

Joaquín Reixa, Director de Symantec Ibérica

«Tras la compra de Axent, Symantec está en disposición de cubrir todos los frentes de la seguridad corporativa»

Es de general aceptación que los productos de seguridad individuales ya no son suficientes para prevenir adecuadamente. El cliente corporativo busca productos que trabajen juntos, compatibles con tecnologías de seguridad de otros fabricantes y con capacidad para integrarse con otros servicios. Este parece haber sido el ideario de la multinacional Symantec, cuyo enfoque estratégico es hoy más que nunca atender las necesidades globales de seguridad empresariales. Su arma: la compra de todo el arsenal de protección atesorado por Axent Technologies. De ésta y otras cuestiones habla en la siguiente entrevista Joaquín Reixa, Director de Symantec Ibérica.



los frentes.

– **Sí, pero se quedan en el tintero las hoy afamadas infraestructuras de clave pública...**

– Es cierto, carecemos de una oferta de PKI propia y es, por el momento, la única parcela que nos quedaría por cubrir. En todo caso justo es decir que muchos de nuestros productos ya están preparados para interoperar con algunas tecnologías y aplicaciones PKI. En este sentido, acabamos de suscribir un acuerdo mundial con RSA Security para poder licenciar su tecnología criptográfica Bsafe tanto para nuestros productos de empresa como de consumo, y planeamos implementar este software en nuestros productos orientados a Internet.

– **¿Descarta Symantec una futura adquisición de alguna empresa especializada en PKI?**

– No lo descartamos en absoluto; de hecho, creo que es un paso lógico para redondear nuestra oferta, pero eso sucederá más adelante. Al día de hoy, y me hago eco de lo manifestado por nuestro Presidente, no queremos ir comprando sin ton ni son. Acabamos de culminar una adquisición sumamente delicada, porque ha significado la asunción de una gama de productos a los que Symantec no estaba acostumbrada, y tenemos que hacerlo sin precipitaciones.

– **Recientemente, el mercado ha sido testigo del ‘traspies’ mercantil de Network Associates, una multinacional que, como Symantec, también había adquirido otras compañías con tecnología orientada a usuarios corporativos. Según los analistas, debido a no haber sabido digerir estas adquisiciones previas. ¿Podría ser esto extrapolable a la casuística de Symantec?**

– Cualquier compra siempre es peligrosa dado que su integración adecuada es una de las tareas más difíciles en este tipo de operaciones. El secreto del éxito consiste en tener bien en cuenta tres aspectos: el primero es el de elegir muy bien la compañía que se desea adquirir; el segundo, diseñar un plan de integración coherente y capaz de salvaguardar todo lo bueno de la empresa objeto de la operación de compra, y, por último, tener un plan de implementación adecuado y sobre todo ejecutarlo rápido. En nuestro caso, Symantec ha hecho una elección muy cuidadosa; han sido prácticamente nueve meses los dedicados a diseñar cómo se iba a llevar a cabo esa integración y, tras su aprobación definitiva, los pasos se están dando muy deprisa. Con esto quiero decir que en sólo tres meses nuestra compañía funcionará como una sola en todos y cada uno de sus aspectos.

– **Una de las decisiones estratégicas más recientes de Symantec ha sido la de abrir una oficina en España con presencia directa para el mercado ibérico. ¿Cuáles han sido sus razones?**

– Claramente, Symantec se ha dado cuenta de que el mercado ibérico es potencialmente muy grande: no en vano, España es el quinto país en la UE y eso pesa a la hora de los números. Hoy día, es muy difícil, por no decir imposible, llevar la nueva estrategia de Symantec que, repito, es netamente corporativa, sin una presencia local. Se puede manejar el *retail* pero no la gran corporación. La única manera es como se ha hecho: abriendo una oficina en Madrid y otra en Barcelona; asimismo, trabajo intensamente para hacer lo propio en Lisboa antes de fin de año. El equipo actual consta de

– **¿Qué es la nueva Symantec?**

– Hoy por hoy, es la unión de una compañía clásica de *retail*, que es la Symantec de siempre, cuyo portafolio ya incluía algunas soluciones para el ámbito corporativo, y de otra puramente de corporación como venía siendo Axent; esta última, lo que aporta básicamente es conformar, por un lado, nuestra gama global de soluciones de seguridad, y por otro, crear una gama de productos cien por cien enfocada a la seguridad de la gran corporación.

– **¿Qué puede suponer la nueva Symantec para el usuario final?**

– Tener un único proveedor con un rango de soluciones de seguridad que cubre el noventa por ciento de las necesidades existentes. Esto implica que la Symantec clásica, la dirigida al consumidor, sigue y seguirá estando, pero también significa la llegada de una nueva y poderosa opción focalizada en las grandes organizaciones como proveedor de referencia en soluciones de seguridad.

– **¿Desde cuándo ha sido efectiva la adquisición y qué impacto tendrá en la operativa global de Symantec?**

– La compra de Axent, valorada aproximadamente en 975 millones de dólares, se anuncia el 27 de julio de 2000 y se hace efectiva, tras la pertinente aprobación de los accionistas de ambas compañías, el 18 de diciembre del mismo año. A efectos de negocio, en tanto una única compañía, arrancamos el 1 de enero de 2001. Inicialmente, se funcionará en paralelo, sobre todo en la parte de

distribución y canal hasta el 1 de abril próximo, fecha en que ya habrá exclusivamente una única operativa y un solo canal de distribución y de comercialización.

– **Del total de la operación de ‘suma de fuerzas’ entre Symantec y Axent, que parte porcentual ha correspondido a cada una del total?**

– Aproximadamente, un treinta por ciento de los ingresos mundiales provienen de Axent y el setenta por ciento restante de Symantec, lo que redondeando supone un billón americano de dólares. Las previsiones oficiales apuntan que para marzo próximo el sesenta por ciento de nuestros ingresos globales provengan de clientes empresariales.

– **La operación de compra ha sido una de las más sonadas el pasado año y supone el ‘ingreso’ de Symantec en el reducido grupo de multinacionales en disposición de ofrecer un conjunto de soluciones prácticamente completo. ¿Su estrategia es, pues, la de presentarse al mercado como un suministrador tecnológico capaz de resolver cualquier necesidad del usuario en esta materia?**

– Sin duda, ese es nuestro propósito. Con la suma de las propuestas de Symantec-Axent, nuestras soluciones ya cubren desde lo más simple y obvio, como pueda ser una solución antivirus, hasta el poder abordar grandes proyectos, por complejos que sean, de gestión centralizada de la seguridad, *single sign on*, auditorías de seguridad, detección de intrusiones, etc., con lo cual la Symantec actual está en disposición de cubrir prácticamente todos

doce personas.

– **¿Cuál es su estrategia de aproximación al mercado español?**

– Partiendo de que Symantec jamás hace venta directa, la llevamos a cabo por dos vías: a través de nuestros comerciales a la gran cuenta, y haciendo pinza con el canal a nuestros usuarios finales. Con este objetivo estamos conformando un canal muy selectivo basado en grandes integradores para que, de la mano nuestra y nosotros de la suya, podamos entrar en las corporaciones presentando una oferta de seguridad coherente.

– **En España, Telcosa ha venido siendo el referente en lo relativo a las soluciones del catálogo de Axent. ¿Cuál es su papel actual?**

– Hasta ahora ha sido el mayorista-distribuidor de Axent –nosotros lo denominamos un ‘mayorista de valor añadido’, es decir, que aporta algo más que el mero movimiento de licencias. Trabajan codo con codo con nosotros para la formación del canal, proveyendo soporte técnico. De hecho, Telcosa va a seguir siendo uno de los mayoristas de Symantec, ahora mismo especializado exclusivamente en la parte de productos de Axent y, a partir de abril, también llevará la gama corporativa clásica de Symantec referida a soluciones antivirus, inspección de contenidos y control de accesos: Norton Corporate Edition, Mail Gear e I Gear... En paralelo, a alguno de los tres mayoristas clásicos de Symantec, que son GTI, Ingram Micro y Tech Data, les ofreceremos llevar lo que era la gama más básica de Axent, esto es, los productos cortafuegos Raptor, a fin de que sus departamentos de *networking* puedan completar una oferta de seguridad básica focalizada hacia la pyme.

– **A finales de 2001, ¿cuántos integradores trabajarán con Symantec para el mercado corporativo?**

– Nuestra intención es no superar, en ningún caso, la cifra de quince. Han de ser pocos y buenos. Naturalmente todos ellos se encuentran entre los más conocidos y pujantes de nuestros país.

– **Cuales han sido los resultados recientes de Symantec en España?**

– Nuestras estadísticas recientes registraron un crecimiento del 35 por ciento, y desde la apertura de oficinas en España, el incremento se ha elevado al 41 por ciento. Esto demuestra claramente que la presencia local sí es determinante. En la parte de *retail* las cifras se mantienen, con crecimientos normales cercanos al 20%; en cambio en la venta corporativa de licencias se ha experimentado más de un 60% en el último trimestre.

– **¿Qué percepción tiene de las necesidades de seguridad corporativas en nuestro país?**

– Las grandes compañías se están dando cuenta cada vez más de la importancia de la seguridad. Eso no es nada nuevo, aunque, paradójicamente, no priorizan este aspecto todo lo que debieran en parámetros de inversión y rapidez. Pero, efectivamente, esto está cambiando y la ‘nueva economía’ no es ajena a este fenómeno.

– **La tecnología es lo suficientemente transparente, fácil y gestionable para atender adecuadamente las demandas corporativas en este sentido?**

– Hay de todo; depende del nivel en que uno se mueva. Tecnologías como las subyacentes en so-

luciones antivirus o de cortafuegos pueden considerarse ya como *commodities*, prácticamente son *plug & play*; en otros aspectos de la seguridad que quizá no se relacionan tanto directamente con la tecnología como con el concepto, sí se percibe a la tecnología como algo engorroso, difuminado y requiere muchos servicios. Me refiero a cuestiones relativas al diseño de políticas, diagnósticos y auditorías de seguridad, *tracking*...

Ahora mismo la realidad tecnológica proporciona productos que resuelven muchísimos de los problemas y suponen una gran ayuda para cuestiones tales como la gestión centralizada, etc., pero no es menos cierto que abordar un proyecto de seguridad en toda regla requiere un plan concienzudo, con todos sus pasos, sus costes, sus impactos y que hay que abordarlo desde una perspectiva global e integral y no a base de parches aquí y allá.

– **¿Cuáles serían las necesidades de seguridad que se deberían atender prioritariamente?**

– La principal, quizá, sea la creación de las políticas de seguridad y las correspondientes auditorías, seguida muy de cerca por la autenticación de usuarios y el *single sign on*, sobre todo en estos tiempos debido a la apertura de las intranets a todo el mundo; Y todo ello, naturalmente, con una gestión centralizada.

«Una solución antivirus debería ser percibida simplemente como una pieza más de las que han de componer el proyecto global de

– **Como quien dice, a cada segundo aparece un nuevo virus. ¿La tecnología para la gestión de esta problemática está madura para darle cumplida respuesta en los ámbitos corporativos?**

– Definitivamente sí. La gestión de todo lo que es la instalación del antivirus, el mantenimiento al día de los motores y las firmas y definiciones de virus se pueden hacer prácticamente de forma centralizada y, si me apura, hasta automática. Esto incluye la actualización de nuevas versiones de la solución implantada, propagándose en toda la red corporativa sin que los usuarios lo noten.

– **De todas formas, el gran reto para la tecnología antivirus es la de poder aplicar sus funciones de detección y desinfección en los archivos que se envían cifrados ...**

– El problema es que se necesita la clave para poder saber lo que hay dentro, punto. En lo que sí se está trabajando es en tecnologías capaces de analizar los ficheros y anexos cifrados en el momento exacto del descifrado y antes de que se implemente en el disco del *desktop*. Cuando el puesto cliente recibe el fichero y le aplica la clave correspondiente para descifrarlo, es en ese preciso instante cuando actuaría el antivirus chequeando si existe algún tipo de virus, infección o ataque. Según me han informado los técnicos de nuestro laboratorio, las primeras tecnologías comercializables para este cometido podrían ser anunciadas, aproximadamente, a comienzos del segundo semestre de este año.

– **Un segundo calvario para los desarrolladores es poner a punto una tecnología capaz de solven-**

tar el desafío que supone aplicar el antivirus a un mensaje firmado digitalmente sin alterar su integridad ...

– Sin duda, eso parece un reto de muy difícil solución a menos que surja una tecnología que conlleve ambas funciones, es decir, que la firma mas el antivirus sean una misma cosa y trabajen juntas. Frente a esto, ahora se aplican rutinas y procedimientos que vienen a parchear el asunto; por ejemplo, si es un mensaje, pues ponerlo en cuarentena, o que el propio sistema envíe un mensaje al emisor y receptor indicando que se ha detectado un virus en el mensaje en cuestión. En todo caso, es cierto, lo que no se puede hacer es enviar el mensaje al receptor habiéndolo limpiado de virus porque precisamente dejaría de estar firmado.

– **¿Las grandes empresas españolas están bien pertrechadas de soluciones antivirus corporativas?**

– En líneas generales, no. Todavía hoy muchas compañías utilizan soluciones antivirus de forma puntual, sólo se instalan en departamentos concretos, etc. Es más, incluso una misma empresa tiene diferentes antivirus. Escasean las grandes decisiones en esta materia para tratar de implantar una solución homogénea, coherente y para toda la

empresa. Y esto, en síntesis, conecta con lo que antes he mencionado: hay que empezar por el principio y si no hay un proyecto real global de seguridad no se están haciendo correctamente las cosas. Una solución antivirus debería ser percibida simplemente como una pieza más de las que han de componer el proyecto global de seguridad empresarial.

– **¿Qué opina sobre la tendencia a ofrecer servicios de seguridad gestionados, sobre todo al gran colectivo de pymes que no pueden permitirse el lujo de tener un departamento TIC, librándolas así de cometidos que no les corresponden y al tiempo protegiéndolas?**

– No hay duda de que va a ser una gran línea de negocio para los oferentes de estos servicios, y, al tiempo, muy beneficiosa para las pequeñas y medianas empresas, especialmente para aquellas que tienen alrededor de cien empleados y carecen de un departamento específico de informática. La posibilidad de acogerse a unos servicios de *outsourcing* de seguridad puede suponerles enormes ventajas.

En lo que a Symantec respecta, dado que nuestra oferta tecnológica cubre cuantas necesidades pudieran demandar esos usuarios, está en disposición de ofrecer la tecnología necesaria para que los prestadores de estos servicios, típicamente operadoras, ISP's y empresas especializadas en *outsourcing*, se sirvan de nuestros productos y apoyo tecnológico para ofertar servicios de seguridad gestionados. Ya estamos en conversaciones con los principales operadores españoles para que evalúen ofrecer servicios antivirus, cortafuegos y VPN's, e incluso inspección de contenidos y detección de intrusiones. ■

Texto: Luis G. Fernández
Fotografía: BGS