Riesgos en el entorno Cloud. Una perspectiva holística de los riesgos

El pasado lunes, se celebró en Bilbao uno de los eventos más importantes relacionados con la ciberseguridad (Basque Cybersecurity Day) y como no era de extrañar, en prácticamente todas las conferencias se citó de una forma u otra los posibles riesgos asociados a las tecnologías emergentes (entre las cuales se incluye, el Cloud Computing) . No obstante, el enfoque que se le dio a los riesgos tecnológicos era radicalmente distinto a la opinión que tenía acerca del tema.

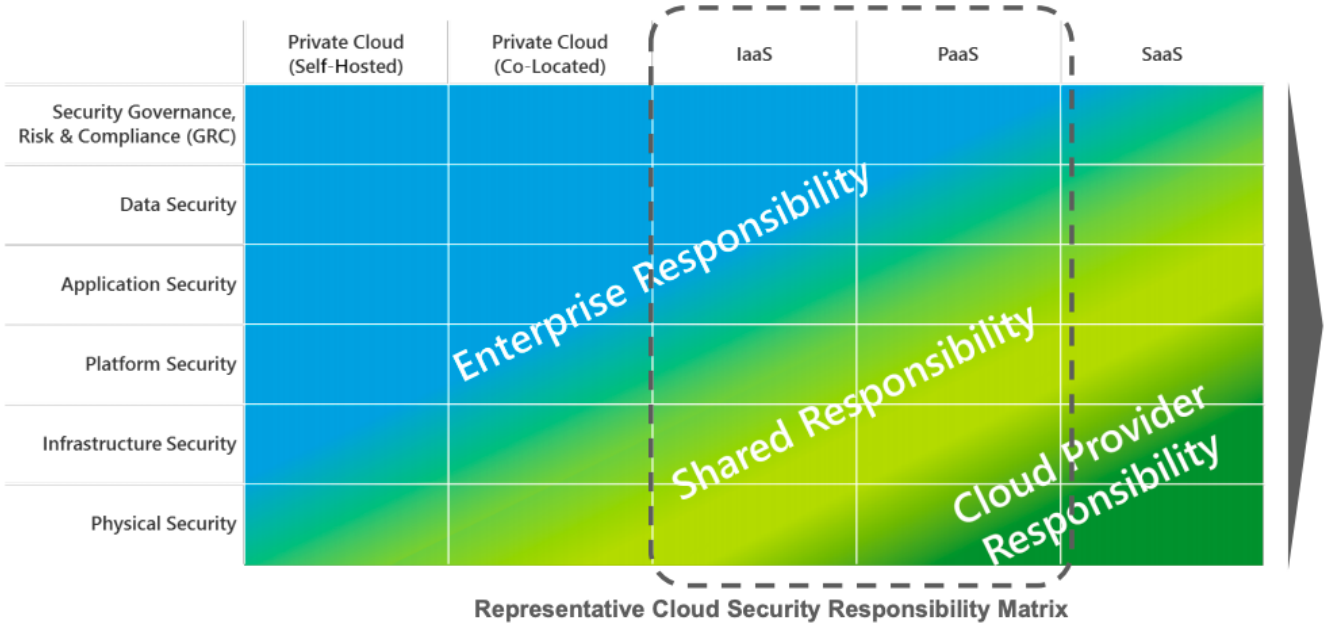
Por lo tanto, el post que tenía pensado escribir la semana pasada ha sido totalmente reescrito, y he decidido explicar el framework propuesto por ISACA [1] para abordar los riesgos de la tecnología del Cloud Computing pero enriquecido con todas las aportaciones de relevancia que escuché en el ciclo de conferencias.

Entre todas las conferencias hubo una que me llamó la atención en particular, la realizada por la actual CEO de Siemens España, Rosa García [2]. En esta conferencia se abordó la gestión de los riesgos desde un punto de vista holístico y destacaba como en el punto en el que nos encontramos hoy en día los riesgos IT se deben entender como una parte más de la estrategia empresarial. En pocas palabras, cuando se habla de seguridad en estos términos, no solo nos referimos a la parte de la tecnología o la parte "ciber", sino a todo el entorno que compone la seguridad (la seguridad de los datos y la información, el plan de gobernanza IT, los modelos de fallo y de contingencia, la gestión del cambio, etc …).

Por otra parte, otro de los puntos relevantes (especialmente para entender el mundo de los riesgos del Cloud Computing), es el referido al papel de los proveedores. La robustez de la seguridad de una organización, viene marcado por el eslabón más débil de la cadena y muchas veces este eslabón ni siquiera es parte central de la organización como es el caso de los proveedores (en los cuales se incluyen los proveedores de servicios cloud). En este punto, son destacables los datos de la encuesta elaborada por KPMG [3] donde cita como el 44% (12 puntos más que en el año 2017) de los encuestados no posee ningún tipo de instrumento para el control del framework de seguridad con los proveedores. Además el 34% de los encuestados, tampoco poseen ningún tipo de control de ciberseguridad en los contratos de terceros y finalmente, el 59% ni siquiera tienen el derecho contractual a la realización de una auditoría

del proveedor.

En definitiva, la adopción del cloud computing muchas veces va ligada a contratos con terceros, los proveedores de servicios. No obstante, muchas de las empresas no realizan ningún tipo de supervisión o control de estos y ello supone un claro riesgo para la seguridad de sus empresas. Para explicarlo mejor, me valdré de la siguiente infografía elaborada por Deloitte.[4]



Representative Cloud Security Responsibility Matrix

La infografía representa el nivel de responsabilidad que debe adquirir una compañía en función de su grado de dependencia de terceros. Es decir, una empresa cuyos sistemas estén totalmente gestionados a nivel interno, es totalmente responsable del sistema pero una empresa cuyo entorno está totalmente alojado en la nube, debe ceder esa responsabilidad al tercero.se

Pero siempre hay que tener en cuenta un hecho crucial, aunque cedas la responsabilidad de tu sistema a un tercero, la responsabilidad de los datos que se gestionan en él siempre va a seguir siendo tuya. Pongamos como ejemplo la seguridad de un teléfono móvil: la seguridad del terminal es responsabilidad del fabricante. Sin embargo, el usuario sigue siendo responsable de la forma en la que use este terminal y en el mundo Cloud sigue siendo igual.

Por otra parte y siguiendo con lo planteado inicialmente, me gustaría listar cuales son los riesgos más comunes que deben afrontar las empresas en el mundo del Cloud. El próximo listado de riesgos se extrajo de un informe de ISACA donde se mencionaba una encuesta elaborada por la Cloud Security Alliance [5].

En primer lugar, los CSP (Cloud Service Providers) suelen ofrecer APIs públicas para el acceso a los sistemas en la nube, desde la autenticación y gestión de credenciales hasta la monitorización del uso de recursos. No obstante, estas APIs pueden suponer una puerta de entrada a posibles vulnerabilidades.

En segundo lugar, el documento destaca un problema que mi compañero Pablo ya

ha tratado en sus respectivos posts con mucho más detalle, los Insiders Threads. En este caso, el problema se extiende no solo al personal propio de la organización sino al personal perteneciente por ejemplo a los CSP. Este elemento resulta crucial para entender la importancia que tienen los controles al personal implicado de la organización, especialmente a las relaciones con terceros.

Por otro lado, en la mayoría de servicios en la nube los recursos computacionales son compartidos por diferentes usuarios y organizaciones. A pesar de poder contar con elementos de seguridad que permiten aislar el acceso a estos recursos, siempre pueden ser un foco de conflicto.

El cuarto y último aspecto a tratar entre los principales riesgos asociados está relacionado con la pérdida de datos e información. En este punto, hay dos riesgos que hay que tener en cuenta con los datos que se alojan en la nube: la posible pérdida de datos y la aún peor posible filtración de los mismos. Actualmente, las organizaciones y sus estrategias de negocio están completamente orientadas a los datos y por ende, este punto debe ser supervisado y auditado con especial atención.

En definitiva, los servicios alojados en la nube suponen un nuevo reto a las organizaciones que lo incorporan. Además, a pesar de que los riesgos relacionados con la tecnología no son nuevos, el paradigma del cloud computing acrecienta estos riesgos de una forma u otra como ya he mencionado anteriormente.

Por último, me gustaría adelantar el contenido del próximo post donde expondré un caso práctico elaborado por ISACA explicando las medidas y controles que se deben tomar en las organizaciones que decidan adoptar esta tecnología.

Fuente consultadas:

[1] «IT Control Objectives for Cloud Computing – Information Security ….» https://www.isaca.org/chapters2/kampala/newsandannouncements/Documents/IT%20contro%20objectives%20for%20Cloud%20computing.pdf. Se consultó el 10 noviembre del 2018.

[2] García, R. (2018). *Perspectiva del CEO en la gestión del Riesgo Empresarial*. Conferencia realizada en el Basque Cybersecurity Day.

[3] «Clarity on Cyber Security – KPMG.» 25 mayo 2018, https://assets.kpmg.com/content/dam/kpmg/ch/pdf/clarity-on-cyber-security-2018.pdf. Se consultó el 10 noviembre del 2018.

[4] «Cloud Cyber Risk Management – Deloitte.» https://www2.deloitte.com/content/dam/Deloitte/us/Documents/about-deloitte/us-allian-deloitte-cloud-cyber-risk-considerations-amazon-web-services.pdf. Se consultó el 10 nov.. 2018.

[5] «Top Threats Cloud Computing V1.0 – Cloud Security Alliance.» https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf. Se consultó el 10 noviembre del 2018.

[6] «Risk Landscape of Cloud Computing – isaca.» https://www.isaca.org/Journal/archives/2010/Volume-1/Pages/Risk-Landscape-of-Cloud-Computing1.aspx. Se consultó el 10 noviembre del 2018.