Mesa redonda

La cloud puede ser segura

Data Center Market, en colaboración con Bitdefender, ha organizado un desayuno de trabajo para analizar cómo garantizar la seguridad en las soluciones virtualizadas de los CPD. Al encuentro han acudido Aryse Infraestructuras, Colt Technology Services, Fibernet, Gigas, Huawei, Interoute Iberia y Uniway.

Cristina López Albarrán
cristina.albarran@bps.com.es
@DataCenterBPS
www.datacentermarket.es

Bajo el título de *¿Cómo garantizar la seguridad en las soluciones virtualizadas de los CPD?*, Data Center Market organiza un desayuno de trabajo, con la colaboración de Bitdefender, para dar respuesta a esta cuestión. Al encuentro, celebrado en el Hotel Intercontinental de Madrid, han acudido representantes de Aryse Infraestructuras, Colt Technology Services, Fibernet, Gigas, Huawei, Interoute Iberia y Uniway.

Entornos virtuales protegidos

La mesa comienza con la constatación de una necesidad: las infraestructuras virtuales también han de ser protegidas, pues existen ataques específicos a estos entornos. Ante la pregunta de cómo están abordando las diferentes compañías presentes en el encuentro la protección de estas infraestructuras Horatiu Bandoiu, Channel Marketing Manager SE & LATAM de Bitdefender, inicia el debate explicando que Bitdefender tiene en el mercado un producto pensado para grandes empresas y orientado a proteger las infraestructuras virtualizadas. Se trata de una solución con un consumo de recursos reducidos pero que aporta una seguridad extensa "porque en entornos virtualizados hay una posibilidad de ataque muy amplia, debido al uso compartido de recursos". Lanzada hace seis años, la venden en muchos CPD en todo el mundo y ya está presente en algunos de España.

Para una empresa como Gigas, que ofrece servicios de infraestructura cloud a mediana y gran

empresa, los ataques forman parte de la dinámica y los mitigan con "protección, estando al tanto de los ataques que van surgiendo y atendiendo la causística del cliente", confiesa José Antonio Arribas, COO de Gigas.

"El proveedor tiene la obligación de garantizar la seguridad de la cloud, que la infraestructura esté protegida a nivel de base, y para ello hay que securizar la plataforma", matiza José Manuel Armada, Head of Sales Engineering de Interoute. Eso sí, reconoce que el propio cliente ha de determinar hasta cuándo o dónde quiere que el proveedor le proteja, pero sin olvidar que existen vulnerabilidades a determinadas partes de la infraestructura a las que el cliente no debería tener acceso. No en vano, asegurar la infraestructura virtualizada es más crítico que nunca, porque puede suponer una caída del negocio.

Es una obligación del proveedor garantizar que la arquitectura está protegida

"La estructura de Huawei es no sólo ir a hardware sino más bien a soluciones cloud. La seguridad es un paso más", señala Santiago Julián, IT Senior Product Manager de Huawei. "El mundo ya se mueve hacia la nube, pero uno de los requisitos que nos piden los clientes es saber qué seguridad me ofrece tu cloud", continúa. En su opinión, la virtualización existe hace muchos años y ahora la cuestión es qué tipo de seguridad se tiene que llevar -física o lógica- a ese entorno porque "si atacan a un cliente nos atacan a todos". En este sentido, menciona que los clientes quieren saber qué normativa y legislación cumplimos y saber dónde está el dato ubicado.

Por su parte, a una compañía como Colt, enfocada a los servicios de colocation, los clientes le piden que dé cuentas de cómo va a garantizar la seguridad de sus activos y si hablamos de un modelo híbrido, cómo aseguran que la transferencia de datos está cien por cien segura. La clave está, según apunta Francisco Ramírez Soto, Site Manager de Data Center Services de Colt, en ajustar el servicio en función de las necesidades del cliente. "Nosotros aseguramos que el dato está donde decimos que está", puntualiza. Y aventura que aunque todo el mundo se preocupa por la seguridad lógica, "también hay que fijarse en el posible riesgo -algo que no es fácil porque va cambiando continuamente-, y conocer desde qué dispositivos se va a acceder a la información".

"Aunque el cloud computing ha llegado para quedarse, todavía hay ciertos recelos respecto a su seguridad"

"La virtualización llegó para quedarse y nos tenemos que adaptar", sentencia Miguel Ángel Gutiérrez Sánchez, responsable del Departamento de Energía y Data Center de Aryse Infraestructuras. El directivo reconoce que la tecnología ha cambiado mucho y los clientes quieren una optimización de la energía y del equipo, un ahorro de costes, algo que aporta el modelo virtual.

Pablo Prieto, director técnico de Uniway, que indica que "como proveedor de servicios tenemos que garantizar que nuestra plataforma está securizada desde el punto de vista de la arquitectura". Eso sí, admite que "la solución de seguridad perfecta no existe y si existe, su coste es infinito". También hace hincapié en la importancia del análisis de riesgos y un gran aliado del mismo es el GDPR cuyo cumplimiento "implica que el análisis de riesgos interno que tienes que hacer es muy alto". Esas son las dos grandes bazas: arquitectura y análisis de riesgos. Pese a ello, menciona que desde Uniway están mirando muy de cerca la seguridad en la virtualización, "sobre todo la definición de compartimentos estancos para evitar su ruptura".

El usuario sigue siendo el punto más débil

Asimismo, Esther Gómez Vidal, directora general de Fibernet, subraya que como fabricantes de tecnología que son, los clientes huyen del puro hierro, así que "lo tenemos difícil para defender la tecnología como tal, por lo que tenemos que recubrirla de herramientas que se enfoquen a ese

"Las vulnerabilidades se pueden mitigar cumpliendo la normativa vigente, analizando continuamente los riesgos y formando a los empleados sobre seguridad"

"Virtualización y seguridad tienen que ir de la mano y evolucionar en el mismo sentido"

Miguel Ángel Gutiérrez Sánchez, responsable del Departamento de Energía y Data Center de Aryse Infraestructuras.

"El cloud puede ser seguro, la virtualización también porque hay soluciones que pueden ayudar a que así sea... Se pensaba que la seguridad era un stopper para la nube, pero en realidad es un habilitador"

Horatiu Bandoiu, Channel Marketing Manager SE & LATAM de Bitdefender.

"Cuanto más securizo, menos flexible o menos gestionable soy. Lo que tenemos que ofrecer los proveedores son soluciones flexibles y fáciles de gestionar"

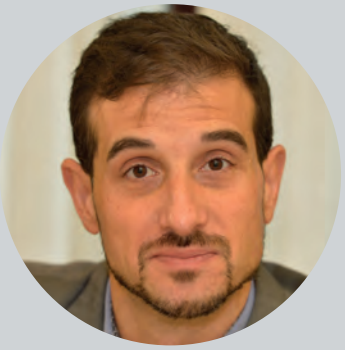
Juan Jesús Merino, Sales Regional Director Spain de Bitdefender.

"El cloud está aquí para quedarse, aunque aún hay mucha reticencia a su adopción por el tema de la seguridad. La manera de que evolucione es formar y educar"

Francisco Ramírez Soto, Site Manager de Data Center Services de Colt.

"Tenemos por delante un futuro apasionante y lleno de grandes retos porque la tecnología está en constante evolución. Aparecerán nuevas carreras para dar respuesta a lo que nos plantea el porvenir"

Esther Gómez Vidal, directora general de Fibernet.



"No hay que hablar de inseguridad en cloud, sino de la seguridad que aporta. Una de las ventajas que concede es esa"

José Antonio Arribas, COO de Gigas.

servicio y a esa seguridad". Por otro lado, como proveedores de servicios de CPD, "no podemos ofrecer un servicio generalista". En Fibernet proporcionan infraestructura al data center as a service y con mecanismos de seguridad. Esther Gómez constata que al principio, cuando se empezaron a montar los CPD el problema era el espacio, luego fue el consumo y ahora es la seguridad.

La nube es segura

Aunque la adopción de la nube cada vez es mayor en nuestro país, lo cierto es que todavía hay que vencer muchos miedos. "He visto una gran reticencia a migrar a la nube en España y eso que la nube se puede controlar mucho mejor que on premise", expone Horatiu Bandoiu, de Bitdefender. Según el directivo, en nuestro país los clientes

"Apostamos por la I+D basada en modelos de cloud. Nuestra obligación como fabricante es dar seguridad, pero de forma global"

Santiago Julián, IT Senior Product Manager de Huawei.

"El cloud lo inventaron los operadores y la virtualización los informáticos, pero está llegando a las redes. Hay convergencia"

José Manuel Armada, Head of Sales Engineering de Interoute.

"La seguridad es un concepto global que aborda diferentes elementos y procedimientos. El cloud puede ayudar a la continuidad del negocio"

Pablo Prieto, director técnico de Uniway.

suelen hacer muchos controles de tipo perimetral, pero les falta tener en cuenta el contexto. "Hay ciertas bases que no se cubren con lo que están proporcionando algunos fabricantes de virtualización". Es el caso de los ataques dirigidos, más avanzados, que no están cubiertos.

"Nos gustaría que la evolución a la cloud fuera más rápida de lo que está siendo", afirma el COO de Gigas. Considera que para muchas empresas la tecnología es un mal necesario y aunque muchas están solicitando soluciones cloud, todavía existen diferencias regionales. Cree que cuando las organizaciones ven las ventajas que ofrece la nube se animan a dar el salto. Y respecto a la seguridad de la nube sentencia: "El tema no es si la cloud es cien por cien segura, sino si esa solución que le propones al cliente es más segura que la que tiene en la actualidad. Hay que adecuar esa necesidad a lo que los clientes quieren".

"La seguridad es una cuestión de percepción, te puedes sentir seguro o no. Evidentemente la nube tiene riesgos, pero hay que poner en contexto", manifiesta Pablo Prieto, de Uniway. En este terreno, "los procedimientos asociados a la seguridad de los equipos (el cumplimento de normativa o las actualizaciones pertinentes) es lo que podemos aportar los proveedores". Precisamente sobre este asunto, Esther Gómez, de Fibernet, observa que es imposible que un cliente se dote de los recursos necesarios y que esté al tanto de todo. De ahí el valor de los proveedores de servicios. Además, esgrime que hay sectores muy tradicionales y reaccionarios a poner el dato en la nube. Para convencerlos, hay que medir el análisis de riesgo acorde al tipo de cliente, pues cada uno exige unas medidas de seguridad determinadas. La mejor premisa es, en su opinión, la sencillez: cuando diseñas una cosa, cuanto más sencilla sea, mejor.

"Con la virtualización se han expuesto los equipos, y en un CPD un ataque puede suponer una parada y hacer mucho daño al negocio"

Para Santiago Julián, de Huawei, la preocupación está en que no se promulgue el cloud público. "Hay que influenciar para ir hacia esta nube porque así la seguridad queda controlada". Pero también en el cloud público hay muchas variedades, matiza, pues no es lo mismo el dato en una Administración Pública que en otra organización.

"El esfuerzo que va a hacer el atacante va a depender de la recompensa que obtenga", cita José Manuel Armada, de Interoute. En su intervención argumenta que la tecnología tiene un efecto multiplicador muy importante que es la red, y que no hay que perder de vista un hecho: muchos de los agujeros de seguridad se producen desde dentro de la compañía, por una vulnerabilidad de los terminales y de los propios trabajadores. Por eso, insiste: "la seguridad no se puede dejar de la mano del proveedor, también hay que tener en cuenta al propio empleado pues el usuario sigue siendo el punto más débil". Las empresas han de tomarlo como un riesgo a valorar y tratar de conseguir un equilibro entre agilidad de negocio y seguridad.

CPD protegido

Ante esta problemática, ¿cómo se debe tratar la protección de los centros de datos? Desde Fibernet responden de dos maneras: la detección de posibles intrusiones en la fibra "aunque es uno de los

Protección del hipervisor

Las agresiones existen y proseguirán, y más en entornos virtualizados debido al uso compartido de recursos. Incluso el hipervisor está en el punto de mira y éste es un elemento crítico porque soporta la infraestructura de los clientes y actúa como puerta de entrada a la red interna. De acuerdo con el directivo de Bitdefender, "se conocen ataques avanzados altamente especializados, no solo teóricos a nivel del hipervisor, e incluso hemos interceptado algunos, pero sin embargo, no son muy conocidos, ni mediáticos. Suelen aparecer varias vulnerabilidades en las soluciones de virtualización, algunas afectando la asignación de memoria, otros el uso de periféricos compartidos, que se pueden usar como vectores de ataque. Por razones de funcionalidad, la virtualización se basa en el uso compartido de recursos y los atacadores conocen y abusan las debilidades del modelo".

medios más seguros, no es infalible"; y segundo, a través de mecanismos de cifrado en el servidor, en las infraestructuras intermedias.

En Uniway siguen una estrategia de ofrecer la seguridad como un servicio basada en tres pilares: prevención, tratando de evitar los ataques y reduciendo el calibre de estos, pero apoyándose en los procedimientos; monitorización de los sistemas 24 horas de cada una de las redes; y análisis forense.

"Intentamos minimizar el impacto de los posibles riesgos", asevera Francisco Ramírez Soto de Colt. Atendiendo a las necesidades de cada cliente, expresa que poner en el foco en los procedimientos está muy bien pero no hay que olvidar el error humano: si no haces un procedimiento sencillo y suficiente ágil, nadie lo seguirá. "Tienes que ser partícipe de lo que ocurre en tu negocio y minimizar el impacto". Además, aboga por una cooperación de todo el sector, que se hagan públicos los ataques y se aprenda de ellos, como ocurre en aviación cuando se detecta un fallo.

Por su parte, el portavoz de Huawei admite: "Vigilamos constantemente la seguridad del dato porque cualquier dato es susceptible de ser robado y todos los elementos son vulnerables".

En Interoute definen la seguridad por estratos: la física, la lógica y la operativa. "La tecnología nos permite trabajar en arquitecturas distribuidas. No pensemos en la era monolítica. Los sistemas, las redes… se pueden distribuir. Aprovechamos el cloud para el ahorro, pero no para las ventajas tecnológicas que nos ofrecen".

También desde Gigas aluden a la importancia de la seguridad física y lógica, a la par que observan las ventajas de cloud en seguridad como la de democratizar las soluciones para todos los clientes. José Antonio Arribas declara que muchas empresas cuando externalizan su infraestructura a

"Los proveedores tienen miedo de compartir información sobre ataques y vulnerabilidades"

entornos cloud entienden que externalizan su operativa. "La empresa se migra al cloud porque también están externalizando operación", puntualiza.

"Los proveedores invertís en formación de vuestros equipos, pero la seguridad no es una foto estática: hay que invertir en el mantenimiento, en la operación, en el día a día. Por desgracia la operación va por detrás y estamos obligados a ir por delante. Esta parte operacional es tanto más importante", denuncia el directivo de Aryse. En el caso de esta compañía, cauterizan la red para que no haya acceso de un tercero.

Para potenciar la seguridad en el datacenter moderno, Bitdefender, como recalca Horatiu Bandoiu, "tiene en cuenta la funcionalidad y piensa que las soluciones han de ser muy ligeras, independientes de las firmas. Por eso han desarrollado una nube de threat intelligence basada en IA, que responde a 7 billones de interacciones con datos proviniendo de más de 500 Millones de sensores. Tanto esta nube 'inteligente' como los agentes locales tienen varias capas y algoritmos de Machine Learning que les permiten aprender de los eventos de seguridad, potenciando soluciones adaptativas basadas en inteligencia a nivel global".

Por último, Juan Jesús Merino, Sales Regional Director Spain de Bitdefender, confiesa que al usuario le dan miedo nociones como entornos cloud, de virtualización, hiperconvergentes… Además, cuanto más securizo, menos flexible o menos gestionable soy. "Lo que tenemos que ofrecer son soluciones flexibles y fáciles de gestionar".