AURACRYPT SYSTEMS[1]

LA EMPRESA

A mediados de 2022, en Auracrypt Systems tenían listo su plan de negocio, elemento imprescindible para conseguir los fondos necesarios para lanzarse al mercado europeo.

Auracrypt Systems era una compañía dedicada a la fabricación de equipos de seguridad informática, que nació de la experiencia en proyectos de consultoría de seguridad de sus dos fundadores: Nacho Pérez y José Luis Trávelez.

Ambos llevaban casi dos años juntos, trabajando de forma autónoma como fabricantes de un pequeño equipo de seguridad y no se decidieron a constituir Auracrypt Systems hasta mediados de 2021, cuando creyeron que su negocio comenzaba a asentarse. José Luis era físico, tenía 45 años y, desde sus comienzos en el mundo laboral, se había centrado en sistemas informáticos. Siendo muy joven, como respuestas a la aparición de "ILoveYou", un *malware* de los más dañinos, con alta capacidad de propagación, programó en un tiempo récord de tres días el antivirus "IKillYou", que repartió gratuitamente.

Por su parte, Nacho tenía 43 años, era ingeniero industrial, MBA y un excelente organizador. También había trabajado en proyectos informáticos en empresas de *software*. Era muy creativo, un gran conocedor del sector y de los entresijos de los departamentos de I+D en el sector informático.

EL ORIGEN DE LA IDEA

Teniendo en cuenta que las grandes empresas tenían la capacidad de acceder a proyectos costosos de consultoría informática para resolver sus problemas de ciberseguridad con aplicaciones desarrolladas a medida, decidieron probar suerte diseñando un pequeño sistema específico, tipo *firewall*[2].

---

[1] Caso de la División de Investigación de San Telmo Business School, España. Preparado por el profesor Josep Mor Figueras, con la colaboración del profesor Isauro Lopez Polo, ambos de San Telmo Business School, para su uso en clase, y no como ilustración de la gestión, adecuada o inadecuada, de una situación determinada.

[2] Un *firewall* es un dispositivo de seguridad de red que monitoriza el tráfico entrante y saliente y decide si debe permitir o bloquear un elemento específico en función de un conjunto de restricciones de seguridad

Para desarrollar este sistema se autoimpusieron unas especificaciones muy concretas y sencillas: sería un dispositivo de *hardware*, se auto instalaría como cualquier aplicación, debía adaptarse a todas las situaciones de ciberseguridad y entrar en el mercado con un precio cercano a los 1.000 €, que era lo que costaba de media un ordenador personal de sobremesa estándar en 2022. Como tenían claro que el suyo era un mercado en deflación, sus equipos deberían ser capaces de seguir la evolución de los precios de este tipo de ordenadores personales. El equipo estaba específicamente dirigido a pymes, que quedaban fuera del negocio de las grandes firmas proveedoras de seguridad.

La compañía, hasta entonces, tenía un sistema de producción muy simple: una vez recibido cada encargo, se compraban unidades compactas de CPU, memorias —según la versión y potencia instalada— y discos duros (HDD o SDD). Mientras uno de los técnicos montaba las memorias, se hacía una copia del programa en otro equipo, se instalaba el sistema operativo y después se encajaba la unidad HDD/SDD en la CPU. Todo este proceso de fabricación duraba unos 15 minutos.

EL SECRETO DEL PRODUCTO

Para conseguir el bajo precio de salida del equipo, habían pensado emplear dos métodos completamente distintos a los que eran habituales en aquel momento en el sector: (i) por un lado, el uso de lenguajes de código abierto para la programación y por otro, (ii) trabajar con un paradigma diferente a la competencia para evitar las costosas labores de mantenimiento y mejoras.

Finalmente, aplicando estas dos ideas, consiguieron encontrar la forma de romper con el patrón de funcionamiento de los *firewalls* habituales, realizando dos cambios por los que nadie más en el sector habría apostado:

1. En lugar de *software,* ellos ofrecían un dispositivo *hardware*, lo que permitiría utilizar un solo equipo para toda una red de ordenadores. Este equipo se conectaría en la entrada de la señal y filtraría todo tráfico de datos de la red de ordenadores en ambos sentidos.
2. En lugar de trabajar, como era habitual, identificando patrones de comportamiento de los virus, lo que incluía describirlos, parametrizarlos y finalmente mantener los correspondientes antivirus operativos, su equipo "aprendería la normalidad" de la red a la que protegía, de forma que no fuera necesario evitar más que aquello que no fuese normal. Para ello utilizaban un sistema de IA entrenada al efecto.

previamente definidas. Los *firewalls* habían sido la primera línea de defensa en seguridad de la red durante los últimos 25 años. Su función es establecer una barrera entre las redes internas seguras, controladas y fiables y las redes externas poco fiables, como Internet. Un *firewall* puede ser un dispositivo de *hardware*, de *software* o ambos.

Bajo estas premisas consiguieron desarrollar un equipo muy versátil que a mediados de 2022 había resistido millones de ataques de *hackers* sin que nadie hubiera conseguido traspasar la barrera de seguridad[3].

EL MERCADO

Como reconocimiento a los logros obtenidos y las posibilidades del producto, la compañía Oracle les propuso fabricar el equipo bajo una marca conjunta que identificara tanto a Auracrypt Systems como a Oracle y comercializarlo a través de su distribuidora para toda Europa. El pacto no implicaba exclusividad por ninguna de las dos partes, por lo que Auracrypt Systems podría ofrecer el mismo equipo, con su marca exclusiva, y distribuirlo por los canales que estimase oportunos.

Para Auracrypt Systems, la alianza con Oracle constituía la posibilidad de desarrollar más rápidamente nuevos equipos y utilidades, enfocarse en el *software*, llegar a nuevos mercados en un plazo menor al que habían imaginado y crecer a mayor velocidad, lo que en el sector de la tecnología tenía una importancia vital. En su plan de desarrollo, Auracrypt Systems tenía pensado ampliar la gama de productos con aplicaciones de ciberseguridad completas: antivirus, anti-*spam*, y similares. Con esta alianza, la empresa tenía la posibilidad de enfocarse "en lo suyo" y esperaba aprovecharla para que la salida al mercado de las nuevas versiones y aplicaciones fuese más rápida.

Todas estas ventajas serían posibles porque Oracle se hacía cargo de la producción de equipos, en sus propias plantas, utilizando únicamente un sistema de *software* máster que Auracrypt Systems les proporcionaba junto con un sistema que actuaba de contador de las copias realizadas.

Por otro lado, todas las tareas de preventa, venta y distribución para todos los países de Europa quedaban también en manos de Oracle. Auracrypt Systems debía encargarse, no obstante, de todas las operaciones de posventa relacionadas con el *software* y de atender las reclamaciones relativas al funcionamiento de los equipos en lo relativo al *software*.

Aunque la compañía quedaba descargada de una parte de los procesos, debían solucionar el problema de financiar todo el crecimiento comercial que esperaban, ya que, fruto de esta alianza, José Luis y Nacho preveían la necesidad de abrir entre tres y cuatro oficinas comerciales en países de la Unión Europea, contratar a varios comerciales multilingües y desarrollar un servicio de soporte para distintos países.

[3] AuraCrypt retó de forma pública a los *hackers*, conectando a Internet seis sistemas de seguridad: uno de su marca y cinco más de competidores de primeras marcas internacionales (entre lo que se encontraban Microsoft y Cisco). Los seis sistemas se habían configurado para proteger varios archivos. El reto consistía en burlar la protección del suyo; quien fuese capaz de atravesar su barrera, recibiría un premio de 10.000 € pagaderos, bajo control notarial, por el Banco Sabadell, que actuó como patrocinador. Durante un año y medio, el equipo estuvo expuesto a millones de ataques sin que nadie consiguiera abrir aquellos archivos que protegía. Los otros equipos resistieron entre 80.000 y 300.000 ataques antes de ser vulnerados.