Vídeo Jorge Pariente
Fotografía Jorge Pariente
Texto Rufino Contreras

ÓSCAR FLOR, TRUST SOLUTION MANAGER DE WISE SECURITY GLOBAL

"MEE es un ciber notario"

<< Las notificaciones por medios electrónicos son una realidad que ha venido para quedarse. Las organizaciones tienen la imperiosa necesidad de certificar estas notificaciones, de poder demostrar que se han emitido y que han llegado. Esto hace que la evidencia digital certificada sea cada vez más relevante. Wise Security Global es una empresa de ciberseguridad y ciberconfianza especializada en este campo, como relata Óscar Flor, Trust Solution Manager de la compañía.

¿Qué es Wise, a qué mercado se dirige?
Wise Security Global tiene dos líneas principales de negocio: Cybersecurity y Cybertrust. La primera está centrada en la ciberseguridad, la prevención de amenazas, y está constituida por equipos de hackers que se dedican a 'romper' barreras de seguridad. Especialistas que pueden atacar una aplicación y detectar sus debilidades para ayudar a las empresas a solventarlas. Esta división también monitoriza. Colocamos sondas y visualizamos lo que ocurre en ese tráfico de red para comprobar si hay algo sospechoso… Si detectamos algún tipo de amenaza, la resolvemos y avisamos a la compañía. En tercer término incluimos 'CISO as a service'. Si bien todas las empresas importantes cuentan con este rol interno, no siempre abarca todas sus necesidades y nosotros ofrecemos un especialista que sí lo cubra.

¿Y qué puede contar de Cybertrust?
Tenemos productos que giran en torno a la criptografía: firmas electrónicas, notificaciones, facturas y tickets electrónicos… Para todo aquello que requiere una capa de criptografía y de confianza, tenemos un producto correspondiente.

¿Qué importancia tiene cada una de las divisiones?
A día de hoy es del 50% para cada una. Cybertrust, por naturaleza, genera más soluciones innovadoras que se pueden trasladar al mercado con mayor escalabilidad, pero el peso específico de cada área está en equilibrio. De hecho, se unen cada vez más en proyectos ya que la fusión de ambas logra alcanzar entornos ciberseguros y confiables.

¿Hablamos de gran cuenta?
Nuestros clientes son gran y mediana empresa, aunque nuestro objetivo es democratizar la ciberseguridad y ampliar nuestro foco en la pyme. Normalmente, nuestro cliente es grande y requiere un equipo de desarrollo para poder integrar nuestros servicios en sus sistemas. No es algo que te pongo y me voy. Vendemos framework, funcionalidades… y por ello tiene que haber un equipo de programadores en el lado del cliente.

¿Cómo define la evidencia digital?
Una evidencia digital es una prueba de un hecho. Es un documento, un email, una traza de un log de una determinada aplicación. Son metadatos, una fecha de cuando ha ocurrido algo, son tu nombre y apellidos… Nuestro objetivo con estas pruebas es recabarlas y certificarlas. Existe necesidad en el mercado de poder probar cosas y para ello es preciso tener evidencias de que se han producido.

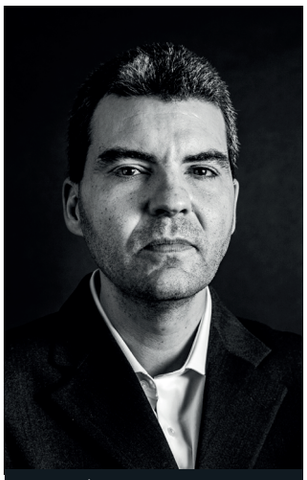
Algo muy indicado para las notarías…
Nuestra solución MEE supone un gran apoyo al notario tradicional ya que respalda sus operaciones y las dota de valor añadido. Como Tercero de Confianza otorgamos más fiabilidad si cabe a la custodia y registro de información.

¿Cómo es la conversación con los clientes de Wise?, ¿quién marca las pautas?
Normalmente, la empresa ya sabe lo que necesita, porque entramos a raíz de un problema. Nuestro primer cliente de notificaciones electrónicas certificadas fue una compañía que se encargaba de gestionar las rutas de los pilotos de vuelos comerciales. Les enviaba un SMS indicando la fecha y hora de su vuelo. En algunas ocasiones, el piloto no se presentaba, lo cual llevaba a un cúmulo de problemas. Dicho trabajador podía negar haber recibido el mensaje y la compañía aérea necesitaba demostrar que sí se le había entregado. Un SMS per sé no es una prueba, y nosotros hemos ideado un proceso completo de certificación. Nuestro producto da las garantías de que se ha enviado, entregado y leído.

¿Cómo 'aterriza' en el cliente su solución?
En grandes empresas lo habitual es que integren nuestros servicios en su ERP o herramientas corporativas, para lo que no es necesario ningún tipo de implantación (todo el servicio es oncloud). Wise proporciona servicios y el cliente automatiza los procesos. Para mediana empresa que no tenga estas capacidades de integración ofrecemos un portal web sencillo. Para certificar, nosotros somos los que enviamos y recabamos todas las evidencias del proceso: Enviamos el SMS con las credenciales de quién envía y con las trazas que nos sirve el operador. Con todos estos datos confeccionamos un acta certificada en PDF, que va acumulando trazas. Cuando tengo esa acta que prueba el envío, certifico el PDF, firmándolo electrónicamente para darle autenticidad, y luego pedimos a un tercero un sello de tiempo. Algo a destacar de nuestro servicio es que certifica cada estado (envío, recepción y lectura). Cada uno de ellos en diferentes momentos de tiempo y todos ellos con sus trazas correspondientes, sus firmas electrónicas y sus sellados de tiempo. Esto nos diferencia de la competencia (que sólo certifican al finalizar).

¿Cómo sigue el proceso?
Solicitamos al operador que envíe el SMS, cuando el envío está realizado nos avisa. Nos vuelve a avisar cuando el SMS ha sido entregado. Por último, la confirmación de lectura es una funcionalidad extra que proporciona nuestro servicio en base a un link en el SMS. Cuando el usuario pincha en el link sabemos que lo ha leído. El acta certificada va incorporando todos estos pasos.

¿Y por qué recurre Wise a blockchain?
Ofrecemos un documento autocontenido y autoverificable con suficientes garantías legales a raíz de las firmas electrónicas. Pero quisimos darle una capa extra. Una vez que tenemos el acta que hemos comentado, generamos una huella de esa acta y la incrustamos en la cadena de bloques. Después incorporamos al documento la dirección del bloque de la cadena como una prueba más, la huella del acta permanece inalterable por la propia naturaleza de blockchain. ■



¿CUÁL ES SU PERFIL DE CLIENTE?

Tenemos Administración Pública (ayuntamientos, puertos, ministerios…) debido al impulso de las sedes electrónicas, que permiten tramitar expedientes online y que requieren herramientas que nos doten de esos procesos criptográficos. Si la AAPP me va a comunicar algo de manera telemática, tiene que dar garantía fehaciente de que la comunicación se ha producido. Todos esos procesos burocráticos requieren de nuestras herramientas. La banca es un sector muy preocupado por la seguridad, especialmente en lo referido a la banca online. Las aseguradoras son empresas que tienen mucha relación con el cliente final y tienen que comunicar información. Antes se enviaba la documentación de una póliza en un sobre al domicilio del usuario, que en muchos casos no la devolvía firmada. Ahora, mediante sistemas de on boarding, se resuelve esta ineficiencia.