

Protegerse en medio de la crisis

La pérdida de información afectará a 190 millones de personas en el mundo, en 2009. La disyuntiva es cómo montar una arquitectura de seguridad eficiente en tiempos de reducción de presupuestos.

El 2008 se fue, no sólo dejando la crisis financiera mundial en pleno desarrollo, sino, también, instalando una preocupación entre los CIOs y gerentes de Sistemas que enfrentan 2009: desde noviembre último hasta febrero, la cantidad de personas que sufrieron incidentes de pérdidas de datos (47,8 millones) fue mayor a la cantidad registrada durante los primeros ocho meses del año (2008), y un 38% mayor a la cantidad registrada durante el mismo período de 2007 (34,5 millones). Los datos, surgidos de un informe de **KPMG** a nivel mundial, plantean una clara disyuntiva: cómo hacer para montar una arquitectura de seguridad eficiente en las empresas, en medio de las presiones sobre reducción de presupuestos que trae la crisis.

El caso argentino

Si bien, al ser consultados, los especialistas plantearon que el panorama no es para alarmarse a escala local, hay una afirmación que sí provoca más de un resquemor: el informe plantea que "a medida que los países con mayor penetración de la banca electrónica han reforzados sus mecanismos de protección, países como la Argentina, con un volumen todavía limitado de transacciones *e-banking*, se han situado en el punto de mira de

posibles atacantes. Ahora se enfocan en mercados que eran antes secundarios", dice **Alexandre Villeyra**, gerente de IT Advisory de **KPMG**.

Hoy, las grandes compañías locales han avanzado en herramientas de recuperación automática de información y en mecanismos de seguridad que antes no contaban, pero las pymes todavía se ven vulnerables. "Se arma una infraestructura, pero no se hacen cursos de capacitación a los empleados. Falta ingeniería social, trabajar en la gente, en la cultura", admite Juan José Dell'Acqua, vicepresidente de Usuaría (Asociación Argentina de Usuarios de la Informática y las Comunicaciones).

Pero la crisis no sólo afecta a la caja de las gerencias de Sistemas, sino que el temor también está en que muchos de los empleados tienen información que le interesa a la competencia: "Muchos, por miedo a perder su empleo y con acceso a información valiosa, la toman para usar como valor agregado al momento de buscar otro trabajo", comenta Claudio Pasik, director de NextVision, empresa de tecnología focalizada en temas de seguridad, con oficinas en la Argentina y España. "No necesariamente se modifican las formas de protección, pero sí hay un mayor foco y preocupación de las empresas para que sus nego-



Claudio Pasik, de NextVision.



Juan José Dell'Acqua, de Usuaría.



Alex Villeyra, de **KPMG**

cios estén protegidos", afirma Edwin Bowman, director General Latinoamérica de Attachmate, empresa que proporciona soluciones para el gerenciamento de seguridad informática.

Actualizar herramientas

Entre los pasos preventivos aconsejados están: establecer políticas de seguridad claras que cubran toda la información importante de la compañía, esto es, identificar al usuario (personal, cliente, proveedores u otras personas ligadas a la empresa) y quiénes tienen acceso, por qué

terminales y en qué momento; entrenar y concienciar a los empleados con contratos de confidencialidad; clasificar la información estratégica; actualizar herramientas de seguridad: tanto físicas como tecnológicas (claves, control de acceso, *firewalls*, anti-virus). "Siempre es saludable ajustarse a una norma y no depender de criterios particulares. Aconsejamos alinearse a la norma ISO 27002, que cubre todos los aspectos de seguridad de la información", aclara Pasik.

"No hay estrategias mágicas para resolver problemas de pér-

didas de datos. Lo fundamental es tener recursos para prevenir los episodios", destaca Bowman. Las principales amenazas están relacionadas con dispositivos móviles, como *pen drives* o laptops con información que no está encriptada. Pero la técnica más utilizada suele ser el *phishing*, donde un servicio financiero solicita al usuario que ingrese para cambiar sus datos.

Pero ante este problema: ¿qué medidas son convenientes? Es importante, coinciden los especialistas, tener una buena comunicación interna y, si se da el caso, dar a conocer el incidente. Luego, hacer una evolución de qué tipo de información está sujeta a la pérdida y ver si está respaldada en otro sitio (*back up*). Una vez elaborado el marco de situación, es conveniente definir los procedimientos de actuación.

Dentro de las compañías locales, los *data centers*, las compañías financieras y las tecnológicas parecen estar más preparadas para afrontar estos ataques, mientras que los sectores de servicios públicos y de telecomunicaciones aparecen como las más vulnerables. "Excepto algunos organismos, como la AFIP o la ANSES, faltan muchos recursos financieros en el sector público para concientización", afirma Pasik. También enumera empresas de sanatorios o clínicos.

Panorama mundial

El informe de **KPMG** sostiene que la cantidad de personas en todo el mundo que en 2009 sufrirán pérdidas de datos podría ascender a 190 millones, en comparación con los 92 millones alcanzados en 2008. Sostiene que los países que reportan la mayor cantidad de personas afectadas son el Reino Unido y los Estados Unidos, mientras que el sector financiero es el más preparado para hacer frente a la amenaza. El panorama de la ciberdelincuencia toma dimensión cuando se lo compara con otras actividades de fraude: según datos no oficiales, genera un negocio de u\$s 106.000 millones, un monto superior al que genera el narcotráfico.

Manuel Parera

Consejos para el frente interno

Hasta un 25% de los incidentes relacionados con pérdidas de datos se originan por el robo de computadoras y otros dispositivos móviles. Por eso, es importante, de la mano de la cada vez mayor penetración de estos dispositivos, mantener la información encriptada o codificada para reducir el riesgo a que, ante robos, no puedan acceder a la información. Es recomendable usar *passwords* no evidentes y alternativos, que combinen números y letras que no denoten referencia explícita a algo. Memorizarlo es preferible a dejarlo anotado en algún sitio donde pueda ser tomado por un tercero.

En determinadas áreas dentro de la organización, donde circula información sensible como Recursos Humanos por ejemplo, se recomienda deshabilitar todos los puertos USB, cuando no están siendo utilizados por el usuario indicado. Si tiene acceso a Internet es importante contar con una adecuada protección de la red perimetral.

Por último, dos puntos por demás importantes y que se anotan los menos desarrollados en las compañías locales: la sensibilización del cliente de *e-banking* y la concientización de los activos de la empresa. En el primero, hay prácticas que un banco nunca le va a pedir al usuario, como ingresar datos personales o códigos de la tarjeta de crédito por *e-mail*, en cuanto a los recursos humanos se recomienda concientizarlos sobre los verdaderos activos de la compañía y que trabajen sobre discos o directorios de red, protegidos por el centro de datos de la compañía.

La amenaza en cifras

Datos Argentina

2do semestre de 2008: incremento significativo de incidentes de pérdida de datos.

- 25%: por robo de computadoras y dispositivos móviles.

(Fuente: **KPMG**)

130: robos de identidad por mes (**)

\$500 millones: pérdidas anuales de las entidades bancarias (**)

220: tipos de fraudes y malas prácticas en Internet (**)

Spam o correo basura: el más común

(Fuente: Datos del mercado; entrevistas realizadas / (***) Estimado)

Datos Mundo

2009: 190 millones personas afectadas (aproximado)

2008: 92 millones personas afectadas

589 incidentes desde enero 2009

(Fuente: **KPMG**)