computing

Autor: REDACCION

VPE: 6.900,00
Difusión: 9.179
Audiencia: 36.716
Documento: 1/2
Archivo: 000399QP
Sección: ESPECIAL SEGURIDAD

Fecha: 25/05/11

La principal preocupación es el cumplimiento normativo y las buenas prácticas de gestión de servicios

Mitos y verdades de la seguridad en la nube

Computing ha reunido a representantes de Arsys, HP, Akamai, Exevi y Ontinet para debatir alrededor de la problemática de la seguridad en entornos de cloud computing, concluyendo que la nube es suficientemente segura, aunque nunca se puede garantizar al 100% una protección completa. En definitiva, de la administración y gestión de la información corporativa sensible se tiene que ocupar la propia compañía, y no responsabilizar exclusivamente a un proveedor de servicios.

● No es ningún secreto que la seguridad figure como uno de los grandes quebraderos de cabeza de las empresas, y supone un freno a la implantación de los entornos de cloud computing. Sin embargo, las compañías deberían tener también presentes otras cuestiones que normalmente suelen pasar desapercibidas, y que son mucho más relevantes y críticas. Así, aunque la protección de la información corporativa es clave, muchas compañías deciden delegar con total exclusividad la responsabilidad del dato a un tercero, cuando realmente de la administración y gestión de la información sensible se debe ocupar la compañía, o al menos estar más pendiente. Estas conclusiones se desprenden de una tertulia organizada por Computing para conocer cuál es la demanda real de este tipo de entornos y si el cloud es o no seguro.

Para comenzar, los participantes pusieron sobre la mesa los problemas para iniciar la transición hacia la nube, "esa problemática se entiende de dos maneras, por un lado, el cumplimiento normativo, ya que hay ciertas regulaciones que limitan el uso de los servicios en la nube, y por otro lado, la seguridad en sí misma, ya que tiene que tener en cuenta criterios como la confidencialidad o integridad, por lo que el problema no es tanto la seguridad, sino la propia gestión de la misma", aclara Félix Martín, gerente del departamento de Servicios de Seguridad de HP. Mientras tanto, Juanjo García, responsable de Grandes Cuentas de Arsys, añade que efectivamente, el cloud no da tantos problemas de seguridad como de cumplimiento de normativas y estándares de calidad, y es que "la seguridad se está convirtiendo en tabú, cuando en realidad es lo menos importante", puesto que pesa más "el desconocimiento: todo el mundo llama cloud a todo, hay mucho temor y desconocimiento". Al respecto, Manuel Pérez, director comercial de Exevi, se muestra de acuerdo, "el problema se reduce a una falta de conocimiento, pero además es imprescindible que los proveedores de ese servicio de cloud, en la modalidad que sea, incorporen buenas prácticas en la gestión del servicio adecuadas para el cliente, porque si los proveedores adquieren buenas prácticas, mejorarán sus servicios y darán más garantías".

Los proveedores deben incorporar buenas prácticas en la gestión del servicio

"El problema", afirma por su parte Miguel Serrano, responsable de Ventas de Akamai, "es que algunas compañías tienen recelo porque muchos proveedores prestan servicios de cloud a nivel usuario y no a clientes corporativos, y tienen dudas a la hora de delegar a un tercero su información". Por ello es necesario "dar confianza y educación a un mercado que tiende a mezclar y confundir conceptos". También hay quien considera al cloud computing como una evolución natural de la informática, como es el caso de Fernando de la Cuadra, director de Educación de Ontinet, confirmando que "se tiene que comprender que la nube es una nueva forma de hacer las cosas, que sí implica seguridad y que funciona de verdad: es más sencillo, y por tanto más barato, más seguro y más cómodo".

¿Cloud o no cloud?

En ocasiones se piensa que la seguridad es un concepto distinto al estar en la nube, pero los proveedores participantes en la tertulia aseguraron que en realidad es lo mismo. Por lo tanto, nadie puede ofrecer garantías al 100%. "Los clientes que no cuenten con políticas adecuadas de contingencia y backup de datos, tienen más probabilidades de per-

computing

Autor: REDACCION

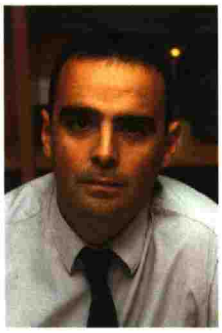
VPE: 6.900,00
Difusión: 9.179
Audiencia: 36.716
Documento: 2/2
Archivo: 000399QP
Sección: ESPECIAL SEGURIDAD

Fecha: 25/05/11

Especial Seguridad

"Recomiendo evaluar a fondo los requisitos del negocio y la oferta, así como evitar delegar toda la seguridad en el cloud".

Félix Martín, gerente del departamento de Servicios de Seguridad de HP

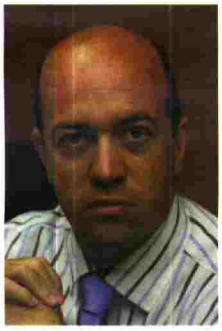


"Hay que pensar y preocuparse más por el tratamiento de la información que en la propia seguridad de la plataforma".

Juanjo García, responsable de Grandes Cuentas de Arsys

"La gestión de la seguridad es responsabilidad del cliente, quien es el encargado final de la administración integral de su información".

Manuel Pérez, director comercial de Exevi



"Hay numerosos casos de éxito de muchas compañías que han decidido no tener en casa un montón de sistemas y procesos".

Miguel Serrano, responsable de Ventas de Akamai

"La nube es bastante segura, pero también hace falta cumplir con las normativas establecidas y con las buenas prácticas".

Fernando de la Cuadra, director de Educación de Ontinet

derlos, estén o no en la nube", sentencia Félix Martín de HP, añadiendo que "el cloud no es seguro ni inseguro, lo que hay que hacer es evaluar a fondo los requerimientos. La oferta cloud es muy variada, hay mucha oferta comercial que puede no tener detrás las garantías necesarias, por ello hay que saber elegir al mejor proveedor".

Además, no tiene por qué trasladarse todo a este entorno, "no todo el core se puede subir al cloud", opina Juanjo García de Arsys. Efectivamente, "la oferta de seguridad tiene que ofrecer los servicios más seguros posibles a un coste mínimo, y el cliente no puede delegar absolutamente todo al cloud porque no se lo puede ofrecer", completa Félix Martín. Mientras tanto, para Manuel Pérez de Exevi, "la seguridad no está siempre más garantizada si se tiene en casa, porque el hecho de no tener un administrador a veces para ciertas compañías es más seguro, especialmente en el caso de las pymes, que tienen por lo general pocos recursos y no pueden contar con servidores de alta disponibilidad". Por esos motivos, "el modelo cloud en sí por naturaleza no es más inseguro; depende de cómo se haga". El problema es que "hay que concebir el cloud como una arquitectura con un enfoque diferente, hay casos de éxito de muchas compañías que han decidido no tener en casa un montón de sistemas y procesos. El mejor camino para tomar decisiones consecuentes es mirar al mercado y comprobar cuál ha sido su experiencia", añade Miguel Serrano de Akamai.

Otro aspecto a tener en cuenta a la hora de optar por una estrategia de seguridad en cloud computing es considerar también a los proveedores de redes de comunicación, según alertó Fernando de la Cuadra de Ontinet, puesto que "son los que están en medio. El cloud implica a tres actores: empresa, proveedor de servicios y proveedor de comunicaciones, y este es un factor que puede ser determinante".

El tamaño de la empresa sí importa a la hora de tomar la decisión de llevar las infraestructuras a la nube, y es que "las necesidades cloud son diferentes, y eso va a determinar la evolución del mercado a corto plazo. Una pyme generalmente demanda no tener nada de infraestructuras por necesidad de costes. Sin embargo, una empresa grande ya tiene la infraestructura montada, y tiene que evaluar qué aplicaciones concretas debe trasladar, porque no todo es susceptible", explica Félix Martín. Siguiendo con esta idea, Manuel Pérez añade que no solamente el tamaño importa, sino también el tipo de aplicaciones que se deseen llevar a la nube.

¿Nube pública o privada?

Igualmente, ha quedado claro que la divergencia entre nubes públicas y privadas no es la seguridad, ya que "con la normativa vigente no es un problema porque hay garantías suficientes", apunta Miguel Serrano de Akamai. Félix Martín añade que "más importante que el debate entre nube pública o privada es el nivel de servicio que se ofrece en la nube. Toda la seguridad desde las infraestructuras a nivel físico y lógico se controla desde dentro de la empresa, y lo mismo sucede con las aplicaciones, pero a medida que evoluciona el nivel de servicio se delega al proveedor esa seguridad. Entonces en conclusión el debate no debe ser si es público o privado, sino el nivel de transferencia que se delega", comenta Martín.

Fernando de la Cuadra quiso poner sobre la mesa el hecho de que "existe miedo, pero ya no tanto por la seguridad sino por la sensación de pérdida de control de los datos". Sin embargo, hay quien considera que ese problema está ampliamente solventado con el outsourcing, como es el caso de Miguel Serrano y Juanjo García.

Una tendencia imparable

Otra cuestión interesante tiene que ver con el tratamiento que se hace con la información, especialmente en aquellos casos en los que el cliente quiera darse de baja del servicio. El problema es que, aunque la LOPD obliga a proceder al borrado total de la información una vez que el cliente se dé de baja, "en otros países no sabemos si esto sucede, lo que podría llegar a ser un problema para una multinacional que decida romper un contrato de cloud computing", asegura Miguel Serrano. Sin embargo, este problema puede solventarse con los proveedores globales, que están preparados para aplicar la normativa en los sitios donde haga falta.

Con todo, la informática en la nube es una tendencia imparable, "no es una moda. Las empresas se podrán subir antes o después, pero acabarán vinculadas en mayor o menor medida al cloud", asevera Manuel Pérez. El resto de participantes se muestra de acuerdo, aunque "todavía queda mucho, porque hace falta acostumbrar a los usuarios", explica Fernando de la Cuadra. "La pelota está más del lado de la oferta: los proveedores tienen que ser capaces de ofrecer el modelo adecuado. El mercado irá evolucionando de acuerdo con la demanda", concluye Félix Martín.