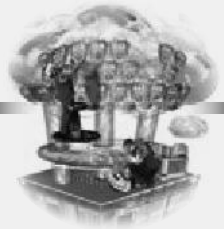


CASB: Salvando *gaps* de seguridad en la Nube

Han pasado casi diez años desde que se empezó a establecer en el mercado el concepto de Computación en la Nube [1] o *Cloud Computing*. En nuestro mundo de la seguridad TI, es un tiempo enorme, que fue suficiente para que muchas tecnologías floreciesen y se agotasen. Sin embargo, este no ha sido en el caso de la Nube. Si ya en 2009 hacíamos referencia en esta revista SIC [2] a la Nube y a las nuevas necesidades de seguridad que surgían en su aplicación, el panorama en 2016 no ofrece la adopción masiva que se prometía. Cierto es que el uso de la Nube sigue popularizándose en España pero por debajo de las expectativas iniciales. Se apunta nítidamente a la Seguridad como barrera de entrada. Un escenario que las soluciones CASB (Cloud Access Security Brokers) quieren resolver. O al menos, mejorar.

Juan Antonio Abánades / Mariano J. Benito Gómez

Estado de adopción de la Computación en la Nube

La Computación en la Nube (*Cloud Computing*) es cualquier cosa menos una recién llegada al mercado TIC. Pocas palabras y conceptos han sido tan mencionados en estos últimos años, tanto por medios especializados como por medios generalistas, de forma que la Nube no es un concepto ajeno, incluso para un ciudadano medio.

Figura 1

La industria ha participado y se ha unido decididamente al uso de concepto. De hecho, la propia evolución del mercado contempló como todos los proveedores de servicio, fabricantes de productos, y compañías proclamaban sonoramente que se habían establecido en la Nube, bien ellos, bien sus productos y/o servicios. En algunos casos, usando el término de forma sonrojante [3]. Actualmente, el término se usa más ajustado a la definición del NIST, comúnmente aceptada [4], y es una opción plenamente establecida más de empleo de servicios TIC, y en ocasiones, la única opción. SaaS, PaaS, IaaS, XaaS… ya son paradigmas asumidos por el mercado.

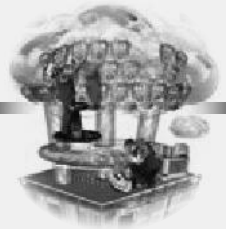
La respuesta por parte de los usuarios a esta potente tracción del mercado desde el lado de la oferta no ha sido igual de entusiasta. En este punto, no hay analista de mercado o proveedor de servicios que no se haya interesado por esta adopción ralentizada de la Nube y no haya realizado su propio estudio. Las conclusiones de estos estudios son variopintas, pero plantean como denominador común de (prácticamente) todos ellos que la seguridad de los servicios en la Nube es una barrera de adopción de estos servicios. En particular, en el mercado español.

De estos estudios, la serie que el Capítulo Español de Cloud Security Alliance [5] lleva realizando desde el año 2013 es particularmente relevante. Los sucesivos estudios de los años 2013 [6], 2014 [7] y 2015 [8] detectan crecimiento en el número de organizaciones que usan servicios en la Nube, que sube desde el 60% en 2013 hasta casi un 80% en 2015.

Figura 2

Contabilizando como usuarios de la Nube a aquellos que tienen algún servicio en Nubes Públicas o en Nubes Privadas, no a aquellos que tienen el total o la parte más importante de sus servicios en la Nube.

El estudio se centra en el mercado español, y ofrece varias explicaciones para este resultado, aparentemente por debajo de las expectativas. En primer lugar, apunta a que las expectativas en seguridad de los usuarios de servicios en la Nube están por encima de la capacidad que tienen los proveedores de satisfacerlas (ver en la **Figura 1** la imagen extractada del estudio CSA-ES de 2015). En segundo lugar, los usuarios prefieren usar servicios de Nube Privada, en particular, cuando tratan de datos sensibles y/o sujetos a legislación. Y la legislación y la limitada capacidad de los proveedores de servicios en la Nube para soportar el cumplimiento por las organizaciones de sus requisitos legales aparece como un tercer elemento relevante, en particular, en lo referente a las limitaciones geográficas que impone la legislación en materia de protección de datos personales.



¿Es pues el estado de adopción de la Nube insuficiente? ¿Está fallando la Nube en proporcionar seguridad a sus usuarios?

Los problemas de seguridad en *Cloud*

Aparte de los conceptos generales de privacidad, integridad y geolocalización de los datos ya citados, y del propio conocimiento de la tecnología *cloud* mencionados, queremos destacar algunos aspectos más concretos y relacionados con la seguridad que desde un primer momento deben ser analizados y considerados a la hora de migrar servicios a la nube.

La falta de visibilidad sobre quién accede a los datos y las aplicaciones es una de las más notorias. Este aspecto está normalmente asociado a la percepción de confianza en las funcionalidades de seguridad que proporcionan los distintos proveedores de servicios en la nube. Incluso en el nivel de garantías acerca de los propios administradores de la nube. Y por otro lado, en caso de ataque, fuga de información o de perdida de disponibilidad, ¿hasta dónde estoy cubierto por mi proveedor?

La propia naturaleza multihuésped (*mutitenancy*) de la Nube Pública es en sí misma un factor de riesgo. ¿Son capaces otros usuarios de la nube de acceder a mis datos, aun en un escenario y/o vector de ataque no previsto? ¿Qué posibilidades existen de que esto ocurra? ¿Qué medidas ha previsto el proveedor de servicios para que no ocurra? ¿Son suficientes? ¿Cómo reaccionará si llegase a ocurrir? ¿Tendría noticia de ello?

Otra circunstancia que puede llevar a reconsiderar nuestro nivel de riesgo es el hecho de que el propio servicio en la Nube se convierta en un apetecible objetivo para los atacantes, por ser punto de concentración de datos de gran valor de múltiples organizaciones. Agravado por la dificultad de los usuarios de cambiar de proveedor de servicio de forma rápida (efecto *locked-in*).

El paradigma CASB asume desde sus fundamentos que ya existe información corporativa fuera de las organizaciones y que esta información reside en servicios de Nube Pública. CASB asume también que esta información puede haber sido movida a la Nube en una decisión corporativa (consciente o no) o por una iniciativa particular de empleados.

Otro aspecto de gran calado es la constancia de que, de facto, los usuarios de las organizaciones pueden usar de forma indiscriminada (y usan) servicios públicos en la Nube, ya sea de correo, almacén de datos, organización del trabajo, etc. Es la considerada Shadow IT ¿cómo podemos controlar o al menos saber qué servicios usan nuestros usuarios y si mueven información corporativa en la Nube? Y todo ello en un entorno IT multidispositivo, multiacceso y móvil.

¿Qué se está haciendo para resolver este problema?

Hasta el momento, hemos mencionado (o quizás, solamente recordado) algunas de las debilidades de la Nube que los usuarios perciben o para las que plantean preguntas. Por lo tanto, los proveedores las conocen y ya han tratado de responder a las mismas.

La primera reacción fue pedir a los usuarios de los servicios confianza ciega en el proveedor, con nula o poca aportación de pruebas y basada en argumentos de potencia de la marca del proveedor de Nube o de difícil verificación por los clientes. Otros proveedores simplemente optaron por ignorar la pregunta y mantener un argumento de "*el servicio es ASÍ, lo tomas como es o lo dejas*".

Las segundas reacciones de los proveedores han sido más sólidas y variadas: algunos proveedores de servicios han acometido la implantación de modelos de certificación (ISO 27001, en su mayoría); otros han reforzado sus campañas de comunicación; otros han hecho bandera del cumplimiento de los requisitos legales por encima de los mínimos establecidos por ley. El asunto incluso ha escalado al ámbito judicial y político, con la sentencia de 6 de octubre de 2015, del Tribunal de Justicia de la Unión Europea sobre Safe Harbour [9], que afecta de lleno a los proveedores de servicios basados en EE.UU.

Entre todas estas reacciones, los autores echamos de menos dos acciones sencillas de señalar (y posiblemente, complejas de implantar) y que no han sido generalmente adoptadas por los proveedores: uno, incluir compromisos de seguridad (de la información, de los servicios, de las personas…) y privacidad en los SLA de los servicios de *Cloud*; y dos, ofrecer facilidades para que los usuarios puedan ostentar derecho de auditar a sus

proveedores (o, al menos, que sea el proveedor quien les facilite la información y evidencias que precisan los clientes para sus propios procesos de cumplimiento legal y/o auditoría).

No son estas las únicas opciones existentes: la vía de las certificaciones de seguridad específicas de entorno Cloud (como CSA-STAR [10]) aún no está suficientemente explorada.

Y ahora también tenemos CASB.

El paradigma CASB

El paradigma CASB se apalanca en la aplicación de tecnología para proporcionar capacidades de detección, prevención y respuesta a incidentes, que mejoren y complementen las capacidades nativas ofrecidas por los proveedores de servicios en la Nube. Estas soluciones han sido desarrolladas de forma independiente por diversos fabricantes, siguiendo esta misma filosofía.

Este paradigma CASB asume desde sus fundamentos que ya existe información corporativa fuera de las organizaciones y que esta información reside en servicios de Nube Pública. CASB asume también que esta información puede haber sido movida a la Nube en una decisión corporativa (consciente o no) o por una iniciativa particular de empleados. Esta información, con las capacidades y nivel de servicio actuales de los proveedores, debe considerarse como no controlable. Sin embargo, las organizaciones desean seguir conociendo qué pasa con su información, porque además en ocasiones deben cumplir requisitos legales y/o contractuales para controlar la información.

El principal factor motivador para el empleo de un CASB debe ser la existencia de una estrategia global de uso de la nube.

Aun así, la organizaciones reconocen las ventajas que puede proporcionar la nube y quieren apoyarse en ellas, para lo cual necesitan esa capacidad de control adicional.

Si los proveedores no proporcionan los controles adicionales necesarios, se necesita algo más y ese algo más es un CASB.

¿Qué es CASB?

La sigla CASB hace referencia a los términos *Cloud Access Security Broker* (por cierto, de difícil traducción al castellano). Se trata de un término ideado por Gartner, inicialmente centrado en determinadas funcionalidades de seguridad que, debido a su éxito y a la propia evolución de los fabricantes, el mercado está aplicando para abarcar todas aquellas soluciones que proporcionan seguridad para servicios de Nube pública, incluyendo los conceptos de visibilidad, cumplimiento, seguridad de los datos y protección frente a amenazas.

Los términos usados en el propio concepto CASB son muy aclaratorios:

- **Cloud**. Su objetivo es la información en los Cloud Service Providers y además el propio CASB puede proporcionarse desde la nube.
- **Access.** Sobre todo en su concepción inicial, son soluciones orientadas al control de acceso, su autorización y la autenticación.
- **Security**. Se trata de permitir o no el acceso, de registrar y tratar los accesos y de aplicar inteligencia sobre los mismos.
- **Broker.** No se trata de mover la información ni de cambiarla de sitio, sino de actuar como pasarela de acceso y dar visibilidad.

En los últimos años se ha hablado incluso de solapamiento de funcionalidades entre los CASB puros y otros sistemas con otras denominaciones, tales como los llamados SPSM (*SaaS Platform Security Management*), más enfocados a arquitecturas API fuera de banda o los CDPG/CEG (*Cloud Data Protection Gateway/Cloud Encryption Gateway*), centrados en el cifrado de la información que se lleva a la nube.

¿Necesito un CASB?

El concepto CASB parece interesante, pero ¿cuándo necesita un CASB una organización?

En primer lugar es necesario ser consciente del uso de Nube que se realiza en la organización y la utilidad buscada con él. Podemos sacar conclusiones partiendo de varias fuentes: resultados de auditorías, los accesos en cortafuegos y *proxies*, trazas en IPS y otros dispositivos de monitorización… e incluso revisando adquisiciones de estos servicios en el departamento de compras.

En ocasiones, la adopción de CASB está ligada a un servicio específico, como por ejemplo un gran proyecto de migración a correo en la nube. Pero es cuando son múltiples los servicios en la nube en uso o en proyecto de uso, cuando un CASB se hace casi imprescindible.

En todo caso, el principal factor motivador para el empleo de un CASB debe ser la existencia de una estrategia global de uso de la nube.

En ocasiones, la adopción de CASB está ligada a un servicio específico, como por ejemplo un gran proyecto de migración a correo en la nube. Pero es cuando son múltiples los servicios en la nube en uso o en proyecto de uso, cuando un CASB se hace casi imprescindible, ya que aunque los proveedores cada vez proporcionen más controles, lo hacen exclusivamente para sus servicios; tener un punto centralizado de visibilidad y aplicación de políticas es una ventaja evidente.

Sea cual sea el caso, dada la situación del mercado, aún inmadura, es recomendable tomar ciertas precauciones a la hora de elegir un CASB. Lo primero es saber si necesitamos proteger servicios en IaaS, Paas o SaaS. Existen notables diferencias de cobertura, siendo mayor

en SaaS que en el resto de modalidades. El siguiente paso es aplicar la medida de seguridad adecuada al riesgo y a nuestras necesidades: visibilidad, cumplimiento, seguridad de los datos y/o protección frente a amenazas, teniendo en cuenta que las soluciones CASB actuales suelen estar claramente especializadas en una de las áreas.

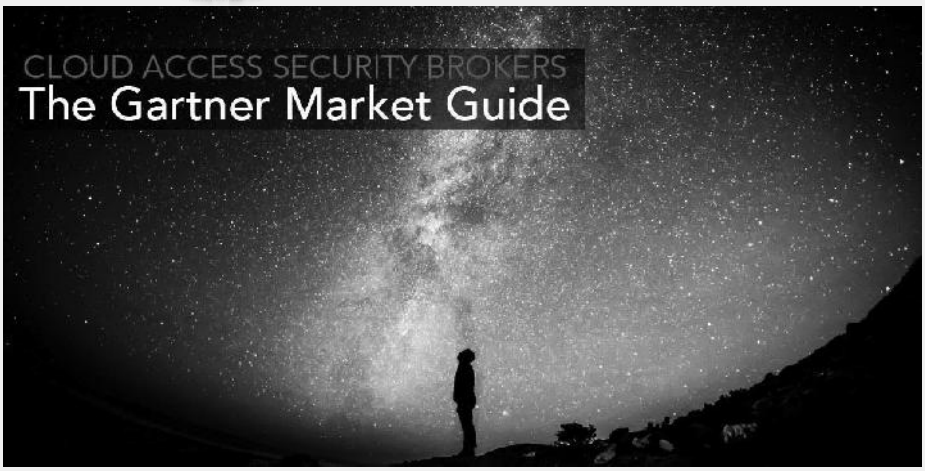
Hay diversos aspectos técnicos relacionados con el despliegue de estas soluciones, que afectan mucho, tanto a las funcionalidades que permiten o no como al grado de transparencia de cara a los usuarios.

Modelos de despliegue

Básicamente existen tres formas de controlar el acceso a los servicios en la nube: empleando un *gateway,* integrando *logs* de otros dispositivos y mediante API. Algunas soluciones son capaces de combinar estos métodos para cubrir más funcionalidades. El despliegue empleando *gateway* fuerza el paso del tráfico hacia la nube por este *gateway* (ya sea *inline*/*offline*). Se trata de una solución potente, siempre cuando sea posible esta redirección de tráfico al *gateway*. Para determinadas capacidades, como el cifrado, resulta de gran ayuda.

La integración con *logs* de terceras partes, tales como *firewalls* y proxies, resulta más interesante si el foco del proyecto CASB está en la visibilidad de la información y/o en la detección de Shadow IT.

La integración mediante API depende en gran medida de las funcionalidades que permiten los proveedores con dicha API y del grado de *partnership* del fabricante del CASB con dichos proveedores. Con este método el CASB se conecta directamente con el proveedor y realiza las acciones pertinentes de seguridad, resulta cómodo y transparente, aunque aún no permite cubrir todas las necesidades de protección y control. Finalmente tendremos que elegir entre equipo *on-premise* o servicio desde la propia nube para nuestro CASB.



Dada la situación del mercado, aún inmadura, es recomendable tomar ciertas precauciones a la hora de elegir un CASB. Lo primero es saber si necesitamos proteger servicios en IaaS, Paas o SaaS. Existen notables diferencias de cobertura, siendo mayor en SaaS que en el resto de modalidades.

Conclusiones

Como conclusión, el paradigma CASB ofrece a un CISO una nueva herramienta tecnológica con la que aumentar su arsenal de soluciones para los problemas de su organización.

CASB ofrece un nuevo enfoque para tratar de resolver el aún pendiente problema de la seguridad y el control de la información en la Nube, proporcionando la capacidad de control y de seguridad adicional que los proveedores no facilitan y que las organizaciones pueden necesitar para hacer honor a sus compromisos contractuales, políticas corporativas y requisitos legales aplicables.

CASB no es sin embargo la única opción. Es un complemento más a las buenas prácticas en seguridad de la organización, a otras líneas de trabajo en marcha (formación, certificación, colaboración con los proveedores), y sobre todo, para reforzar y soportar la implantación efectiva de la necesaria estrategia de uso de la Nube de las organizaciones. ■

Juan Antonio Abánades
Jefe de Sección
Tecnologías de Ciberseguridad
GMV Secure e-Solutions
jabanades@gmv.com

Mariano J. Benito Gómez
CISO
GMV Secure e-Solutions
Coordinador. Cloud Security Alliance, Spanish Chapter
mjbenito@gmv.com

REFERENCIAS

[1] https://es.wikipedia.org/wiki/Computaci%C3%B3n_en_la_nube#Historia
[2] Revista SIC, Número 86, Septiembre 2009. "Cloud Computing ¿Nubarrones en La Nube?"
[3] http://dilbert.com/strip/2011-01-07
[4] NIST SP 800-145, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
[5] www.cloudsecuriyalliance.es
[6] https://www.ismsforum.es/ficheros/descargas/estudio-del-estado-de-la-seguridad-en-cloud.pdf
[7] https://www.ismsforum.es/ficheros/descargas/csa-es-2014-cloudsecuritystateoftheart20141119.pdf
[8] http://www.ismsforum.es/ficheros/descargas/csa-es-pe-2015-estudio-estadodelarte-nube-es.pdf
[9] http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117es.pdf
[10] https://cloudsecurityalliance.org/star/e