

S21sec: “El triunfo de una precursora apuesta por la seguridad telemática

■ Texto: Nuevo Siglo

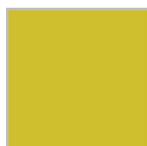
■ Fotos: Sara Santos

Cuando a comienzos del año 2000 nació S21sec, empresa guipuzcoana dedicada a diseñar e implementar servicios y soluciones de seguridad telemática para la protección de los sistemas de información de sus clientes, muy pocas personas eran capaces de imaginar entonces un mundo futuro en el que la máxima salvaguardia de las estructuras, los sistemas y los procesos productivos de las diferentes organizaciones iba a adquirir una importancia absolutamente estratégica.

Hoy, cuando apenas ha pasado un lustro desde que varios socios guipuzcoanos se lanzaran a la idea de poner en marcha esta compañía de nombre insólito y dedicada a ofrecer servicios que entonces resultaban no menos extraños, el 95% de la información que habitualmente manejan las instituciones, las empresas y los ciudadanos occidentales circula a través de las mallas informáticas, convirtiendo las redes de cualquier compañía en la base crítica de la gestión de los negocios y de la transmisión y el almacenamiento de datos.

Xabier Mitxelena, director general y socio fundador de S21sec.





Esta realidad ha convertida a S21sec en una empresa referente en el mercado nacional, donde cuenta con más de 300 socios, tanto clientes como partners. Entre éstos destaca, por ejemplo, el 80% del sector financiero, la mayor parte de la administración pública local y central, las principales compañías de telecomunicaciones, un porcentaje importante del sector sanitario, y muchas de las compañías más renombradas de comercio electrónico, así como las mayores líneas aéreas del país y otros medios de transporte y logística. En sus escasos cinco años de vida, la compañía donostiarra, además, ha abierto delegaciones en Madrid y Barcelona, y ha impulsado la apertura de diferentes oficinas en lugares tan dispares como Algeciras, Murcia y Atlanta (Estados Unidos).

"Nuestra idea inicial consistía en poner en marcha un concepto de seguridad diferente en Internet", explica Xabier Mitxelena, director general y socio fundador de S21sec, en la sede central que la empresa tiene en San Sebastián. "Desde un primer momento entendimos que la clave del éxito de una organización como la que queríamos impulsar iba a estar en el personal, en que fuéramos capaces de encontrar a los mejores ingenieros de seguridad del mercado, a los especialistas más destacados en técnicas de hacking. Con el fin de potenciar el contacto con este tipo de profesionales, en julio de 1999, en Mallorca, organizamos el I Congreso de Hacking Ético, en el que participaron 60 personas y con el que obtuvimos el convencimiento de que existía el suficiente potencial en recursos humanos como para poder continuar con el proyecto que estábamos desarrollando. De hecho, y con la experiencia del Congreso todavía reciente, comenzamos a trabajar en dos frentes: convencer a personas, a hackers de diferentes lugares del país, para que vinieran a San Sebastián a participar en una empresa nueva que se estaba creando bajo la óptica de un concepto de seguridad diferente; por otro lado, debíamos empezar a estructurar la empresa desde un punto de vista corporativo, para que ésta fuera lo suficientemente fuerte como para introducirse en un mercado incipiente, sumamente variable y dinámico, en el que apenas habían comenzado a aparecer algunos proyectos."

Si actualmente, cuando el contacto con Internet se ha extendido ya a extensas capas de la población y las informaciones relacionadas con el



mundo de las nuevas tecnologías aparecen habitualmente en los medios de comunicación, todavía resultaría bastante complicado tratar de poner en marcha una empresa formada en su mayor parte por hackers, hay que imaginar el esfuerzo que supuso en su momento encontrar los apoyos iniciales para la puesta en marcha de S21sec.

Explica Xabier Mitxelena que presentar la empresa afirmando que casi la mitad del personal de la misma estaba formada por este particular grupo de especialistas era, cuando menos, una forma difícil de comenzar cualquier contacto y, por ello, una de sus principales preocupaciones consistió en que se entendiera que *"el hacker no es más que un investigador que se pasa el día evaluando la seguridad de las redes y de los sistemas para ofrecer un diagnóstico preciso del grado de inseguridad que éstos puedan presentar. A partir de estos análisis se trata de intervenir en aquellos elementos que puedan tener un riesgo, proporcionando las soluciones y previniendo los peligros antes de que éstos se conviertan en realidades graves para las empresas. Resulta fundamental no confundir a los hacker con los ciberdelincuentes o con los crackers que, estos sí, tratan de evitar o romper los elementos de seguridad existentes en la red para la comisión de sus delitos"*.

- Resulta fácil imaginar que, dadas las particularidades de la empresa, el equipo humano que forma S21sec tendrá unas características especialmente definidas...

- En S21sec, los grandes investigadores provienen del mundo del hacking ético, es decir, son hombres y mujeres con una larga experiencia de trabajo en la comunidad virtual intentando proporcionar a Internet un valor elevado como instrumento clave que aporte riqueza a las sociedades. Se trata de personas generalmente autodidactas, muy creativas y

“La edad media de los ingenieros en seguridad que trabajan en S21sec es de 22-23 años”

“Resulta urgente impulsar de una vez por todas los grandes planes de I+D+i”

con un sexto sentido excepcional. En mi opinión, son los artistas de la red, profesionales que tienen una gran capacidad para intuir los riesgos de seguridad que van a surgir en el ciberespacio, Además, todos ellos están muy acostumbrados a trabajar en comunidades virtuales y poseen una elevada capacidad para innovar.

- ¿Resulta especialmente complicada la gestión de equipos de trabajo formados por personas con unas características profesionales tan marcadas?

- En el momento de liderar el trabajo llevado a cabo por este tipo de especialistas hay que tener en cuenta que éstas son personas un poco anárquicas en sus funciones y que, además, están acostumbradas a hacer lo que mejor saben hacer, y no otra cosa: cuidar de la seguridad en las redes. Hay que tener en cuenta que estamos hablando de hombres y de mujeres que son diferentes a nosotros, porque pertenecen a una generación diferente a la nuestra. La edad media de los ingenieros en seguridad que inician su trabajo en S21sec es de 22-23 años y, de hecho, quienes comenzaron a trabajar con nosotros en los orígenes de la compañía, hoy ya tienen 27 ó 28 años y ocupan puestos con una mayor responsabilidad. Desde cualquier punto de vista, el activo más importante que tiene S21sec es el del personal, independientemente de que la empresa haya ido generando tecnologías propias, patentes, etc.

- En algún momento le he escuchado decir que, en el ámbito de las nuevas tecnologías, el largo plazo son dos años, que el medio plazo escasamente dura un año y que el corto plazo apenas equivale a unos meses... ¿Cómo ve ahora, cinco años después, los primeros pasos de S21sec?

- El comienzo del proyecto es complicado, sobre todo por el volumen importante de capital que es necesario para poner en marcha la empresa. Cuando hay un proceso de emprendizaje, hay que marcarse los objetivos y, una vez que éstos están claros, es necesario diseñar un plan de financiación para los mismos. En nuestro caso, el objetivo era liderar el mercado nacional de la seguridad en las redes informáticas y esto exigía unas inversiones importantes. Aún hoy, todos los beneficios que va generando la empresa se invierten en la propia compañía, hasta que ésta alcance un equilibrio idóneo.

- Según su experiencia, ¿cuáles son los principales problemas a los que tiene que hacer frente un emprendedor, especialmente en el ámbito de las nuevas tecnologías?

- Por un lado, se echa en falta de un modo importante la cultura del capital-riesgo, lo que complica mucho la financiación inicial de algunos proyectos. Además, creo que hay una excesiva burocratización de las ayudas y de las subvenciones administrativas. A pesar de que llevamos años oyendo hablar de la ventanilla única, la realidad es que poner en marcha una empresa sigue siendo un proceso que consume muchas energías y muchos recursos. Personalmente, estoy convencido de que en S21sec nos hemos dejado subvenciones en el camino por falta de tiempo, por una desinformación importante y por lo complicado que, en ocasiones, resulta acceder a estas ayudas. De cualquier modo, recuerdo que en 1999, cuando nosotros comenzábamos, las únicas ayudas administrativas existentes eran las que se daban a la generación de empleo. Posteriormente, en los años 2000 y 2001, tanto la Diputación Foral de

Gipuzkoa como el Gobierno vasco ya comenzaron a impulsar algunos proyectos de apoyo a la innovación en el ámbito de actuación de nuestra entidad.

Explica Xabier Mitxelena que, a pesar de todo, "tanto Gipuzkoa como el País Vasco son territorios propicios para la puesta en marcha de este tipo de empresas, porque hay una capacidad importante de recursos, tanto humanos como económicos, para impulsar iniciativas empresariales de corte tecnológico. Solamente aquí, en Zuatzu, donde nos encontramos, resulta sorprendente el número de NEBT (nuevas empresas de base tecnológica) que están instaladas." "De cualquier modo, es necesario reconocer - añade el director general de S21sec - que



cada vez resulta más urgente lanzar de una vez por todas los grandes planes de I+D+i. Se dan subvenciones a planes de I+D+i, pero no existe un seguimiento auténtico de cómo se emplean estas ayudas. En mi opinión, en el ámbito de la innovación resulta fundamental chequear cuál es el impacto que han generado los productos o servicios que se han puesto en marcha con esos apoyos administrativos.

Concretamente, se trata de preguntar: ¿qué productos o servicios finales se han conseguido?. Pienso que se apoya mucho -y se debe seguir apoyando- a los centros tecnológicos, que se apoya menos a las empresas que hacen esfuerzos en I+D y que no se evalúan suficientemente las iniciativas existentes para potenciar la innovación. Se tiene la sensación de que, se invierta mucho o poco en este campo, los resultados siempre son escasos y, en no pocas ocasiones, éstos ni se revisan."

- ¿Cómo se contempla la I +D+i en S21sec?

- S21sec es una empresa de investigación y quiere ser un Centro de Excelencia en Seguridad Telemática. Más del 40% de nuestros recursos los dedicamos a la I+D+i y este elevado nivel inversor nos permite ofrecer unos servicios de alta calidad y maximizar el nivel de seguridad de las organizaciones.

S21sec trabaja bajo la premisa de que "la seguridad no es cara, sino que lo que resulta muy costoso es la falta de seguridad". En este sentido, e independientemente de su tamaño, Xabier Mitxelena considera que toda aquella compañía en la que la información sea un activo importante ha de introducir el factor seguridad en sus procesos empresariales con el objetivo de proteger sus activos digitales. Con este objetivo básico, S21sec ofrece a las compañías un amplio catálogo de servicios, entre los que destacan los siguientes: gestión y análisis de vulnerabilidades; almacenamiento y gestión de logs; servicios continuos 24x7; monitorización de sistemas de gestión y correlación de eventos, prevención y gestión de alertas,



análisis forense; vigilancia digital; evaluación de seguridad de los sistemas de información; elaboración de un Plan Director de Seguridad; Implantación de la Norma de Seguridad ISO 17799; y, finalmente, acciones formativas.

- De los productos y servicios desarrollados por su empresa, ¿cuáles son, en su opinión, los más relevantes?

- Toda nuestra estrategia está volcada en ofrecer a nuestros clientes un servicio de seguridad preventivo para su empresa. Bajo este prisma, hemos desarrollado un producto que se llama HIVE, que es lo que se conoce como una Pasarela de Control de Transacciones Web.

Es un producto que está orientado a proteger las aplicaciones web de una empresa en su nivel 7, que es el nivel de la aplicación, ya que es aquí, en las aplicaciones, donde hoy en día, en Internet, se concentra el mayor nivel de riesgo. También hemos desarrollado, junto con Bankinter, Bitácora, que es un sistema de gestión, de centralización de logs y de correlación de eventos que, en mi opinión, es el corazón de lo que en futuro habrá de ser nuestro centro de seguridad. También tenemos en marcha un proyecto que se llama Vulnera, que es un sistema de información de todos los nuevos problemas de seguridad que van surgiendo en el tiempo y que en este momento ya recoge más de 15.000 incidentes, archivados tanto en castellano como en inglés. Vulnera, además, nos está sirviendo como un motor para evaluar los niveles de riesgo de nuestros clientes y, en conjunción con lo que es Bitácora, nos permite proporcionar un eficaz servicio preventivo. Con esta base de partida en S21sec estamos poniendo en marcha el primer centro nacional de seguridad, S.O.C. (Security Operation Center), desde el cual ofrecemos a nuestros clientes servicios preventivos y evolutivos de seguridad.

Gracias a esta centralización se garantiza una optimización de la gestión del conocimiento en beneficio del usuario final. En este sentido tenemos además relación directa con otros S.O.C. a nivel internacional que nos aportan una correlación mayor y, sobre todo, un acceso inmediato al conocimiento de los nuevos tipos de riesgo que van surgiendo. Por ejemplo, esto nos permite un servicio de especialización en sectores tan críticos como el financiero.



“Sería conveniente poner en marcha una mesa de actuación en la que reunirnos todos los agentes sociales para encauzar el concepto de la seguridad informática en el ámbito universitario”

- ¿Qué papel desempeña la formación dentro de S21sec?

- Creo que resulta llamativo que la seguridad telemática todavía no esté contemplada en los programas de las diferentes universidades. Dentro de nuestras posibilidades, hemos puesto en marcha, en colaboración con Vicontech, ciclos formativos orientados a los centros de formación de formación profesional. Por otro lado, hemos desarrollado programas de formación que per-

miten certificar a las personas y a las empresas e intentamos transmitir a nuestros clientes algo tan esencial como que la cultura de la seguridad debe alcanzar a todo el personal de la empresa.

Intentamos también que la relación con las universidades sea fluida. Ya he hablado del I Master en Comercio Electrónico que pusimos en marcha junto con la Universidad de Deusto de San Sebastián, pero, por ejemplo, también hacemos trabajos de investigación con la Universidad del País Vasco o con la Universidad de Mondragón. Por otra parte, y en colaboración con la Diputación Foral de Gipuzkoa, mantenemos los programas de Miramon Digital (que se han extendió a los parque tecnológicos de Zamudio y Miñano) un concepto de formación para los agentes sociales y económicos del territorio en el que la seguridad es un aspecto muy importante del programa. De cualquier forma, creo que sería conveniente poner en marcha una mesa de actuación en la que deberíamos reunirnos todos los agentes sociales para decidir cómo encauzar el concepto de la seguridad informática en el ámbito universitario.

- Actualmente, ¿en qué momento de su desarrollo se encuentra S21sec?

- En estos momentos, en S21sec nos encontramos definiendo lo que para nosotros significa ser un gran Centro de Excelencia de la

Seguridad Telemática: un lugar en el que exista I+D+i, en el que la empresa desarrolle todo su potencial y que esté acompañado de un ciclo de formación directa con la universidad. Además de la puesta en marcha del S.O.C., que supone una fuerte inversión y nos reafirma en una posición de servicio avanzado diferencial en materia de seguridad telemática.

- Por su experiencia, ¿cuáles son los principales riesgos de seguridad que acechan a las empresas en Internet?

- Accesos ilegales, robos de información, fraudes, daños a los sistemas informáticos, denegación de servicios e inoculación de virus. Todo esto lleva a las empresas a importantes pérdidas económicas y de productividad, a padecer la desconfianza de sus clientes y de sus proveedores, e, incluso, a ser objeto de acciones legales en su contra.

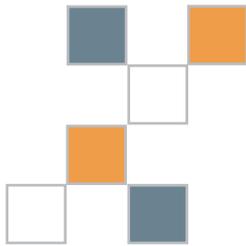
- Y desde un punto de vista más global, ¿cuáles son los delitos más importantes que pueden producirse a través de las redes telemáticas?

- Hoy en día, existen tres grandes tipos de delitos que pueden producirse a través de Internet (o dentro de las propias organizaciones): el fraude económico y financiero, que intenta atacar a las empresas o a los clientes de éstas; el espionaje, que puede ser tanto de carácter interno como externo; y el ciberterrorismo, que se aprovecha de que, en la actualidad, todos los sistemas que se consideran vitales para la existencia de nuestras sociedades, electricidad, agua, energía, etc, se sostienen sobre redes informáticas. Por ello, que alguien te pueda hacer caer un sistema de estas características es una posibilidad que entraña un alto riesgo.

- ¿Qué espacio ocupa hoy S21sec en el sector europeo de la seguridad telemática?

- A nivel del País Vasco y a escala nacional creo que S21sec es una referencia, sobre todo en lo que toca a su modelo de empresa. Desde un punto de vista internacional, somos una empresa más. Todavía no podemos decir que hayamos realizado un proceso importante de internacionalización, aunque sí podemos señalar que comenzamos a ser conocidos por alguna de las tecnologías que hemos desarrollado y con la que estamos intentado llegar a los mercados internacionales.





Ubicación: Donostia

Página web: www.s21.com

Año de Constitución: 2000

Número de personas: 80

Actividad Principal: DiS21sec es una compañía especializada en ayudar a las empresas a alcanzar el grado de seguridad telemática necesario para desarrollar con éxito su negocio. La compañía recibió el premio Start-up 2000 de McKinsey & Company a la mejor idea empresarial de Consultoría de Seguridad Informática en Internet. Tiene una empresa filial: Encriptalia.

Tfn: 943317330

Fax: 943317476

E-mail: info@s21.com

Web: www.s21sec.com

Dirección: Parque Empresarial Zuatsu.
Edificio Urgull. N° 3. Planta 2ª. Local N°10
20018 San Sebastián