Dealer World
Fecha: viernes, 22 de junio de 2018
Página: 32, 33, 34, 35, 36, 37
Nº documentos: 6

Recorte en B/N % de ocupación: 569,28 Valor: 14801,36€ Periodicidad: Quincenal Tirada: 12.338 Audiencia: No disp. Difusión: 12.084

No hay seguridad, no hay nube

Que la nube es un fenómeno imparable es algo indiscutible. Es uno de los pilares de la transformación digital, y por lo tanto de la nueva economía. Podemos discutir sobre si triunfará la nube púbica, la privada o la híbrida; o sobre el tipo de información que debe guardar la empresa “in situ” y la que debe trasladar a la nube, pero lo que nadie discute es sobre la seguridad que requiere. Por lo que las empresas demandan proveedores especializados que les puedan ofrecer todas las garantías necesarias para sentirse seguros.

Isabel Campo

Dealer World
Fecha: viernes, 22 de junio de 2018
Página: 32, 33, 34, 35, 36, 37
Nº documentos: 6

Recorte en B/N % de ocupación: 569,28 Valor: 14801,36€ Periodicidad: Quincenal Tirada: 12.338 Audiencia: No disp. Difusión: 12.084

Las empresas, cuando trasladan sus aplicaciones y datos a la nube, están trasladando también su confianza y tranquilidad. Cualquier empresa que se dedique a este sector del mercado sabe que la seguridad de sus datos y el buen funcionamiento de sus aplicaciones están por encima de otras capacidades. Tanto es así que la seguridad en la nube es uno de los mercados con mayores oportunidades. Gartner prevé que los servicios de seguridad basados en la nube alcanzarán 9.000 millones de dólares —7.646,50 millones de euros— en 2020.

Para Iván Abad, Technical Services Manager de Commvault, la razón está en que "las soluciones *on premise* están siendo reemplazadas por los servicios en la nube y por las arquitecturas *Hyper-Scale*, que aportan beneficios inequívocos, pero que implican que los datos están lejos físicamente de las instalaciones corporativas y que no siempre permanecen bajo el control del departamento de TI. Es imprescindible tener control y poder gestionar dichos datos. Y cada vez será más importante en el futuro según se migren servicios críticos a Cloud. La nube aporta un sinfín de posibilidades.

Pero aquellos que no hayan asegurado el control sobre sus datos, no importa dónde se encuentren, están poniendo en riesgo la supervivencia de su negocio".

Álvaro Rudíez, PR Manager de Arsys, destaca el hecho del enorme volumen de información que manejamos. "El ingente volumen de datos con que cualquiera de nosotros gestiona en el día a día, tanto en el ámbito personal como profesional, así como la creciente sensibilidad por cómo se utilizan estos datos, ha hecho que la seguridad en el mundo *online* se haya convertido en una prioridad irrenunciable para cualquier empresa. De hecho, según un estudio hecho público recientemente por Teradata, la seguridad continúa siendo una de las principales preocupaciones para los CIO. Pero, aun así, más de la mitad de los datos críticos para sus empresas estarán en la nube en 2019". Y precisamente, por ello, piensa que "es el momento de cambiar el enfoque con el que nos posicionamos en temas de seguridad. Debemos asumir que la realidad de la seguridad es tan nueva como la forma en la que hemos decidido utilizar los servicios IT y ser conscientes de que los conceptos tradicionales de seguridad se han visto desbordados. Una vez aceptamos esta realidad, el Cloud se convierte en el mejor de los aliados y el proveedor pasa a ser el *partner* de confianza que securiza nuestros datos de negocio", admite.

Igor Unanue, cofundador y CTO de S21sec, coincide con la falta de conciencia que hay todavía estos temas, y señala: "Probablemente, ahora mismo no seamos

Dealer World
Fecha: viernes, 22 de junio de 2018
Página: 32, 33, 34, 35, 36, 37
Nº documentos: 6

Recorte en B/N % de ocupación: 569,28 Valor: 14801,36€ Periodicidad: Quincenal Tirada: 12.338 Audiencia: No disp. Difusión: 12.084

conscientes de las amenazas que puedan existir en el entorno Cloud, pero conocemos casos graves de fuga de información o de ataques de denegación que claramente afectan. Y, sin duda, van en aumento, ya que cada vez ponemos más datos de negocio en la nube".

La necesidad de contar con especialistas

La seguridad en Cloud es un ámbito tan extenso y complejo que, con el fin de poder sintetizar el estado actual, es necesario considerar el principio de responsabilidad que recae, en función del modelo de servicio, en el proveedor Cloud, por un lado y en el cliente, por otro. Según explica Arancha Jiménez, responsable de GRC y Ciberseguridad en Atos Spain, "en relación con la responsabilidad de los proveedores de servicios Cloud, su nivel de madurez actual en cuanto a seguridad permite realizar una apuesta por el uso de cualquiera de sus modelos (IaaS, PaaS y SaaS), sin que ello suponga un aumento significativo del riesgo. De hecho, podría decirse que incluso se reduciría en muchos aspectos. Creo que esto es especialmente cierto en los servicios de provisión de infraestructura, en los que se aprecia la adopción definitiva de procesos de certificación respecto a estándares y normativas para dar cumplimiento a las necesidades de los clientes finales. Todo ello, lógicamente, aplicado a los principales proveedores de referencia de *cloud* pública".

En muchas ocasiones, las empresas contratan servicios sin valorar cuáles son sus necesidades reales o qué garantías son más importantes, Jiménez destaca que "el papel del cliente en su ámbito de responsabilidad, el punto principal lo pondría en la adquisición de conocimiento respecto a los servicios contratados, de forma que se puedan tomar las decisiones más adecuadas tanto técnicas como organizativas u operativas. Este nivel de conocimiento puede adquirirse con formación reglada específica, aunque la velocidad de evolución por parte de los proveedores de referencia obliga a estar permanentemente al día de los nuevos servicios y capacidades de seguridad que se incorporan a los productos y servicios Cloud en general, y al catálogo de funcionalidades de seguridad en particular. La colaboración con *partners* especializados en seguridad Cloud parece, a día de hoy, el modelo más adecuado de iniciar el viaje a la nube con la velocidad requerida por los procesos de transformación digital que se están llevando a cabo en las compañías".

Arancha Jiménez hace hincapié en la necesidad de la colaboración y explica: "En aquellos aspectos en los que las capacidades nativas de los proveedores no cubran el nivel de seguridad, existe también la madurez suficiente en el mercado, para alcanzarlo con soluciones y herramientas de terceros, como los CASB, CWP, aparte de la incorporación continua de soluciones tradicionales de seguridad (red, *endpoint*, DLP, cifrado, etc.) al mundo Cloud, bien integrándolos directamente en servicios de los proveedores de Cloud pública, bien como servicios de seguridad en modelo Cloud propios (*FW* en nube, *proxy* en nube, etc.)" y añade: "Es cierto que aparecen nuevos retos en los que es necesario realizar un foco especial, como por ejemplo, la visibilidad y exposición a Internet de interfaces administrativas, la adopción de medidas de seguridad en procesos *DevOps*,

Dealer World
Fecha: viernes, 22 de junio de 2018
Página: 32, 33, 34, 35, 36, 37
Nº documentos: 6

Recorte en B/N % de ocupación: 569,28 Valor: 14801,36€ Periodicidad: Quincenal Tirada: 12.338 Audiencia: No disp. Difusión: 12.084

para contenedores y microservicios, pero en resumen, creo que es posible, a día de hoy, alcanzar un nivel de seguridad adecuado en los servicios Cloud, contando para ello desde soluciones nativas a servicios profesionales especializados.

Por su parte, Alejandro Salvador, Sales Manager Europe, Business Solutions de Exact, explica que "los proveedores de soluciones Cloud somos conscientes de la relevancia e importancia de nuestras inversiones en seguridad para los clientes, especialmente para los de menor tamaño, ya que gracias a las economías de escala pueden tener acceso a servicios de máxima calidad a precios asequibles", y añade: "Los centros de datos con medidas de seguridad físicas y lógicas, copias de seguridad, estándares de desarrollo del software, monitorización 24x7 de los sistemas, evitar la filtración de datos, ataques de *hacking* ético..., son algunos ejemplos de los beneficios de basar los procesos de negocio y almacenar sus datos en un proveedor Cloud. Por eso, una de las principales ventajas de los servicios en la nube es que las organizaciones pueden operar a escala en función de sus necesidades, sin poner en riesgo la protección de sus datos y con total confidencialidad de su información".

Álvaro Rudíez, por su parte, hace hincapié en que los proveedores especializados permiten ofrecer servicios que, de otra manera, muchas empresas no podrían tener: "La economía de escala permite a los proveedores especializados en Cloud ofrecer a sus clientes medidas de seguridad que, bajo un modelo internalizado, serían imposibles de amortizar. Hablamos de soluciones para la detección y prevención de intrusiones, análisis y gestión de vulnerabilidades y parches, cortafuegos de aplicaciones web. Pero también de la redundancia de elementos críticos (climatización, hardware, conectividad, electricidad...) o del mantenimiento 24x7 de sistemas por parte de personal especializado. Estas medidas se incorporan por defecto a los servicios que los proveedores IT comercializan en soluciones como los Servidores Cloud, y por eso es clave contar con el asesoramiento de un proveedor experto que cuente con una solución flexible y ofrezca distintos grados de aislamiento en el despliegue de arquitecturas IT; que puedan gestionarse fácilmente desde un mismo panel, por ejemplo implementado soluciones de Cloud híbrido que permiten combinar, conectar y gestionar de forma conjunta, tanto recursos dedicados en exclusiva, con Servidores *Cloud*. Un modelo mixto, bajo demanda y en pago por uso, que permite aprovechar lo mejor de ambos mundos y garantizar la seguridad", y termina asegurando: "Hoy más que nunca, el Cloud es una herramienta empresarial irrenunciable. Y no sólo por la forma en la que los usuarios trabajamos. Sobre todo, porque el Cloud ha demo-

Dealer World
Fecha: viernes, 22 de junio de 2018
Página: 32, 33, 34, 35, 36, 37
Nº documentos: 6

Recorte en B/N % de ocupación: 569,28 Valor: 14801,36€ Periodicidad: Quincenal Tirada: 12.338 Audiencia: No disp. Difusión: 12.084

cratizado también la seguridad IT entre pymes y profesionales".

Igor Unanue coincide en el hecho de que este tipo de empresas pueden ofrecer servicios que, de otra forma, no podrían tener las empresas. "Ofrecemos servicios orientados a proteger estos entornos teniendo en cuenta que requieren de una especialización dada la complejidad de fabricantes, proveedores y tecnologías que podemos encontrar. No hay que olvidar que esta complejidad siempre va a dificultar la gestión y respuestas ante incidentes, y por ello es importante tener mecanismos para monitorizar y responder con rapidez, independientemente de donde esté el dato", considera Unanue.

Qué buscan las empresas

El mercado Cloud sigue creciendo como una de las preferencias de las principales empresas de todo el mundo, y se calcula que el 53% de ellas tiene, al menos, la mitad de su infraestructura alojada allí. Sin embargo, explica Hideki E. Hashimura, CMO de redk, "la seguridad aún es uno de los principales frenos para trasladar las infraestructuras IT hacia la nube, cuando precisamente se trata de una de sus grandes cualidades".

La nube se ha convertido en uno de los principales objetivos de los ciberdelincuentes

"Todas las previsiones indican que las empresas continuarán moviendo sus datos a la nube durante los próximos años. Esto responde a la búsqueda por hacer sus operaciones realmente rentables en un mundo altamente competitivo", según explica Javier Hijas, Cloud Security Team Manager – Europe.

Aunque los entornos Cloud son cada vez más comunes, siguen siendo una tecnología relativamente nueva y en constante evolución. Esto proporciona a los ciberdelincuentes una serie de *backdoors* mediante las que acceder a las redes corporativas. Otra de las causas de los ataques exitosos a la nube es que se tiene un concepto erróneo sobre los niveles de seguridad necesarios. Además, muchas organizaciones no tienen claro quién es el responsable de la protección de la nube, dejando la puerta abierta de par en par a las brechas de seguridad.

Durante el último año, más del 50% de los incidentes de seguridad gestionados por el equipo de respuesta a incidentes de dicha firma estaban relacionados con la nube. Y la mitad de ellos se debían a problemas de aplicaciones SaaS o servidores cloud. Las filtraciones de datos siguen siendo una de las principales preocupaciones de las organizaciones que se mueven en entornos cloud, especialmente debido al uso de los servicios de envío de archivos que utilizan esta tecnología. Por otra parte, la creciente adopción del correo electrónico basado en SaaS, como Office 365 y Google G Suite, así como el modelo IaaS, convierten a la nube en un objetivo muy atractivo para los ciberdelincuentes, y que seguirá siéndolo durante los próximos meses.

Por último, las altas sanciones en caso de no cumplir las nuevas regulaciones en materia de privacidad y seguridad, como el RGPD, son importantes agravantes de estas amenazas.

Y es que, a la preocupación de la seguridad, ahora las empresas suman la necesidad de cumplir con la nueva reglamentación, por lo que Hashimura destaca que los proveedores deben "facilitar el cumplimiento de este nuevo reglamento y potenciar el buen uso y respeto de los datos de clientes que, al final, son el material con el que podemos crear nuevas estrategias de negocio", y añade: "Aquellas empresas que están en un proceso de transformación deben tener en cuenta esta nueva norma a la hora de seleccionar su software CRM y el entorno de infraestructuras Cloud, ya que será un factor decisivo de sus resultados. La apuesta por soluciones seguras, escalables y de alto rendimiento es una cuestión decisiva para cualquier organización actual".

Traspasando el departamento de TI

Cada vez más, la comunicación entre los departamentos de las empresas es mayor, y en el caso de las TI es más notorio. Antes estaban completamente aislados, y ahora están "condenados" a entenderse desde el CEO hasta el departamento de logística o ventas pasando por el de marketing. Cualquier fallo o problema

Dealer World
Fecha: viernes, 22 de junio de 2018
Página: 32, 33, 34, 35, 36, 37
Nº documentos: 6

Recorte en B/N % de ocupación: 569,28 Valor: 14801,36€ Periodicidad: Quincenal Tirada: 12.338 Audiencia: No disp. Difusión: 12.084

de aplicaciones o funcionamiento afecta directamente a la cuenta de resultados, como no había pasado nunca. Para Javier Antón, director de Ciberseguridad de Fujitsu de la región de WEMEI (Europa Occidental, Oriente Medio e India), "la ciberseguridad se ha convertido en uno de los grandes pilares y una de las apuestas fundamentales de las compañías, ya que ha pasado de ser un problema tecnológico a ser una prioridad para los comités de dirección, por lo que llega a influir en su negocio. Y especialmente en las empresas cotizadas, debido al nacimiento de regulaciones específicas y sobre todo, por cómo puede impactar un ataque en su negocio y producir temas tan relevantes como la caída de las acciones".

Los datos hablan

El incremento de ciberataques y el robo de datos como una nueva forma de delincuencia ha hecho saltar las alarmas entre las empresas. "En cuanto a los datos que vemos a nivel global —señala Javier Antón—, son especialmente relevantes, ya que el 67% de las medianas y grandes empresas ha identificado una brecha de seguridad o ataque en los últimos 12 meses. El 45% ha tenido un incidente en sus procesos de gestión. Se estima que unos 120 días es lo que puede permanecer un *hacker* en la red de la compañía. Y, por otro lado, hay una gran preocupación por establecer perfectamente en sus organizaciones las regulaciones de la Unión Europea —RGPD y NIS—, tanto a escala de control de la información y de la red. Sin olvidarnos de que existe una carencia de recursos en ciberseguridad, lo cual lleva a que se den agujeros, especialmente si pensamos que los profesionales de este segmento que son muy demandados y retenerlos es difícil".

Álvaro Rudíez considera que, ante esta escalada, "la nube se ha erigido en los últimos tiempos en la solución que más y mejor resuelve las exigencias de seguridad de cualquier empresa, pyme o autónomo. Las soluciones que, en su momento, sólo podían implementar las grandes multinacionales ya están al alcance de prácticamente cualquiera, como un servicio, sin costosas implantaciones y en pago por uso".

Evolución del mercado español

La aceptación de la nube en nuestro país ha sido muy buena, según explica Hashimura: "Las empresas en España llevan varios años apostando por las soluciones Cloud, porque han despejado cualquier duda en cuanto a la posible pérdida de control sobre sus activos. Entre sus grandes valores, destaca la agilidad que aportan a las transacciones más operativas, precisamente las que tienen que ver con las interacciones que mantienen con sus clientes", y añade: "Los clientes españoles están cada vez más interesados en la combinación de inteligencia de clientes, soporte Cloud y total confidencialidad de los datos. En los próximos años, esta tendencia se acentuará porque, además, ofrece enormes ventajas a los negocios a la hora de abordar estrategias globales de acercamiento a sus clientes". **DW**