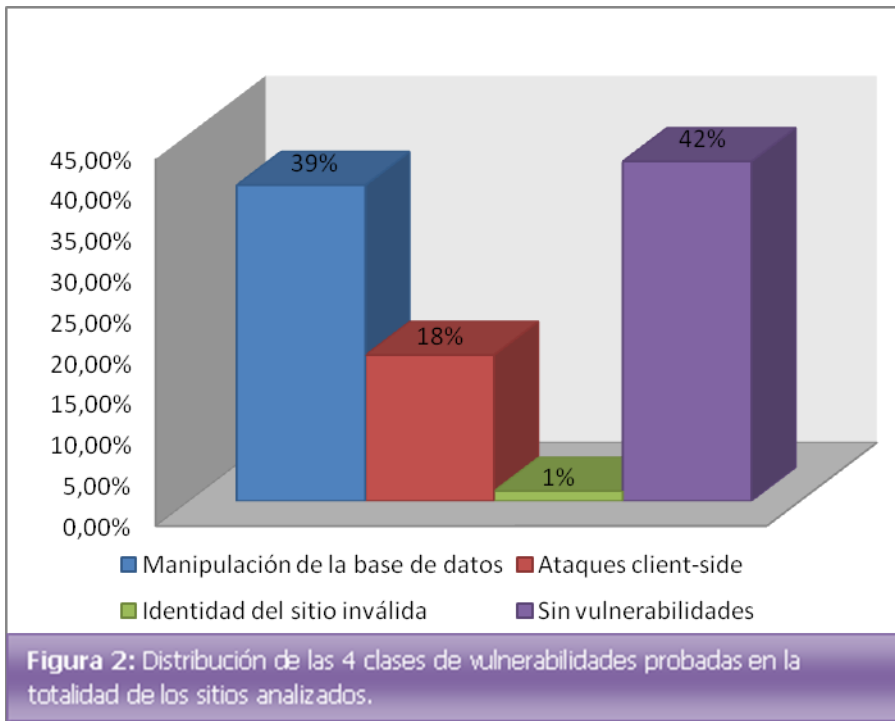


Esta situación de presión constante demuestra resultados muy adversos. Lejos de considerarlo tan sólo un juicio de valor, hemos tomado una muestra (figura 1) de doscientos cuarenta (240) sitios WEB, donde incluimos empresas líderes de los cuatro (4) mercados que, en nuestra opinión, son -por distintas razones- los mejor posicionados en el mercado.¹

Sobre la totalidad de los sitios hemos desarrollado durante aproximadamente sesenta (60) minutos por cada uno de ellos, pruebas clasificadas en las cuatro (4) principales técnicas de

ataque (figura 2), las que fueron realizadas en forma controlada para evitar el normal funcionamiento de las compañías². La manipulación de la base de datos, implica fallas del tipo SQL Injection en todas sus variantes, los ataques de Cross Site Scripting, es decir el medio para lograr ataques efectivos de Client-Side, por ejemplo lograr contraseñas de usuarios aplicando la técnica de Phishing; y pensando en una combinación de ataques, evaluamos la falta de importancia que se da a los certificados digitales de los sitios, donde, o no son firmados por entidades certificadoras conocidas o son autofirmados.³

Las conclusiones de éste artículo debe darnos una herramienta más de debate y análisis sobre el resultado arrojado en las pruebas, errónea y generalmente justificado por la "crisis económica" y en otros casos a sapiencias de haber heredado un mercado de TI



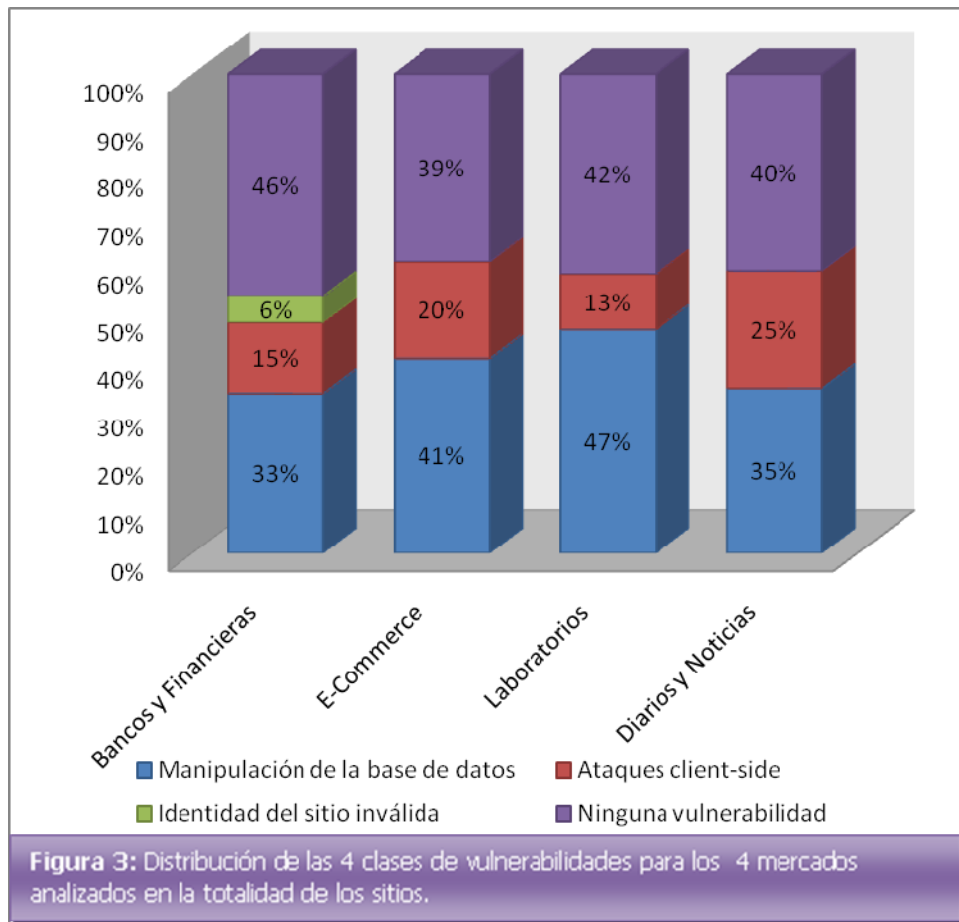
¹ El negocio de los laboratorios a diferencia de los otros, tiene una menor exposición y dependencia en portales de Internet, lo cual permitirá contrastar los resultados obtenidos.

² Todas nuestras pruebas fueron no intrusivas; y solo el resultado de un hipotético ataque es el que puede causar perjuicios.

³ Los certificados digitales son el medio digital por el cual un tercero confiable garantiza la veracidad de un sitio web y/o su contenido. (http://es.wikipedia.org/wiki/Certificado_digital)

desgastado por sí mismo.

Los resultados están a la vista (figura 3) y sin importar el negocio o la conclusión elegida, se muestran fundamentos suficientes para acreditar los niveles actuales de riesgos, manipulación y abuso al que está expuesto el mercado argentino en términos de información y negocios. Entendemos, por ello, que los modelos de seguridad sobre estas nuevas fronteras de negocio deben evolucionar al ritmo de la tecnología y las exigencias, sosteniendo “en las buenas y en las malas” y a pesar de cualquier variación exógena, los máximos niveles de servicios para los clientes, puesto que es ésta la única manera de garantizar la estabilidad y evolución del sistema.



Análisis desarrollado durante los meses de Julio y Agosto de 2009
SHELLCODE © Todos los derechos reservados.