



Seguridad y disponibilidad, en ruta hacia un modelo de servicios

Concienciación, imperativo de la Ley, responsabilidad en las inversiones, afianzamiento de nuevos modelos comerciales basados en el servicio, y mayor especialización, como soluciones a la problemática de la pyme

La realidad es que muy pocas pymes cuentan actualmente con políticas de seguridad, y sólo en escasas ocasiones desarrollan campañas para advertir a sus empleados sobre las consecuencias que pueden llegar a suponer determinadas amenazas. El antivirus ya no es suficiente, y las estrategias a este respecto han de incluir todos los activos de software, como la protección basada en la reputación. En definitiva, se trata de hacer de este concepto una prioridad. Como ejemplo, el informe "Principales

tendencias en seguridad y disponibilidad" a lo largo de 2009 de Symantec ratifica con respecto al spam que desde 2007 esta práctica ha aumentado un 15%.

Otra problemática reseñable tiene que ver con la carencia de planes de backup ante posibles desastres, ya que muy pocas pymes cuentan con una propuesta a este respecto. Entre otras tendencias cabe destacar que se empleará la ingeniería social como principal vía de ataque, y que las aplicaciones de otros fabricantes para redes sociales se convertirán en objetivo clave de fraude. Entretanto, Win-

dows 7 se encontrará en la diana de los agresores.

DISPONIBILIDAD

Por otra parte, y en materia de disponibilidad de la información, el estudio de Symantec apunta a que 2010 será "el año de la limpieza de datos", pues, al no aumentarse los presupuestos de gasto en TI, muchas empresas tendrán que eliminar información. También en 2010 se terminará con la acumulación de cintas de backup para retenciones a largo plazo, ya que esa funcionalidad ha de cubrir la el archivado. La expansión de la deduplicación, que

se implementará de forma generalizada como una función en lugar de como tecnología independiente; y el almacenamiento en la nube como motor de la gestión de datos serán otras dos tendencias a lo largo de este año.

En este contexto, Symantec ha querido reunir a distintas organizaciones junto a representantes del canal y de la administración local para debatir sobre todos estos puntos y sus posibles consecuencias. Entre las factibles soluciones se ha barajado la necesidad de concienciación a todos los niveles; la urgencia de un

imperativo coercitivo de la Ley; una mayor responsabilidad en las inversiones de entes públicos y empresas; el afianzamiento de nuevos modelos como servicios gestionados o cloud computing; y una mayor especialización entre el canal. Así lo corrobora José Miguel Rodríguez, socio director de la consultora TIC e-Quatium: "Vivimos en un entorno donde no existen políticas de seguridad o, de haberlas, no existe conciencia a la hora de su aplicación. Más que de planes de seguridad podemos hablar de políticas de asalto. Esto cobra importancia cuando

se producen salidas de empleados insatisfechos de las organizaciones, donde se percibe un daño inmediato, o potencial respecto a la empresa”, explica. Y en este sentido, como paliativo, apela a la concienciación generalizada así como a la llegada de nuevos horizontes que dejan entrever la imposición de la modalidad SaaS (Software as a Service, software como servicio) y del concepto cloud. “De esta forma, comienza a implementarse una política de seguridad auspiciada por un tercero”, puntualiza. La gestión en la nube parece ser también la panacea para las administraciones locales, en especial para los pequeños ayuntamientos que, aunque caminan en la dirección adecuada hacia el establecimiento de prácticas seguras, se encuentran con el hándicap de que las vicisitudes inherentes a esta materia avanzan mucho más deprisa, dejando al descubierto agujeros necesarios de cubrir. Y en este recorrido, los cavados por la falta de concienciación del propio funcionariado son, al igual que en la empresa, los más profundos. Así lo explica Virginia Moreno, directora de sistemas del Ayuntamiento de Leganés y miembro del Grupo Técnico de Sociedad de la Información de FEMP. “Contamos con normativas que nos afectan directamente en materia de seguridad, pero nos encontramos con la misma problemática que la pyme. Por ejemplo, la Ley 30 en temas de contratación nos exige una serie de trans-

sacciones electrónicas con las empresas y diferentes proveedores; la Ley 11, de acceso electrónico de los ciudadanos a los servicios públicos, nos obliga a seguir medidas seguras sobre todo en aspectos de documentación; la Ley de Protección de Datos (LOPD) también nos marca unas pautas muy claras, pero la realidad es que no se están

cumpliendo del todo, a pesar de que durante los últimos años se ha avanzado mucho”.

DESDE EL PARTNER

Consenso generalizado en torno a la práctica del cloud computing como paliativo a las políticas de seguridad, sí, pero, ¿cuál es la realidad de este modelo en lo que a implantación

se refiere? ¿Qué tipo de compañías son las más proclives a este tipo de propuestas? En calidad de partner preferente de Symantec, SCC, en boca de su director general, Eloy Cano, asegura que el concepto de la nube se encuentra todavía “un poco verde entre el canal”, aunque no duda de su eficiencia futura. “Hay mucho

miedo a la seguridad en cloud. Lo que intentamos aportar al cliente está en función de sus propias necesidades. No obstante, lo cierto es que la mayoría de las pequeñas empresas no tienen definidas políticas de seguridad y las que sí lo han hecho no las han actualizado. Sin embargo, creemos que la práctica del cloud va a ayudar ➤



“Dada la importante reducción en las inversiones en storage, 2010 será el periodo de la limpieza de datos. Algo que puede hacerse tanto eliminando como limitando”

Gabriel Martín, director general de Symantec para Iberia



“En seguridad y disponibilidad las oportunidades y las economías de escala están en la nube, y van a continuar como tendencia arrolladora”

Carlos Muñoz, director de distribución y SMB de Symantec para España y Portugal



“Es más fácil perder información en el puesto de trabajo que mediante gestión remota. Se trata de que el usuario se conciencie de la existencia de más seguridad a través de este último modelo”

Álvaro Serrano, gerente de ADDETI



“La mayoría de las empresas aún se encuentran en una fase muy incipiente de consolidación de la seguridad”

Antonio Cimorra, director de Tecnologías de la Información de AETIC



“El modelo SaaS abre importantes oportunidades al canal, siempre y cuando éste sea capaz de transmitir el bajo coste que tiene”

José Miguel Rodríguez, socio director de e-Quatium



“La gestión a través de terceros tiene mucho campo en la Administración. Debes tener los recursos justos, y lo demás, delegarlo a un experto”

Virginia Moreno, directora de sistemas del Ayuntamiento de Leganés y miembro de la FEMP



“La normativa es muy importante como efecto tractor, así como la gran compra. Ya nadie se plantea trabajar sin antivirus, como hace cinco años”

Pablo Pérez San-José, gerente del Observatorio de la Seguridad de la Información de INTECO



“Una de las mayores problemáticas en materia de backup en la pyme es que buena parte de la información se encuentra en demasiados puestos distribuidos”

Eloy Caro, director general de SCC

➤ en un futuro a la problemática en el mundo de la seguridad y también en lo relativo al backup. Eso sí, a día de hoy, la mayoría de nuestros clientes de servicios gestionados son organizaciones medianas y grandes; las pequeñas siguen mostrando mayores reticencias a delegar sus activos a un tercero". En opinión de Carlos Muñoz, director de distribución y SMB de Symantec para Iberia, "la propuesta SaaS

tiene comprometidos con su cliente; y también otras derivadas, como las relativas a la protección de datos, etc. Hace falta mayor transparencia en los proveedores de SaaS en cuanto a cómo cumplen con esas normativas y a cómo trabajan esa información, tanto en la parte de seguridad como en la de backup. Además, la legislación vigente tiene que evolucionar a su vez para entrar de lleno en ese

a la calidad debido a la gran exposición a la que se encuentra". En opinión del directivo, al final, lo que este tipo de prácticas va a reportar es que el cliente pueda dedicarse de lleno a su negocio, además de contribuir a la eliminación del software ilegal.

FALTA MADUREZ

Reforzando este capítulo, Álvaro Serrano, director de ADDETI, apela a la falta de sensibilización, "lo que no

y legalidad del software que utilizan". "Respecto al canal –sigue– tiene que especializarse en todas las materias de seguridad que le ayudan a ofertar servicios generadores de rentabilidad frente al hardware".

CONCIENCIACIÓN

Como adelantábamos, al final, la necesidad de concienciación en los diferentes niveles, tal y como ya existe en el ámbito de la gran cuenta, parece ser

torio de la Seguridad de la Información de INTECO: "Hay que concienciar, además de a los trabajadores, a los empresarios, que son quienes toman las decisiones. En los últimos sondeos realizados, hemos comprobado que existe conciencia de la importancia de la información, aunque trasladar todo esto a la existencia de planes de seguridad resulta complicado. Sólo el 17% de las pequeñas organizaciones cuenta con



está muy en boga pero parece que su adopción en el canal está siendo más lenta de lo esperado, entre otras cosas, porque existen incógnitas a despejar con respecto al modelo de negocio tradicional del software bajo licencia, renovación y mantenimiento. Esto es, existen divergencias que el canal aún no entiende. Por otra parte, pensando en el cloud o el SaaS, coincido en que existen aún muchas incógnitas que despejar en términos de la seguridad de esa información gestionada y de los niveles de servicio que el provee-

modelo en un futuro. Será una evolución progresiva, que avanzará a medida que puedan despejarse las incógnitas referidas".

Gabriel Martín, director general de la filial ibérica de Symantec, va un paso más allá, y no vacila en afirmar que "el Software as a Service es la tendencia a imponerse. Y es que, la seguridad cambia cada día. Existen tantos conceptos que la externalización, tarde o temprano, marcará la pauta. En estos momentos tenemos una importante oferta de servicios gestionados de correo limpio, una propuesta muy sensible

implica que los fabricantes no estén aplicando correctamente sus políticas de seguridad ni que el canal, como especialista en ofertar servicios gestionados en esta materia, no esté realizando bien su trabajo. La falta de concienciación procede de las propias empresas, sobre todo de las pequeñas, que no perciben la seguridad como un activo. Por tanto, este mercado debe madurar, y en ese recorrido es importante que asociaciones y administraciones sean capaces de transmitir al empresario la necesidad de actualización en las nuevas tendencias

el eje sobre el que bascula gran parte de la problemática de la seguridad y la disponibilidad en la pyme. Así lo corrobora Antonio Cimorra, director de TI de AETIC: "Pese a las iniciativas y esfuerzos conjuntos, el principal problema reside más en el origen; esto es, los empleados no están concienciados de la necesidad de establecer políticas al respecto. El sector tiene que realizar un esfuerzo importante en desarrollar nuevas aplicaciones y modelos de negocio en ese sentido". Afirmaciones que matiza Pablo Pérez San-José, gerente del Observa-

un plan de concienciación como tal para instruir al trabajador". En opinión del representante de INTECO son dos los elementos que van a diferenciar a la empresa cuando decide abordar una estrategia en materia de seguridad: la existencia de un responsable en esa disciplina y la valoración de la inversión en seguridad efectuada. "En lo relativo a almacenamiento y copias de seguridad hemos observado una implantación cada vez mayor en las organizaciones, algo que, dada la coyuntura, abre una puerta al optimismo".