Medio: **DEALER WORLD**
Fecha: **19/02/2018**
Página: **1** Documento: **1/7**
Autor: **MABEL CAMPO**

Valor (vpe): **29.000,00€**
Difusión: **9.500**
Audiencia: **38.000**
Ocupación aprox. (%) : **100,00**

Medio: **DEALER WORLD**
Fecha: **19/02/2018**
Página: **2** Documento: **2/7**
Autor: **MABEL CAMPO**
Valor (vpe): **29.000,00€**
Difusión: **9.500**
Audiencia: **38.000**
Ocupación aprox. (%) : **100,00**

La seguridad se ha convertido en el caballo de batalla de todas las empresas, sean del tamaño que sean. Por un lado, la dependencia de Internet abre una puerta, enorme, a numerosos ataques, en muchos casos imprevisibles. Por otra parte, los delincuentes han encontrado otra vía para delinquir y que, en la mayoría de las ocasiones, no está ni legislada. La migración de las aplicaciones y datos a la nube genera mucha incertidumbre en empresas. Los grandes centros de datos remotos suponen para muchos una falta de control que les inquieta. En fin, son muchos los frentes que se les abren a las empresas en cuanto a seguridad se refiere.

Los actuales ataques cibernéticos han incrementado su sofisticación en la era Cloud. Para David Núñez Escobedo, Security Principal Sales Consultant de Oracle Ibérica, "la amenaza de los ataques de día cero —contra una aplicación o sistema que persiguen la ejecución de un código malicioso gracias al conocimiento de vulnerabilidades desconocidas— se está expandiendo a una escala inédita, presionando la capacidad de los investigadores para identificar y prevenir el uso de técnicas basadas en firmas. Esto hace que la detección de anomalías sea la única forma de detectar la aguja en el pajar".

El tipo de amenazas ha cambiado, y Núñez señala: "Ahora, las amenazas son multi vectoriales por el uso de múltiples puntos de entrada y dividiendo la secuencia de ataque en segmentos más pequeños que se vuelven a empaquetar y ejecutar. El área de ataque está ahora claramente dirigida en lugar de ser indiscriminada, lo que hace que la conciencia y atribución del usuario sea de inestimable ayuda en la detección. La capacidad de correlacionar eventos anómalos en la red, en las aplicaciones o en el comportamiento de los usuarios, es clave para efectuar una detección temprana y en su contención", y añade: "Esto desafía la filosofía de defensa basada en la red, ya que se solicitan herramientas para proteger los datos y los activos, de forma que ellos no son capaces de hacer por sí mismos. La identidad es ahora el puente entre los mundos del usuario, las aplicaciones y los controles de red. Es el contexto de identidad combinado con nuevas tecnologías como el aprendizaje automático, Big Data, analítica avanzada, que permite a un profesional de la seguridad centralizar y normalizar las actividades de los usuarios. El resultado facilita la decisión sobre las acciones preventivas que deben desplegarse para defendernos de los ataques actuales y futuros en los planos afectados".

"LA CONCIENCIA DEL USUARIO ES INESTIMABLE PARA DETECTAR LOS ATAQUES. AHORA CLARAMENTE DIGIRIDOS EN LUGAR DE SER INDISCRIMINADOS COMO ANTES"

En este sentido también se manifiesta Sogeti. "El panorama de las tecnologías digitales es complejo. Tratar con múltiples proveedores, múltiples arquitecturas y múltiples *hostings* ha hecho que sea más difícil mantener una visión consistente de las amenazas cibernéticas a todos los niveles. Y esas amenazas están en constante evolución, comentan desde dicha empresa.

Incluso cuando un sistema es seguro, los métodos de prevención tradicionales pueden no detectar todos los fraudes y ataques de cibernéticos. Es por ello por lo que las empresas no pueden permitirse el lujo de dejar que estas amenazas

David Núñez Escobedo, Security Principal Sales Consultant de Oracle Ibérica.

Medio: **DEALER WORLD**
Fecha: **19/02/2018**
Página: **3** Documento: **3/7**
Autor: **MABEL CAMPO**
Valor (vpe): **29.000,00€**
Difusión: **9.500**
Audiencia: **38.000**
Ocupación aprox. (%) : **100,00**

se interpongan en el camino de la transformación", indican las mencionadas fuentes de Sogeti.

Servicios de Seguridad Gestionada

Ante esta situación surge la figura de los Servicios de Seguridad Gestionada, que permiten a las empresas, pequeñas y grandes, acceder a los mejores servicios de forma externa. Pero ¿qué son en realidad los Servicios de Seguridad Gestionada (Managed Security Services? Telefonica lo define como una oferta de gestión y monitorización de la infraestructura con una propuesta global que cubre las principales necesidades de seguridad empresarial frente a posibles amenazas en las redes, sin tener que realizar ninguna inversión inicial. Los servicios de Seguridad Gestionada le permiten delegar la gestión de seguridad (seguridad operacional) y la gestión de incidentes de seguridad (preventivo y reactivo) de su organización en un equipo experto y global.

Según cuenta R3 CyberSecurity, la ciberseguridad puede y debe ser una herramienta para favorecer la evolución y crecimiento de las empresas. Para ello no es necesario tener un departamento de ciberseguridad, ni contratar expertos. La respuesta es contratar los Servicios de Ciberseguridad Gestionada. Es decir, contratar a una empresa de expertos que se encargue de la seguridad por usted, por un precio adaptado a sus necesidades reales. Esto asegura una gestión continua de seguridad sin tener que contratar a un equipo de expertos trabajando 24 horas al día, 365 días al año, además de conocimientos y experiencias actualizados, sin tener que invertir en la formación continua de los empleados. Las empresas podrán evolucionar y crecer a mayor ritmo si mantiene un nivel de seguridad que le permita centrarse en su negocio.

"LA CIBERSEGURIDAD PUEDE Y DEBE SER UNA HERRAMIENTA PARA FAVORECER LA EVOLUCIÓN Y CRECIMIENTO DE LAS EMPRESAS"

Enrique Ramírez, experto en Servicios Gestionados de Seguridad de Ajoomal Asociados.

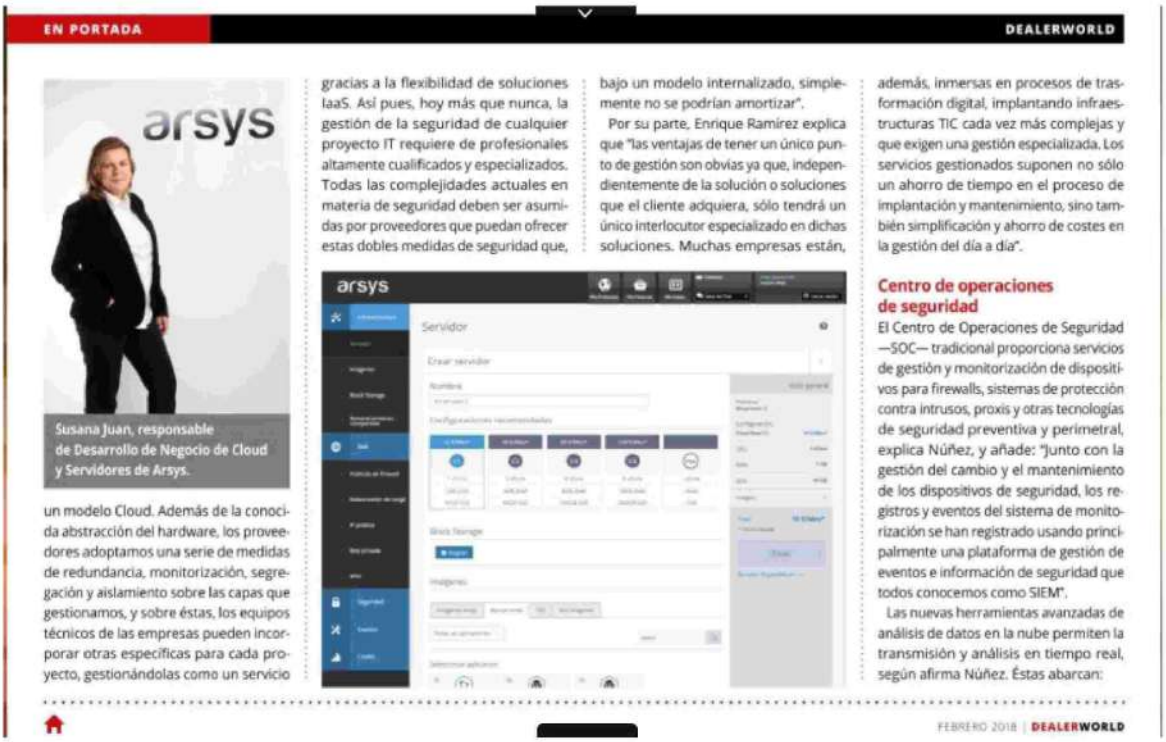
En opinión de Enrique Ramírez, experto en Servicios Gestionados de Seguridad de Ajoomal Asociados, las ventajas de este tipo de servicios son tres: "En primer lugar, hay una clara reducción de tiempos de implantación de la solución. Por otro lado, permite al cliente contar con expertos certificados en el producto en cuestión en desarrollo del proyecto, que por otro lado se entrega como "proyecto llave en mano". Por último, se garantiza el cumplimiento de las normativas sectoriales con la mínima inversión posible".

Evolución de la gestión de la seguridad con la adopción masiva del Cloud

Para Susana Juan, responsable de Desarrollo de Negocio de Cloud y Servidores de Arsys, "la securización de los servicios IT siempre ha sido una cuestión que ha preocupado tanto a empresas como a proveedores, pero con la irrupción de un nuevo modelo de usuario (permanentemente conectado, multidispositivo y en movilidad), la situación se ha vuelto más importante que nunca" Esta ha sido, precisamente, una de las principales tendencias tecnológicas para la externalización en Cloud. Susana Juan añade: "La seguridad es mucho más fácil de gestionar para los equipos técnicos bajo

Medio: **DEALER WORLD**
Fecha: **19/02/2018**
Página: **4** Documento: **4/7**
Autor: **MABEL CAMPO**

Valor (vpe): **29.000,00€**
Difusión: **9.500**
Audiencia: **38.000**
Ocupación aprox. (%) : **100,00**



Susana Juan, responsable de Desarrollo de Negocio de Cloud y Servidores de Arsys.

un modelo Cloud. Además de la conocida abstracción del hardware, los proveedores adoptamos una serie de medidas de redundancia, monitorización, segregación y aislamiento sobre las capas que gestionamos, y sobre éstas, los equipos técnicos de las empresas pueden incorporar otras específicas para cada proyecto, gestionándolas como un servicio gracias a la flexibilidad de soluciones IaaS. Así pues, hoy más que nunca, la gestión de la seguridad de cualquier proyecto IT requiere de profesionales altamente cualificados y especializados. Todas las complejidades actuales en materia de seguridad deben ser asumidas por proveedores que puedan ofrecer estas dobles medidas de seguridad que, bajo un modelo internalizado, simplemente no se podrían amortizar".

Por su parte, Enrique Ramírez explica que "las ventajas de tener un único punto de gestión son obvias ya que, independientemente de la solución o soluciones que el cliente adquiera, sólo tendrá un único interlocutor especializado en dichas soluciones. Muchas empresas están, además, inmersas en procesos de trasformación digital, implantando infraestructuras TIC cada vez más complejas y que exigen una gestión especializada. Los servicios gestionados suponen no sólo un ahorro de tiempo en el proceso de implantación y mantenimiento, sino también simplificación y ahorro de costes en la gestión del día a día".

Centro de operaciones de seguridad

El Centro de Operaciones de Seguridad —SOC— tradicional proporciona servicios de gestión y monitorización de dispositivos para firewalls, sistemas de protección contra intrusos, proxis y otras tecnologías de seguridad preventiva y perimetral, explica Núñez, y añade: "Junto con la gestión del cambio y el mantenimiento de los dispositivos de seguridad, los registros y eventos del sistema de monitorización se han registrado usando principalmente una plataforma de gestión de eventos e información de seguridad que todos conocemos como SIEM".

Las nuevas herramientas avanzadas de análisis de datos en la nube permiten la transmisión y análisis en tiempo real, según afirma Núñez. Éstas abarcan:

Medio: **DEALER WORLD**
Fecha: **19/02/2018**
Página: **5** Documento: **5/7**
Autor: **MABEL CAMPO**
Valor (vpe): **29.000,00€**
Difusión: **9.500**
Audiencia: **38.000**
Ocupación aprox. (%) : **100,00**

- Herramientas de seguridad como cortafuegos, IDS, IPS, Web Proxy, VPN, AV, DLP, DAM, WAF, escáneres VA.
- Aplicaciones y cargas de trabajo, ya sea *on premise* o en la nube.
- Infraestructura como IaaS, PaaS, EMM, middleware, base de datos, servidores web, hipervisores y hosts (Windows, Linux y Unix).
- Herramientas de red como enrutadores, conmutadores, DNS, DHCP y balanceadores de carga.

Este tipo de herramientas de análisis de datos correlacionan el contexto de identidad con los eventos para identificar riesgos de seguridad y facilitar la inteligencia procesable, "lo cual nos permite articular una respuesta automatizada. Sus beneficios son, entre otros, cerrar la brecha que las herramientas centradas en red no pueden cubrir y extender la capacidad de monitoreo sin consumir recursos adicionales al automatizar el post evento, la investigación y la respuesta" explica Núñez.

Para Sogeti, el Centro de Operaciones de Seguridad (SOC) dedicado —que puede estar alojado en sus propios sistemas o ser proporcionado como un servicio gestionado— está dotado del conocimiento necesario para identificar y prevenir las ciberamenazas y eliminarlas de sus sistemas. Con alertas, identificación de actividades sospechosas y la investigación forense, obtendrá una visión de conjunto de los riesgos de ciberseguridad real.

Preocupación de las empresas que quieren adoptar Cloud y externalizar sus servicios de TI

La seguridad continúa siendo la principal preocupación de los directivos de cara a la adopción de la nube. "Pero hablamos de un modelo cuyas ventajas en la gestión de la seguridad está también convenciendo a las empresas para adoptarlo" explica Susana Juan, "y en 2019, más de la mitad de sus datos críticos estarán en la nube según un estudio hecho público recientemente por Teradata", apostilla aquella ejecutiva. Sobre la razón de por qué ocurre esto, explica de nuevo: "Se debe a que, en realidad, la nube es el entorno más seguro en el que operar y guardar nuestros datos. Y no sólo por la calidad de los servicios que presta un proveedor especializado, sino también por la flexibilidad y eficiencia del Cloud de cara al despliegue de medidas adicionales de seguridad en modo as a Service".

Pero ¿por qué las empresas optan por estos servicios externos? Según Susana Juan, "del mismo modo que las empresas son conscientes de la dificultad de rentabilizar un sistema interno de mensajería y optan por recurrir a un tercero para gestionar sus envíos, la decisión más lógica para contar con un servicio IT eficaz y seguro es la externalización. Hoy en día, prácticamente cualquier responsable técnico es consciente de que todas las complejidades actuales de la gestión de la seguridad difícilmente se podrían amortizar bajo un modelo internalizado: redundancia, stock de hardware, personal 24x7... ".

Medidas que ofrecen los proveedores

Los proveedores implementan numerosas medidas de seguridad internas "por defecto sobre nuestros servicios Cloud", explica Susana Juan, quien incide: "Para mantener la seguridad, privacidad y facilitar el cumplimiento de las regulaciones,

Medio: **DEALER WORLD**
Fecha: **19/02/2018**
Página: **6** Documento: **6/7**
Autor: **MABEL CAMPO**
Valor (vpe): **29.000,00€**
Difusión: **9.500**
Audiencia: **38.000**
Ocupación aprox. (%) : **100,00**

además de proporcionar soluciones de continuidad y un plan de contingencia. Son distintas medidas de seguridad física en nuestras instalaciones (suministro eléctrico, redundancia de hardware, conectividad y climatización.....) y seguridad lógica (sistemas de detección y prevención de intrusiones, sistemas SIEM de gestión y correlación de eventos para el análisis en tiempo real...). Garantizamos también el cumplimiento de las normativas y mejores prácticas, gracias a certificaciones internacionales como las ISO 27001 y 9001 o las certificaciones propias de los fabricantes. Y, lo que es más importante, contamos con equipos expertos y especializados que monitorizan nuestros servicios 24x7, dan soporte a nuestros clientes y conocen a la perfección las plataformas *Cloud* que utilizan".

Por otro lado, como cada cliente y proyecto es distinto, una de las medidas más efectivas para garantizar la protección, recuperación y disponibilidad de los proyectos es la experiencia y conocimiento de las prioridades de cada uno. De este modo, explica Susana Juan, "se establece un diálogo entre cliente y proveedor para desplegar soluciones de infraestructura IT a medida, basados en servicios Cloud tan flexibles que permiten añadir medidas adicionales y específicas para los diferentes casos de uso. Se trata de desplegar, dentro del modelo "as a Service" del Cloud, sistemas de monitorización y alerta temprana a todos los niveles, cortafuegos de red y de aplicación, protección frente a intrusiones, ataques DDoS, código malicioso y, por supuesto, copias de seguridad y planes de recuperación".

Desaparición de los centros de datos propios

No cabe duda de que la externalización en Cloud es una tendencia al alza. Basta fijarse en los datos sectoriales, que confirman que la adopción del Cloud crece a un ritmo anual del 30%. No obstante, aclara Susana Juan, "al igual que estoy segura de que hay mercado suficiente para todos los proveedores profesionales, estoy convencida de que aún estamos muy lejos de ver la desaparición de los centros de datos propios. Siempre habrá empresas con necesidades tan específicas que tengan que gestionar su propio CPD, aunque luego se apoyen en CPD de terceros y soluciones Cloud externalizadas para el despliegue de proyectos o servicios de manera más eficiente y fácil de gestionar".

En estos casos, una de las mejores opciones para simplificar la gestión de la seguridad IT de las organizaciones es optar por infraestructuras de Cloud Híbrida, que combinen recursos compartidos y dedicados bajo demanda, de modo que las empresas pueden decidir el grado de aislamiento que necesitan, pero sin renunciar a la comodidad del Cloud ni a sus ventajas: el pago por uso, la implantación en minutos o las funcionalidades avanzadas de seguridad y disponibilidad que podemos activar cuando las necesitamos con sólo unos clics, asegura Susana Juan.

Cómo puede la seguridad gestionada ayudar a abrir nuevas vías de negocio

Los modelos Cloud y la externalización de la seguridad de este tipo de soluciones garantizan una adaptabilidad continua de

Dealer World

Medio: **DEALER WORLD**
Fecha: **19/02/2018**
Página: **7** Documento: **7/7**
Autor: **MABEL CAMPO**

Valor (vpe): **29.000,00€**
Difusión: **9.500**
Audiencia: **38.000**
Ocupación aprox. (%) : **100,00**

las soluciones tecnológicas, de manera que contribuyen a la evolución del negocio sin drenar recursos económicos ni tener que destinar el talento de las organizaciones a tareas que pueden delegarse en proveedores especializados, que ofrecen niveles de servicio que no están fácilmente al alcance de la mayor parte de las empresas.

El *partner* tecnológico referente, por lo tanto, es el Canal, explica Enrique Ramírez. "Acompaña a su cliente a lo largo de toda la cadena de valor del negocio, desde la fase de pre-venta/consultoría hasta la implantación de la solución recomendada, incluyendo mantenimiento, pago por uso y continuidad de negocio", sostiene aquel directivo. Y es que, realmente, desde hace varios años ya lo estamos viendo en otros países como EE. UU. o Reino Unido. Por eso añade Ramírez: "Existe la tendencia de especialización y externalización de cualquier tipo de servicio que requiera continuidad y que sea crítico para el negocio. Empezamos en su momento con la externalización de servicios asociados, sobre todo, comunicaciones de grandes empresas y actualmente está siendo extendido a todos los ámbitos del entorno TIC incluyendo las infraestructuras (IAAS) y también la PYME".

Por ejemplo, señala Susana de Juan, "entre nuestros *partners* tenemos clientes que son ISV (Independent Software Vendors) y que están gestionando su infraestructura en modo Cloud para crear fácilmente entornos de pruebas para el cliente final y evolucionar del tradicional modelo de licenciamiento al modelo SaaS, lo que les está abriendo la puerta a nuevos mercados que hasta ahora no se habían planteado dar un salto cualitativo en sus sistemas informáticos".

Ramírez concluye que desde su empresa tienen claro el concepto del negocio: "tanto para nosotros como por supuesto para nuestros *partners*, que son la pieza clave de nuestro negocio. Estamos trabajando codo a codo con ellos para seguir incrementando el número de servicios prestados a sus clientes finales, y así hacer crecer tanto su negocio como el nuestro". La compañía asegura que las soluciones y tecnologías más demandadas en un modelo de pago por uso por parte de sus *partners* son, por un lado, seguridad perimetral, sobre todo, en entornos multi-delegación. En segundo lugar, las soluciones Cloud anti-ramsomware y de monitorización y auditoría de red descentralizada. Por último, aunque no menos importante, se está demandando mucho todo lo que tiene que ver con archivado de correo y backup remoto. Ajoomal señala que cualquier tipo de empresa hoy en día, independientemente de su tamaño, cuenta con servicios externalizados tipo "pago por uso" que van desde algo tan habitual como el correo hasta soluciones punteras como el backupcloud-to-cloud, HSM´s AAS, protección DNS, antiDDoS, etc.-

El futuro de la seguridad TI

Estamos ante un horizonte complejo, donde seguridad, eficiencia y funcionalidades técnicas deben ir de la mano, "siempre sin perder de vista a los usuarios y su manera de utilizar la tecnología en su día a día", añade Susana Juan. La forma en la que protegemos la información en el mundo digital actual debe ser completamente diferente a la que planteábamos hace apenas unos pocos años. Pero, sobre todo, debemos abordarlo desde una perspectiva y con un asesoramiento experto. De lo contrario, cualquier inversión puede resultar tan poco eficaz como lo sería proteger una ciudad del siglo XXI con una muralla medieval. **DW**