**Albert Morell,
QSA, Director and Co-founder
de A2SECURE**

Albert Morell, con más de 12 años de experiencia en Ciberseguridad y con una sólida formación técnica en ingeniería, comercio electrónico y criptografía, abandonó la industria de las telecomunicaciones para emprender el empeño empresarial de cofundar su empresa de ciberseguridad centrada en la seguridad digital y en la normativa PCI-DSS.

Entrevista a Albert Morell,
QSA, Director and Co-founder de A2SECURE

“Nuestra vocación es, a partir de nuestro trabajo, convertirnos en los referentes de ciberseguridad de nuestros clientes...”

A2SECURE ha otorgado a algunas de las principales empresas europeas, especialmente en la industria de pasarelas de pago y el sector turístico, un servicio destacado en información y seguridad corporativa, así como consultoría y auditoría de la normativa PCI-DSS.

¿En qué consiste la normativa PCI-DSS de IATA?
Antes de explicar en qué consiste la normativa PCI-DSS creo que es importante poner en contexto las cosas. Actualmente al año aproximadamente se realizan más de 100 Mil Millones de transacciones con tarjetas de crédito y débito a nivel mundial. Éste, es un método de pago muy versátil y cómodo el cual sigue en crecimiento pero que su principal riesgo de crecimiento, es la falta de confianza por parte de la sociedad por los riesgos que entraña de seguridad, como robos y fraudes, que están a la orden del día.
Con el objetivo de mitigar estos riesgos y favorecer el uso de este medio de pago, así como aumentar el negocio de tarjetas, las principales marcas de tarjetas (Visa, MasterCard, Discover) desarrollaron ya hace unos años un estándar de seguridad, PCI-DSS, principalmente enfocado en proteger los datos e las tarjetas, que ha ido madurando a lo largo del tiempo. Teniendo en cuenta esta premisa, la normativa para nada es de la IATA, sino del Council formado por las marcas de tarjetas. IATA lo hace suyo ya que como cualquier empresa que manipula datos de tarjetas, como son las aerolíneas, deben de cumplir con PCI-DSS por exigencia de las marcas y de los bancos con los que trabajan.

Hay una fecha límite hasta el 1 de marzo. ¿Cree que se podrá prolongar?
Bajo nuestro punto de vista y basado en nuestra experiencia en otros sectores expuestos a la normativa PCI-DSS, lo importante no es la fecha límite y si esta se va a prolongar o no, lo importante es empezar a trabajar desde ya en la adaptación a la normativa. Esta normativa viene para quedarse, es una normativa que, en algunos casos y escenarios, puede ser bastante compleja, y esperar a prorrogas ampliaciones de la fecha límite, etc. no es la estrategia adecuada.
Nuestra visión es, empezar y llegada la petición por parte de IATA, ser capaces de mostrar el trabajo realizado, es decir, donde estamos y donde y cuando queremos llegar en caso de no tener el objetivo cumplido. Creemos que esta estrategia es más que posible que, frente a la IATA, pueda permitir extender el plazo de cumplimiento.
Asociado a esto, también me gustaría reforzar el mensaje que PCI-DSS es una normativa por un lado tecnológica y por otro de procedimientos y políticas, por esta razón, no hay que verlo como un proceso de certificación, que en el mejor de los casos podría completarse el 1 de marzo, sino en una serie de cambios de procedimientos y de manera de trabajar que tendrán que mantenerse en el tiempo, así como actividades regulares de mantenimiento.

¿Por dónde hay que empezar?
PCI-DSS es una normativa complicada en muchos casos y mucho más complicada sino se entiende correctamente y se coge la documentación oficial. Para nosotros, la mejor forma de empezar es, contactar con una empresa especializada en procesos de adaptación a la normativa PCI-DSS para obtener asesoramiento. A partir de ahí, el primer trabajo que deben de hacer todas las empresas que manipulan tarjetas es poder responder a tres preguntas básicas: 1.¿Cómo manipulo datos de tarjetas de crédito (canales de entrada y salidas)?; 2. ¿Almaceno datos de tarjetas (en mis sistemas o en sistemas de terceros)? y 3. ¿Necesito realmente almacenar los datos? y en caso necesario, ¿Por cuánto tiempo?. Básicamente con la información obtenida de estas tres preguntas, será posible saber a cuál de los escenarios de PCI-DSS se enfrenta la empresa y que requerimientos le aplican a la empresa, cuales a sus proveedores y cuales directamente no le aplican.

Háblenos de su empresa A2SECURE
Somos una empresa de servicios de ciberseguridad enfocada en ayudar a nuestros clientes a mejorar su seguridad de una forma efectiva, y donde nuestros clientes en todo momento, entiendan los que les proponemos y hacemos, para que sean parte esencial y partícipes en todo momento del cambio. Cuando nadie invertía en nada a los inicios de la fuerte crisis que estamos superando, nosotros nacimos, ofreciendo todo tipo de servicios, que empresas en esos momentos necesitaban y seguimos con la misma filosofía, acercar la ciberseguridad a cualquier tipo de empresa ya que estamos en un mundo global donde cualquiera puede verse afectado por un incidente de seguridad.
Nuestra vocación es, a partir de nuestro trabajo, convertirnos en los referentes de ciberseguridad de nuestros clientes y de ahí, ser un referente Europeo de la Ciberseguridad.

¿Cuál es el futuro de la seguridad digital?
Lo que comúnmente la gente piensa o lee en las noticias como el futuro y los riesgos de ciberseguridad, en realidad ya es el presente o incluso el pasado. Nuestras vidas están actualmente conectadas a Internet las 24 horas a través de dispositivos, como móviles que saben en qué locales estas y te lanzan publicidad de los mismos, dispositivos como TV conectadas permanentemente a Internet, relojes, lavadoras que se programan a distancia y podríamos seguir y seguir… Cada día se publican nuevas vulnerabilidades de alto riesgo para todo tipo de sistemas, aparecen noticias de ciberdelincuencia… El futuro y el presente es un mundo cambiante con riesgos en los que, de manera permanente, debemos de trabajar.
Así para nosotros el futuro de la seguridad digital es, entender que debemos de entrar en un proceso continuo de análisis de riesgo y actuación para en la medida de lo posible, mitigar los riesgos detectados, y no dejar de repetir y repetir este proceso a lo largo del tiempo.
Es importante olvidar el paradigma de causa-reacción, es decir, existen virus, la reacción es instalar un antivirus, y empezar a trabajar con el prisma de, qué está pasando ahí fuera, cómo evoluciona y cómo puedo mitigarlo o reducirlo en mi escenario y en mi negocio. En el ejemplo anterior de la existencia de virus, el prisma es, busco un antivirus y regularmente controlo si hay algo más, si me sigue protegiendo o si debo de tomar nuevas medidas… Los riesgos están ahí y seguirán apareciendo y debemos de entrar en esa dinámica para protegernos adecuadamente.

¿Qué otros servicios ofrecen?
Como empresa de ciberseguridad ofrecemos distintos servicios a nuestros clientes como son, proyectos de control de riesgos de ciberseguridad, proyectos de hacking ético para evaluar la seguridad de nuestros clientes frente a un ataque, análisis de vulnerabilidades de sus sistemas, formación y concienciación en seguridad, proyectos de GDRP y como no, proyectos de adaptación y auditoría PCI-DSS, dado que somos una de las empresas certificada como QSA por el Council PCI. Les invito a visitar nuestra web, www.a2secure.com, para conocer un poco más de nosotros.

¿Cuáles son sus principales clientes?
Nuestra tipología de clientes es muy diversa, tenemos clientes del sector consumo, de telecomunicaciones, aerolíneas, pasarelas de pago, y muchos clientes del sector turístico desde hoteles, motores de búsqueda, agencias on-line y físicas. Nuestros servicios son de aplicabilidad a cualquier empresa ya que hoy en día todas las empresas requieren de tecnología, conectividad, Internet y aunque todavía a la gente le cuesta entender, cualquiera puede ser blanco de un ataque, ya que la gran parte de ellos no se tratan de ataques dirigidos, sino indiscriminados, a veces simplemente en busca de recursos para realizar ataques más sofisticados.

¿Qué recomendarían a las agencias de viajes y a sus clientes para estar tranquilos en cuanto a seguridad digital se refiere?
Muy sencillo, su negocio es vender viajes y el nuestro es ayudar a nuestros clientes a controlar su seguridad. Con esto quiero decir que, lo importante es que cada uno se centre en los que mejor sabe hacer y cuente con ayuda de terceros para las cosas que no son propias de su sector y negocio. Por poner un ejemplo, a nosotros nos viene muy bien tener un acuerdo con agencia para que nos gestione nuestros desplazamientos, son especialistas, nos cuidan, nos ofrecen lo que necesitamos y no tenemos que preocuparnos. Pues pretender que en el mundo hacia el que vamos, las agencias de viajes gestionen su propia seguridad, nosotros entendemos que es perder el foco de su negocio. Podemos ayudarles a que esto no sea así.

¿Le gustaría añadir alguna cosa más?
Por mi parte simplemente agradecerles la oportunidad que nos bridan de presentarnos en esta entrevista, así como de expresar un poco nuestra visión sobre la ciberseguridad.