Crece la demanda de Seguridad Informática

Según los datos de Etek en la Argentina, el año pasado comenzó a crecer fuertemente la demanda de sistemas de seguridad informática por parte de las empresas, luego de la crisis de 2001 que "planchó" prácticamente el mercado.

En 2004 su unidad de negocios dedicada a dar servicios de seguridad informática registró un aumento de ingresos del 98% en comparación con el mismo período del año anterior. Asimismo, la base instalada de clientes tuvo un incremento del 20 por ciento.

La mayor demanda se originó en el sector de manufactura, especialmente el negocio de laboratorios de especialidades medicinales. En segundo lugar, se encuentran los ISP (proveedores de acceso a Internet, según sus siglas en inglés), entidades financieras y empresas de servicios y de comercio electrónico los que más ampliaron la demanda de seguridad informática. En la mayoría de los casos se trata de empresas que comenzaron a exportar y debieron reforzar la seguridad en las transacciones bancarias.

"*En el caso de las empresas grandes, en especial en las compañías financieras, existe una alta conciencia sobre los riesgos de la seguridad informática. Sin embargo, si hablamos de las medianas aún falta mucho para llegar al nivel de conciencia necesaria y conducir de forma segura negocios sobre Internet*", describió Jim Bullen, CEO de Etek, para quien, precisamente, la mayor oportunidad de negocio se da en las pequeñas y medianas empresas.

"*Una empresa grande puede establecer su propia infraestructura de seguridad, con firewalls, antivirus y todo lo que se necesita. Pero para una empresa pequeña es difícil, costoso y complicado*", dijo Bullen, que preside la empresa desde 1996.

Certificación de calidad

En diciembre de 2004 Etek cumplió 30 años en América latina y 25 en la Argentina, donde opera con el nombre de Reycom. Enfocada en brindar soluciones de seguridad informática a las empresas, el año pasado facturó 3,2 millones de dólares. Con casa matriz en Miami, cuenta además con oficinas en la Argentina, Colombia, Chile y Brasil y 150 empleados en el nivel regional.

En 2004, asimismo, obtuvo la certificación BS 7799 y se convirtió en la primera empresa de servicios informáticos en lograr esta calificación y la segunda del país. Además, mantuvo la certificación ISO 9001-2000 para todas las áreas de servicios y de negocio.

Fuente: Diario La Nación

La incidencia en los presupuestos de tecnología

En América Latina las empresas asignan aproximadamente el 2% de su presupuesta de TI a la instalación de sistemas de seguridad, mientras que el promedio en el resto del mundo supera el 5 %. Según estimaciones del *Security Operation Center (SOC)* de Impsat, en la Argentina se registran cerca de 70.000 ataques diarios destinados a servidores que ofrecen algún tipo de servicio sobre Internet, y el 80% de las caídas de red con producto de debilidades internas.

Además de nuevos métodos de trabajo, la gran penetración de Internet en el mundo empresarial incorporó también peligros de ataques informáticos. Por eso, los especialistas recomiendan tomar conciencia de los riesgos y diseñar políticas acordes para evitar vulnerabilidades y otros inconvenientes. En el país, los sectores energético, financiero y farmacológico

Superada la crisis, las compañías se encuentran en pleno proceso de concientización sobre la necesidad de proteger sus redes y sistemas. Tanto es así que, en el último año, creció de manera notoria la demanda de consultoría para evaluar y actualizar las herramientas de protección del negocio.

son los más precavidos a la hora de implementar estrategias y soluciones de seguridad informática.

Escenario

La crisis y la devaluación incrementaron el riesgo de las compañías que no pudieron actualizar sus recursos, principalmente, debido a los costos en dólares de los productos y a que los presupuestos destinados a TI priorizaron proyectos orientados a disminuir los precios. Sin embargo, la tendencia indica que las firmas se encuentran en un proceso de mayor concientización sobre la importancia de proteger y sus redes y sistemas. De hecho, existe una mayor demanda de consultoría para evaluar y actualizar las herramientas de protección del negocio. Durante el primer semestre de 2004 **Symantec** registró 1.237 nuevas vulnerabilidades alrededor del mundo, de las cuales el 70% podrían haber sido evitadas fácilmente y la mayoría fueron amenazas moderadamente graves o muy graves.

Juan Carlos Vuoso, gerente general de **Etek Argentina (Reycom)**, consideró que "*sin una adecuada*

Continúa en página 32

Viene de página 28

concientización de los usuarios y políticas de procedimientos, la incorporación de soluciones no alcanza".

Jorge Chapiro, presidente de **Infotron**, coincidió con la visión de Vuoso y sostuvo que "*casi el 80% de las caídas de red son el corolario de debilidades internas*". Un tendido de 500 equipos conectados normalmente recibe 2.000 vulnerabilidades que deberían ser corregidas en el día. "*Los ataques* -aseguró Chapiro- *responden a una cultura de omisión; además de la carencia de profesionales y de recursos a causa de la devaluación*".

Roberto Langdon, vicepresidente de Ventas y Marketing, y Carlos Rienzi, Chief Security Officer, ambos de **Cubecorp**, mostraron preocupación porque "*muchas empresas subestiman el factor riesgo en materia de seguridad*". Por su parte, Juan Carlos Zampatti, director de **Zampatti & Asociados**, resaltó que "*existe un falso sentido del resguardo, porque aquel que atraviesa por inconvenientes no los divulga ni siquiera para llamar la atención de sus pares*".

Para la mayoría de los ejecutivos consultados, un programa de protección de la información debe apoyarse en políticas coordinadas con las principales funciones del negocio, con la protección de monitoreo continuo para auditar y detener amenazas. Entre los riesgos, Pablo Balzi, responsable del área de Soporte Preventa de **McAfee**, enfatizó que "*una PC que se conecta a Internet sin protección pasaría menos de cinco minutos antes de infectarse*".

Panorama

Los proveedores resaltaron que durante la crisis se paralizó la gran mayoría de los proyectos TI, aunque las firmas están comenzando a renovar sus parques informáticos.

Langdon y Carlos Rienzi, de **Cubercop**, evaluaron que "*la desaparición del crédito y el impacto de los costos en dólares tras la devaluación dificultaron la concreción de los planes de inversión y de renovación tecnológica e muchas empresas*". De todos modos, Mario Videla, director comercial de **Ligitech**, advirtió que "*se está comenzando a tomar conciencia sobre los riesgos*" y Vuoso destacó que, en 2004, "*se incrementó la demanda de consultoría para la revisión y el reacondicionamiento de los mecanismos de gestión de protección*". Además, según Daniel Villanueva, director de Desarrollo de Negocios de **Sofnet**, "*luego de la salida de la convertibilidad los clientes comenzaron a ser más específicos en sus pedidos de soluciones*".

Para Santiago Cavanna, consultor de Servicios y Seguridad de **Computer Associates (CA)** "*algunas industrias aún no detectaron la necesidad contar con sistemas de seguridad*". Según María Sol Gatti, responsable de Marketing y Ventas para Argentina y Uruguay de **Symantec**, "*en los departamentos de TI de las firmas locales la premisa es hacer más con menos y son prioritarios los proyectos destinados a la reducción de gastos, integración y consolidación*".

Para Gatti "*usualmente se cree que la seguridad de las redes tiene pocos beneficios y muchos costos, pero la ausencia de estrategias de protección pueden llevar a la pérdida de productividad y ganancias*".

Demanda

Más allá del tamaño de la compañía, siempre va a requerir sistemas que protejan su negocio, por eso la oferta cubre todos los segmentos de mercado.

Cavanna, de **Computer Associates**, destacó que "*la demanda de medianas y grandes empresas pasa, principalmente, por el control del contenido, la identificación de vulnerabilidades, la administración de identidades y el análisis de eventos de ataque que permite integrar distintas soluciones de seguridad*". Las Pymes, en cambio, requieren básicamente sistemas de control de contenido y de acceso a Internet y, en algunos casos, de detección de intrusos. Para Villanueva, de **Sofnet**, "*existe una conciencia marcada en las Pymes acerca de los problemas que afectan su productividad cotidiana*".

Por otra parte, la tendencia al teletrabajo y los constantes viajes de negocios de los ejecutivos trazan un nuevo escenario para la seguridad de las redes corporativas.

"*El cambio de hábitos requiere de sistemas cada vez más inteligentes, usuarios más capacitados, políticas claras e infraestructuras más seguras*", sostuvo Villanueva. Para Cavanna, de **CA**, "*antes de pensar en trabajar en línea o remotamente, las compañías deben resolver aspectos básicos como la educación de los usuarios*".

Al respecto, Gatti, de **Symantec**, explicó que "*si no se definen políticas para el uso de redes wireless, los empleados podrían exponer a la empresa a serios riesgos de seguridad*". Julio Cella, de **Trends Consulting**, por su parte, resaltó que "*el futuro inalámbrico conduce a tomar medidas para los virus que se propagan a nivel de la capa de la red y de los tendidos celulares*".

En este sentido, Videla, de **Ligitech**, advirtió que "*se están produciendo fusiones entre los proveedores de seguridad para distintas redes y dispositivos, con el objetivo de entregar productos en conjunto*".

Fuente: Revista Convergencia, Redes corporativas y Pymes