«Llevamos a los clientes a un estado de mínima inseguridad»

Nacida a mediados de 2000, S21SEC es una joven compañía española especializada en la prestación de servicios de auditoría de seguridad y en la realización de test de intrusión, que en corto espacio de tiempo ha ido ganando una importante cuota en el mercado nacional de grandes organizaciones: banca, administración, operadoras... Cuenta con un equipo de expertos acostumbrados a buscarle las vueltas a la seguridad telemática, y no le hace ascos al desarrollo de herramientas tecnológicas de protección. Su director gerente, Xabier Mitxelena, un experto en calidad, trata en esta entrevista, con la debida prudencia, de un ramo de actividad al que no asusta la palabra 'ataque'.

– ¿Qué resultados económicos ha obtenido S21SEC desde que inició sus actividades, y cuáles son sus previsiones?

– S21SEC se constituyó en 2000, y empezó a facturar, como quien dice, después del verano de ese año. La cifra alcanzada fue de un millón de euros; en este año 2001 podríamos alcanzar los 5 millones de euros, y en 2002 los 12 millones de euros.

– ¿Cuántos expertos en seguridad telemática tienen en plantilla?

– Somos 40 personas, de las cuales técnicos son 32. Nuestra idea es terminar este año con 60 técnicos y a finales de 2002 llegar a 125.

– ¿Y de dónde van a sacar ustedes a tantos especialistas?

– Nuestros técnicos provienen del ambiente cultural de la Red, y tienen sus propias bases de datos y entornos de trabajo. Mediante este canal podemos llegar a disponer de 10 ó 15 técnicos más manteniendo el nivel de calidad que consideramos oportuno, pero a partir de ahí la cosa se va a poner difícil, por lo que tenemos planeado crear un centro de formación, ya que por razones evidentes, el gran activo de S21SEC es su personal especializado en plantilla. Cogemos contratos en función de la disponibilidad de recursos, y si por no disponer de más equipo hay que decirle a un cliente final que no se le puede dar servicio hasta septiembre, pues se le dice.

– ¿Pone S21SEC alguna cláusula especial en los contratos de trabajo de los técnicos que tienen que trabajar 'atacando' los sistemas de sus clientes?

– Si a lo que usted se refiere es a si tenemos un contrato de confidencialidad, la respuesta es sí, tanto con el trabajador –sea o no técnico–, como con el cliente. Al respecto de este último, le diré que nunca se hace un trabajo sin la autorización previa del cliente final; es él quien marca las pautas de las IPs y los lugares que hay que revisar. A partir de ahí seguimos nuestros propios métodos de trabajo.

– ¿Tienen muchos clientes?

– Antes los contábamos con los dedos de una mano, pero en los últimos seis meses han crecido de una forma sustancial. Diría que estamos entre los 50/60, y con unas previsiones de llegar a fin de año en la actividad específica de servicios de análisis del estado de seguridad a los 120. De ellos un 80% pertenece al ámbito de la gran cuenta: administración pública, banca y seguros, operadoras, fabricantes..., y un 20% al de pymes, sobre todo aquellas que manejan I+D propio de los sectores metalúrgico, industrial y de servicios, y que han tenido problemas de fuga de datos a través de la Red.

Llegados a este punto me gustaría hacer dos precisiones: primera, que no siempre aquella empresa que cree haber tenido problemas los ha tenido; y segunda, que en general, cuando alguien nos llama es porque ha tenido problemas desde el punto de vista técnico o porque ha de conocer con exactitud los problemas que se puede encontrar desde el punto de vista legal.

– Un suponer: de las 100 compañías más grandes de este país, ¿cuántas cree que alcanzan el aprobado en seguridad?

– Un 80% están más o menos protegidas. A efectos de los niveles en que trabajamos, un 3%. Hasta hace poco las empresas han estado basando la seguridad en lo que denomino '*kits* de supervivencia': cortafuegos e IDS. Pero en este mercado ha habido mucha chapuza, de tal suerte que entrar a través de un cortafuegos en numerosísimas ocasiones no presenta demasiadas complicaciones. Esto se arregla utilizando profesionales expertos en seguridad.

– ¿Encuentran en el curso de sus trabajos agujeros de seguridad que pueden explotarse?

– Es una realidad. En casi todos los clientes encontramos agujeros lo suficientemente importantes como para que se pueda acceder a información confidencial. También es cierto que algunos de estos clientes llevan mucho tiempo sensibilizados y disfrutan de un nivel de inseguridad mínimo.

En general, diría que las redes internas y externas están expuestas a personas con una formación técnica media-alta que puede acceder a datos e información sin estar autorizados. No obstante, siempre hay que ser comedido, y las inversiones en seguridad han de ser las justas y necesarias. Para nosotros lo importante es que el cliente final sepa cómo está, o mejor, como va estando, ya que la seguridad es un proceso en el que aparecen continuamente agujeros y vulnerabilidades, algunos documentados, otros, quizá, no.

– Hay agujeros de seguridad. Pero, ¿pasan cosas?

– Sin duda. Le mencionaré algunas: usuario interno descontento con su poco reconocimiento, que mediante la introducción de troyanos en la red de su empresa, consigue que se caigan todos los días los sistemas; entidad importante, auditada supongo por una entidad también importante, en la que en menos de 10 horas entramos en un *host* haciendo transacciones en línea; usuario externo que entra en una entidad, se lleva la base de datos y las aplicaciones, todo ello residente en un externo; usuarios internos y externos que husmean información de la dirección general de una compañía; fugas de información, de naturaleza interna, en departamentos de I+D...

– Cabe intuir que una compañía como S21SEC no confía demasiado en la eficacia de las herramientas tecnológicas de detección de intrusiones...

– Los IDS, tanto los de pago como los de libre disposición, cumplen la función de ofrecer seguridad en ciertos niveles de las capas OSI; pero existen otros niveles que no se pueden abordar de una forma completamente automática. Es ahí donde resulta necesario realizar trabajos de ingeniería mediante expertos capaces de explotar los agujeros potenciales que tienen los sistemas, y, además, de determinar hasta dónde podría llegarse conociéndolos. A pesar de esto, somos más amigos que enemigos de los productos de IDS.

– En la experiencia de S21SEC, ¿se cumple el dato estadístico al uso que indica que entre un 70% y un 80% de los problemas de seguridad tienen un origen interno?

– Independientemente de que nuestros primeros 'ataques' los hagamos siempre desde Internet, cuando se abunda en la relación con el cliente y éste nos permite entrar en sus redes internas, descubrimos que muchos riesgos potenciales de seguridad están dentro. Sin embargo, las estadísticas están cambiando: si hace un año se hablaba de un 80% interno y un 20% externo, las más recientes sitúan la proporción en un 68% externo y un 32% interno.

– Además de ofrecer servicios de auditoría de seguridad y realizar test de intrusión –su actividad más conocida hoy–, S21SEC se ha lanzado al desarrollo de herramientas tecnológicas de seguridad. La primera es HIVE, pero habrá más.

– Por razones del origen de esta compañía y de su 'materia prima', era lógico que iniciara sus actividades en el segmento de las auditorías de seguridad. No obstante, pronto nos dimos cuenta de que teníamos potencial para, además, desarrollar herramientas nuevas que elevaran los niveles de seguridad de nuestros clientes.

Por la experiencia acumulada en el mercado sabemos que en el 98% de los casos las intrusiones se hacen al nivel de código de las aplicaciones. Así pues, la herramienta que hemos desarrollado y patentado, HIVE, es un protector de nivel 7. Se presentó el pasado mayo en Amsterdam, y ya tenemos varios clientes internacionales, entre ellos un desarrollador de software norteamericano que quiere implementar la herramienta para fortificar sus aplicaciones, orientadas a dar servicios de ASP a compañías de más de 10.000 usuarios internos.

Esperamos que HIVE no sea el único producto de S21SEC. De hecho estamos diseñando una segunda herramienta, orientada a la realización de auditorías *on site*, que verá la luz después de verano. Ésta es una de las herramientas con la que estamos intentado colaborar con los fabricantes de algunos de los escáneres más conocidos. Los escáneres hacen las auditorías remotas, lo que en tiempo y seguridad puede implicar en ocasiones riesgo; lo que hacemos con nuestro producto es bajar el *web* a un servidor *on site*, auditarlo con la herramienta comercial de la empresa pertinente, y generar un informe de S21SEC.

«En casi todos los clientes encontramos agujeros lo suficientemente importantes como para que se pueda acceder a información confidencial»

También estamos en otros dos proyectos de desarrollo, que nos han llevado a solicitar subvenciones al ministerio de Ciencia y Tecnología, ya que aunque tenemos capacidad de inversión, ésta, sin embargo, es limitada. Se trata del desarrollo de herramientas forenses que permitan a los clientes chequear cuándo han tenido un problema, hacer un seguimiento de los *log*, e intentar llegar al origen del asunto para poder plantear soluciones.

– En el caso de HIVE, ¿cómo se explica que los gigantes de la seguridad no hayan desarrollado ya alguna herramienta parecida?

– Están en ello, y en el futuro el mercado determinará si HIVE es mejor o peor que las del resto. Por el momento nos hemos adelantado, gracias a un equipo de expertos en intrusiones, que saben cómo entrar y, en consecuencia, están en una posición inmejorable para conocer cómo no se puede entrar.

– ¿Qué opina de la auditoría a terceras partes de confianza?

– Pues que es una alternativa de futuro importantísima. Si se ha optado por el modelo de terceras partes de confianza, en el contexto de los sistemas de firma electrónica de amplio espectro, parece lógico que auditar a los proveedores de servicios de certificación, desde un punto de vista legal, e incluso fiscal, es un asunto crítico. Habrá que auditar las plataformas tecnológicas de los proveedores y determinar si hacen lo que ellos dicen, o si ellos dicen lo que hacen. Uno de los objetivos de S21SEC, a medio plazo, es especializarse en auditar soluciones PKI. También tengo que decirle que siempre hemos pensado que desde un punto de vista fiscal el futuro pasa por inspeccionar y auditar a los servidores de comercio electrónico.

Por otra parte, S21SEC mantiene una línea de trabajo, por la que ya factura desde hace 6 meses, que consiste en realizar chequeos de seguridad a herramientas tecnológicas de fabricantes internacionales de seguridad TIC.

– Ya que ha mencionado los servidores *web* de comercio, ¿qué opinión le merecen los sellos de confianza tan de moda últimamente, tipo WebTrust u otros de compañías auditoras específicas?

– Las grandes consultoras y los grandes integradores empiezan a ver a la seguridad como un negocio, y como en el contexto de los negocios siempre se han distinguido por un nombre, pues tienen la necesidad de crear sus propias etiquetas. No creo en los sellos, y menos en materia de seguridad. Y lo digo por experiencia, porque algunos sitios que hemos auditado han pasado los niveles exigidos por alguno de ellos, y la verdad... Nadie puede certificar la seguridad, sí los métodos de auditoría de seguridad. Y me parece bien que existan entidades que sean capaces de dar fe de que otras entidades cumplen una serie de normas para poder auditar sus sistemas.

– En estos tiempos están aterrizando en España muchos fabricantes de sistemas de detección de intrusiones. ¿Le causa esto inquietud?

– Es buen sintoma, porque quiere decir que fuera de nuestras fronteras se están dando cuenta de que el concepto de seguridad en España está madurando. En muchas organizaciones se está llegando a sentir a la seguridad como una parte de los procesos de gestión, y cuando esto pasa, empiezan a encajar muchas piezas: consultoría, herramientas tecnológicas, integración, servicios...

De otro lado, y como ya he apuntado, la seguridad tiene elementos que no contemplan las soluciones comerciales, por lo que nuestra actividad en el campo de la auditoría de seguridad y los test de intrusión es complementaria a la de los fabricantes de sistemas de detección de intrusiones. Con alguno de ellos estamos incluso en conversaciones para encontrar sinergia.

– ¿Con cuál?

– Con ISS. Este fabricante está interesado en que el centro tecnológico de su Xforce en España sea S21SEC; igualmente, está interesado en integrar HIVE –y Araña, otro producto actualmente en desarrollo– en sus soluciones. Otro frente de conversaciones se centra en los servicios 24X7 y en la seguridad gestionada. n

Texto: **José de la Peña Muñoz**
Fotografía: **Jesús A. de Lucas**