Inseguridad On Line Vs Seguridad Gerenciada

Autor: Epifanio Blanco
URL: http://www.portinos.com.ar/
Fecha de Publicación: 07-09-2005

Mucha protección antivirus, firewalls, pero poco análisis de los ataques. Los bancos de primera línea de la Argentina están siendo jaqueados y no todos salen airosos de los ataques, aunque poco se sabe de ellos por una ¿bien cuidada gestión de imagen? Luego de los bancos y aseguradoras, las industrias son la siguiente presa, sobremanera en la modalidad de espionaje industrial. Ante ello crece la tendencia de la seguridad gerenciada.

Conocí a Roberto Langdon como directivo de Impsat, supe luego de su paso por Cube Corp y lo reencontré ahora, ocasión en que me habló de su nueva y propia compañía: 2Minds, que abrió menos de un año atrás y que registra un crecimiento vertiginoso.

Langdon tiene una explicación sencilla: en 2Minds damos lo que otros no dan en materia de seguridad on line; el análisis e inteligencia de cómo parar los ataques o tentativas (log) de vulnerar las redes de la empresa. Indicamos de dónde vienen y qué buscan.

Roberto Langdon (RL) sostiene que los problemas de seguridad on-line son cada día más dramáticos y no alcanzan antivirus, firewall y equipos sofisticados para salvar los valiosos activos que vulneran los hackers y los ataques de todo tipo cada vez más frecuentes.

Existen, además, falacias de seguridad, por ejemplo: "Colocar una PC hogareña conectada a Internet con un personal firewall, provocará asombro al ver que se bloquean más de 70.000 intentos de acceso no permitido a la PC, en sólo una semana... y esta es una comprobación que hice personalmente en marzo de 2005", dice RL.

En materia empresaria se supone que existen más recursos y más recaudos, pero suelen darse problemas como que el área de telecomunicaciones, solo piensa en "la conectividad" y la de IT en "las aplicaciones". Suele detectarse una zona gris sin acción por ambas áreas.

Sigue faltando allí no solo el enfoque panorámico, sino la acción contra adecuada contra los riesgos. Y finalmente, no hay análisis alguno de los episodios que se registran cada día de modo más feroz e indiscriminado.

Para ejemplificar el riesgo que todos corremos RL invita a reflexionar así: ¿Qué pasaría en un banco si la vigilancia policial se limitase a sólo 2 horas durante el horario pico de atención al público?

¿Qué pasaría en su casa -añade- si sólo deja la puerta cerrada por la mañana pero en el resto del día la mantiene abierta y sin cuidados? O ¿si cierra las puertas pero deja las ventanas abiertas, con acceso a la calle y sin rejas?

¿Qué pasaría si su caja fuerte queda abierta sin cerrojo gran parte del día, aunque por la noche la deje cerrada?

Los cuidados, controles y protección deben ser permanentes, pues su vulnerabilidad o negligencia convierte a todo en vulnerable, sostiene Langdon. Y, aún más: la seguridad informática se rige por el mismo sentido común. Debe estar presente siempre y en todo momento.

Y, es en este punto donde 2Minds encuentra su razón de existir: Los servicios de seguridad gerenciada se convierten en pseudo ciberpolicía que vela por sus recursos informáticos en forma contínua, aún cuando la empresa no está en actividad.

El tema de la seguridad empresaria no es menor, aunque no todas las corporaciones toman los debidos recaudos. Según Forrester Group entre las empresas de Fortune 500 se evidenció que el gasto en seguridad informática de dichas compañías entre 2002 y 2004 fue del 0.0025% de sus ingresos. Esto es menos de lo que gastan en café. "Si esto es verdad no sólo serán vulneradas. Merecen ser vulneradas!"

Yproblemas de ese tipo están sufriendo bancos de primera línea de la Argentina, confió Langdon. Quién puede suponer que un banco no tiene recursos para su seguridad.

¿Por qué es necesaria la seguridad gerenciada? El servicio de Security Operation Center (SOC) colecta los incidentes que se detectan, entre los cuales se encuentran los falsos positivos y los ataques reales. El SOC realiza un:

- Monitoreo contínuo de la actividad y los logs de firewalls y análisis del mismo
- Monitoreo de la actividad y de los logs de los IDS e IPS
- Colección de eventos
- Correlación de eventos en base a los incidentes registrados
- Identificación, detección y prevención de ataques
- identificación de patrones de ataque
- identificación de orígen y destino de los ataques
- estadísticas por tipo, severidad, frecuencia, origen y destino

El SOC -resume Langdon- clasifica los tipos de incidentes, descartando los falsos positivos. Y luego la información es provista al cliente mediante reportes, lo cual le permite ajustar sus políticas e, inclusive, realizar acciones legales, si correspondiere.

Para la realización de ese monitoreo permanente y otras actividades como análisis forenses; pruebas de penetración y análisis de vulnerabilidades y la generación de informes y reportes, 2Minds cuenta ahora con una decena de expertos y serán 31 al concluir 2005, según la prospectiva de tareas en curso.

Un lustro atrás, cuando conocí a Langdon en sus funciones ejecutivas para Impsat tenía un horizonte de tareas que abarcaba toda latinoamérica. Ahora, desde 2Minds, ese horizonte parece más vasto aún. Y se suma a ello el campo consolidado que vienen teniendo las empresas argentinas que proveen servicproductos y servicios de seguridad on line. Pongamos por caso Core Technoligies , cuyas herramientas también utiliza 2Minds, entre otras que proveen sus compañías como Cisco, Nokia, McAfee, Symantec, RSA Security, Global Software, ChekPoint, Sinocwall, Internet Security Systems, entre otras.