OLOF SANDSTROM, DIRECTOR DE OPERACIONES DE ARSYS

"Arsys siempre ha hecho de la seguridad uno de sus pilares estratégicos"

OLOF SANDSTROM SE INCORPORÓ A ARSYS EN 2006, CUANDO COMENZABA A GESTARSE LA REVOLUCIÓN DE CLOUD COMPUTING. DIEZ AÑOS DESPUÉS, CUENTA A CSO COMO HA SIDO EL VIAJE DEL PROVEEDOR A LA NUBE DESDE EL PUNTO DE VISTA DE LA SEGURIDAD.

MARIO MORENO

Desde su llegada a Arsys ha sido testigo de primera mano de la transición de la compañía a la nube hasta liderar el mercado español como proveedor de servicios cloud computing ¿Cómo se ha vivido el cambio desde la división de seguridad?

Cuando me incorporé como director de seguridad en 2006 el sector tecnológico empezaba a sentar las bases de la revolución Cloud que hemos vivido en los últimos años. La consecuencia de este viaje hacia la nube ha sido un cambio total en la concepción de la seguridad IT, más desde el concepto del propio usuario que desde el punto de vista de los proveedores. Como usuarios, el cambio ha sido radical porque hemos decidido utilizar los servicios en Cloud de una manera que los conceptos tradicionales se han visto desbordados. Por ejemplo, hace muy poco tiempo, nos escandalizábamos si una empresa hacía un uso poco adecuado de nuestros datos personales y ahora, no tenemos reparos en colgar nuestro currículum con todos nuestros datos personales y ponerlo a disposición de todo aquel que quiera consultarlo. Tampoco tenemos hoy inconvenientes en conectar nuestros equipos profesionales en redes Wi-fi públicas y empezar a trabajar con total normalidad.

Y, ¿cómo ha sido la evolución desde el punto de vista del proveedor?

En realidad, Arsys siempre ha tenido la seguridad como uno de sus pilares estratégicos. Y, realmente no ha cambiado tanto respecto a antes del cloud. El malware, los ataques de denegación de servicios y otras muchas amenazas siempre han estado ahí, y siempre hemos destinado todos nuestros recursos para neutralizarlos. Lo único que hemos debido hacer ha sido modificar el enfoque. Hemos pasado de abordar la seguridad de una forma departamental a hacerlo de manera integral. En 2010 aunamos en Operaciones los principales departamentos, que de una forma u otra, participaban en aspectos como la seguridad IT y física, la eficiencia energética o la disponibilidad.

Las compañías se están subiendo en masa a la nube; ¿qué tipo de seguridad demandan?

Tenemos las habituales medidas de seguridad que aplicamos a nuestros servicios por defecto, tanto del centro de datos como de las plataformas. Es decir, los sistemas de redundancia, monitorización, segregación y aislamiento que deben implementarse sobre las cinco capas que componen todo proyecto Cloud: software, capacidad de computación, almacenamiento, redes y data centers. En esas capas influyen múltiples elementos. Sólo por citar algunos de ellos, hablaríamos de diferentes tecnologías como firewalls, anti-malware, sistemas de detección y prevención de intrusos, sistemas SIEM de gestión y correlación de eventos para el análisis en tiempo real, redun-

“Los usuarios hemos decidido utilizar los servicios en la nube de una manera que los conceptos tradicionales se han visto desbordados

“El volumen de ataques que recibe cualquier servidor que esté conectado a Internet es muy alto y totalmente indiscriminado”

dancia de conectividad, de hardware, de suministro eléctrico (centros de transformación, SAI y grupos electrógenos) y climatización (enfriadoras, bombas de impulsión...), acceso biométrico, sistemas de extinción de incendios de gas, SCADA ... Y, por encima de ellos, el elemento más importante, la prevención y el equipo humano que está detrás, gestionando y monitorizando la infraestructura y aplicando su experiencia a los datos que nos proporcionan los sistemas.

En definitiva, cloud computing deriva en multitud de retos tanto para proveedores, empresas y usuarios finales.

Los usuarios hemos cambiado nuestros hábitos de consumo IT y ahora accedemos más tiempo a servicios distintos y desde más dispositivos. Esto implica que no podemos seguir cuestionando la seguridad hoy en día tal y como lo hacíamos hace una década. Hoy, por ejemplo, no tiene mucho sentido que hablemos de asegurar un perímetro porque tal perímetro ya no existe (o como mínimo está bastante difuso) y tenemos usuarios con varios dispositivos (muchos de ellos personales) y los datos que deben estar almacenados en algún lugar al que se pueda acceder fácilmente desde cualquier sitio. Esto nos obliga a cambiar nuestro enfoque y ser más creativos en nuestro día a día como garantes de la seguridad IT de nuestras organizaciones, compaginando las medidas de seguridad con la usabilidad de los servicios digitales.

Esto, indefectiblemente, pasa por formar y concienciar a los usuarios de los riesgos a los que pueden exponer a su empresa cuando no securizan sus dispositivos móviles ni utilizan contraseñas de calidad, o llevan una base de datos de clientes en un móvil sin medidas de cifrado, o la cuelgan en cualquier servicio online del que no tienen garantía. No podemos olvidar que, en la inmensa mayoría de los casos, el eslabón más débil de la seguridad IT de cualquier empresa es el propio usuario.

¿Cuáles son las amenazas a las que hay que hacer frente en la actualidad?

Ahora mismo, el volumen de ataques que recibe cualquier servidor que esté conectado a Internet es muy alto y totalmente indiscriminado. En la mayoría de las ocasiones los “malos” no atacan un servidor porque es de una u otra empresa. Lo hacen simplemente porque está disponible y es vulnerable. Son este tipo de ataques indiscriminados los que ocupan actualmente la mayor parte de nuestro tiempo y los que generan mayores preocupaciones a nuestros clientes.

Los ataques de denegación de servicio (DDoS) están reflejando un crecimiento significativo en los últimos meses por lo que se requiere una mejora sustancial de la capa de protección frente a este tipo de ataques, manteniendo siempre activo el servicio del cliente.

¿Cuál es la inversión que le dedica Arsys a la seguridad?

Manejamos alrededor de un centenar de iniciativas al año en torno a la seguridad

La seguridad es uno de los pilares sobre los que se sustenta el negocio de Arsys como proveedor de servicios Cloud para empresas. Nunca hemos dejado de invertir en la mejora de nuestros sistemas de seguridad y en proyectos de I+D capaces de mejorar nuestro posicionamiento en esta materia. De hecho, anualmente manejamos alrededor de un centenar de iniciativas en distintas áreas de la empresa, y muchas de ellas están encaminadas a mejorar los principales indicadores de disponibilidad, seguridad, eficiencia energética y niveles de servicio de nuestras soluciones y de nuestros centros de datos.

¿En qué consisten los proyectos europeos TREDISEC y SWEPT y cuál es la participación de Arsys?

El proyecto TREDISEC es una iniciativa de la Comisión Europea para abordar de una manera integral los principales aspectos de seguridad del Cloud Computing y desarrollar procedimientos y soluciones que combinen seguridad, eficiencia y funcionalidades técnicas, facilitando la adopción de la Nube entre las empresas europeas. En este proyecto Arsys colabora aportando un caso de uso con una de sus plataformas de almacenamiento en la Nube (Cloud Storage), así como liderando el análisis de las posibles estrategias de explotación y posibles modelos de negocio que todas las primitivas de seguridad desarrolladas en este proyecto pueden tener comercialmente.

Por su parte, SWEPT es un proyecto destinado a facilitar a las pymes europeas una presencia más segura en Internet, aunque no tengan excesivos conocimientos tecnológicos. Para ello, su principal hito es el desarrollo de una aplicación online, que está disponible en versión beta desde el 30 de noviembre, y que permite a las pymes gestionar la seguridad de sus páginas web desde un enfoque multifacético, basado tanto en la Detección, al analizar la web para identificar malvare y vulnerabilidades, como en la Prevención, al proteger la aplicación web desde dentro y monitorizar el tráfico de red en tiempo real, y en la Verificación, al comprobar que una web es segura y está correctamente protegida.

Por último, ¿cómo les afecta la nueva normativa Privacy Shield en materia de datos y como puede incidir en los clientes?

Arsys es un proveedor nacido en España cuyas infraestructuras están ubicadas en nuestro país. Eso siempre ha garantizado que nuestros servicios cumplan los niveles de protección que exige la legislación española, que son de los más altos de la UE. Privacy Shield es un acuerdo cuyo objetivo es garantizar que los datos que se transfieran entre Europa y EE.UU. gozan de un nivel de protección equiparable. En ese sentido, no podemos estar más de acuerdo y manifestar nuestra satisfacción ante este tipo de medidas, ya que todo lo que suponga mejorar y ampliar la seguridad de los datos, tanto de empresas como de personas, son pasos en la dirección adecuada. **cso**