White Paper

Preguntas para Formular a su Proveedor de Servicios en Nube

Conozca cómo serán protegidos sus datos en la nube

intel Security

Contenido

Emplear a un proveedor de servicios en nube (CSP) para Infraestructura como Servicio (IaaS), Plataforma como Servicio (PaaS) o Software como Servicio (SaaS) ya es una práctica común para la TI empresarial. Es esencial realizar la mejor elección de proveedores y servicios, en particular en lo que se refiere a las prácticas de seguridad, privacidad de datos, y capacidades operativas. Asegúrese de colocar a los partners potenciales de Proveedor de Servicio de Nube (CSP) bajo el microscopio, formulándoles las preguntas adecuadas sobre cómo van a proteger su información más esencial.

Conforme la demanda de servicios en nube continúe disparándose, encontrar el CSP adecuado (o múltiples proveedores) es una responsabilidad importante para la TI empresarial y para los profesionales de la seguridad. Los CSPs vienen en todas las formas y tamaños, desde enormes organizaciones mundiales que ofrecen una amplia gama de servicios en la nube hasta las pequeñas tiendas especializadas en un número limitado de funciones. Incluso existen servicios de correduría de nube que agregan servicios de nube de diferentes proveedores a través de diferentes modelos de entrega de servicios - desde integradores de sistemas y compañías de externalización, hasta proveedores independientes de software y distribuidores de valor añadido.

Esto hace que sea difícil, pero obligatorio, el que las organizaciones escojan dentro de este laberinto de opciones de CSP. Para normalizar las muchas diferencias entre los proveedores potenciales, usted tendrá que formularles preguntas consistentes sobre cuestiones clave. La seguridad debe estar en, o cerca de, la parte superior de la lista mientras selecciona los partners CSP adecuados en su jornada hacia la nube.

Los aspectos esenciales de la seguridad deben ser concentrados en una serie de preguntas cuando se encuentra seleccionando a su proveedor. Estas preguntas le ayudarán a determinar qué CSPs realmente comprenden todas las preguntas relacionadas con la seguridad y sus consecuencias, y aquellos que tienen un enfoque más consistente con las prioridades, prácticas y tolerancia de riesgo de su organización. Dedicaremos mucho del trabajo a preguntas concretas en tres áreas: seguridad, privacidad y operaciones, todo en relación con la protección de datos. Si usted sigue estas sugerencias y filtra a través del lente de su propia experiencia, buen juicio, y consejos de colegas que ya han pasado por este proceso, incrementará las probabilidades de encontrar uno o varios CSP que le ayudarán a garantizar una seguridad robusta para sus activos de datos más importantes.

Potencial de Investigación de CSPs a Alto Nivel

Un primer paso esencial es evitar realizar suposiciones sobre lo que es y no es seguridad con respecto a un proveedor. Cada proveedor es diferente, con diferentes normas, acuerdos de nivel de servicio (SLA), términos y condiciones. Asegúrese de comprender completamente a lo que cada proveedor de servicio se compromete con usted, el cliente.

En segundo lugar, asegúrese de formular preguntas acerca de cómo la seguridad y privacidad de los datos se manejan. Usted necesita saber qué esperan que su organización haga, qué harán ellos como proveedores, y cómo lo harán, entre otras cosas.

En tercer lugar, analice atentamente sus términos y condiciones. Por supuesto que a nadie le gusta leer las muchas páginas de la impresión del contrato, pero usted necesita comprender los detalles para poder elegir un proveedor que ofrezca el servicio adecuado y le proporcione el nivel de confianza adecuado. Así que no eluda sus obligaciones en esta área, no haga simplemente clic en "aceptar" y siga adelante.

Entre y observe detenidamente las diferentes secciones dentro de los términos y condiciones, y concéntrese en los aspectos de datos de esos detalles.

En cuarto y último lugar, no asuma que cada servicio en nube tiene las mismas guías y objetivos de entrega de servicio, incluso con el mismo proveedor. Analice cuidadosamente los términos y condiciones de cada servicio. Revise todos ellos, y no haga suposiciones sin sustento, o usted puede acabar teniendo una enorme y costosa sorpresa.

Preguntas de Seguridad

La buena noticia es que las preocupaciones de la seguridad en la nube han disminuido considerablemente en los últimos años conforme los CSPs desarrollan un historial de prácticas de seguridad exitosas. Aún así, muchos altos ejecutivos, así como muchas juntas de directores, están preocupados acerca de si los datos de la organización son realmente seguros en la nube. Usted debe formular preguntas específicas de CSPs potenciales a fin de lograr el alto nivel de seguridad y confianza que se necesitan para minimizar las preocupaciones y los riesgos.

¿Quién tiene acceso a mis datos, tanto física como virtualmente?

El acceso físico es totalmente diferente del acceso virtual. Es importante preguntar acerca de ambos tipos de acceso.

- ¿Qué postura de seguridad tiene implementada la organización cuando se accede a su centro de datos?
- ¿Su personal tiene autorización de seguridad y está protegiendo el acceso físico a los datos de las personas de afuera?
- ¿Cuáles son las políticas de la institución o del centro de datos y cómo están protegidos?
- ¿Quién tiene acceso a los datos de manera virtual? ¿Desde dónde se accede y por qué?
- ¿Cómo están accediendo a ellos? ¿Utilizan VPN y los datos están cifrados? Si están cifrados, ¿cómo se brinda seguridad a las claves de cifrado?

¿El CSP externaliza el almacenamiento de datos?

Muchas compañías utilizan compañías de externalización para prestar servicios, pero es posible que su CSP esté externalizando sus datos hacia otra ubicación o incluso hacia otro proveedor. Si es así, usted necesita decidir si usted está de acuerdo con esa situación.

¿Cómo maneja el proveedor las peticiones legales para la revisión de los datos?

Si dichas solicitudes provienen de sus clientes o de cuerpos gubernamentales derivadas de cuestiones legales o reglamentarias, el manejo de estas peticiones requiere delicadeza, experiencia y sensibilidad para las políticas de gobierno corporativo, así como con los mandatos de conformidad. No es inaudito que la calidad de sus datos se vea impactada por peticiones legales, y usted necesita entender la trazabilidad de los datos y cómo se manejan las peticiones.

¿Cómo y cuándo se suprimen los datos?

Porque cada proveedor es diferente, es importante comprender que existen complicaciones de almacenamiento dada la cantidad de datos que recorren el mundo hoy en día. Usted querrá comprender qué tantos datos son almacenados por su CSP y, en particular, cuántos de sus datos específicos se almacenan. Además, pregunte cuánto tiempo serán almacenados sus datos, cuándo serán eliminados y cómo se toman las decisiones de eliminación de datos.

¿Cuál es la arquitectura de datos?

Concretamente, pregunte si están aislados sus datos de los de otros clientes en un entorno de múltiples inquilinos. Pida a su proveedor explicar cómo se segmentan sus datos de los datos de otros clientes y cómo podría cambiar esto en el futuro.

¿Qué certificaciones y/o auditorías de terceros se realizan?

Las certificaciones le proporcionarán una mejor comprensión de qué tan maduro es el proveedor, qué cosas le preocupan, y si está comprometido con la mejora continua. Desde una perspectiva de auditoría de terceros, usted deseará saber con qué frecuencia el proveedor está en busca de cambios y asegurarse de que está cumpliendo con las expectativas de sus clientes y proveedores.

Preguntas de Privacidad

La seguridad y la privacidad están estrechamente entrelazadas, pero hay una serie de preguntas únicas para la privacidad que usted debe formular a su CSP. Y las preguntas acerca de la privacidad, aunque evidentemente están arraigadas en la conformidad, no se limitan sólo a temas reglamentarios.

¿Qué datos se recolectan desde nuestra organización y cómo se mantienen privados?

La privacidad es un poco diferente para cada organización, por lo que es especialmente importante definir lo que la privacidad significa para los interesados clave dentro de su organización.

¿Para qué se utilizan los datos?

A menudo es sorprendente conocer los distintos usos de los datos, algunos de los cuales lo sorprenderán o quizás incluso le conciernen. Asegúrese de que su CSP comprenda sus políticas de gobernanza de uso aceptable de datos.

¿Cuánto tiempo conserva el CSP esos datos?

Los términos y condiciones podrán indicar que los datos se recolectan durante 30 días, o quizás 90 días o incluso un año. Pero eso no necesariamente determina cuánto tiempo la organización puede mantener sus datos. Esto será muy diferente para cada proveedor, para cada servicio, y por cada grupo de datos recolectados. Usted podría tener datos hechos anónimos, almacenados y utilizados para probar durante muchos, muchos años, así que asegúrese de preguntar acerca de la retención.

¿El CSP cifra sus datos?, ¿de qué manera?

Es importante saber esto, para garantizar que cualquier cosa que usted considere confidencial o privada o que de otra manera le preocupe, no sea aprovechada para otros usos por el CSP.

¿Donde se almacenan los datos?

¿Tiene reglas o normas de almacenamiento de datos geográficos que los CSPs deban seguir? Los proveedores de servicios de nube está almacenando datos en muchas ubicaciones diferentes para muchos fines diferentes, y usted necesita comprender eso y cómo se alinea con sus prácticas de negocios.

¿Los datos se acumulan y se transmiten a otras entidades internas o externas?

Todos sabemos que esto es generalizado en toda Internet y que hay muchos diferentes programas de opciones de entrada y salida. Es muy importante entender si el CSP comparte datos con alguien, cómo los comparte, cuándo los comparte, el motivo por el que los comparte, y donde se transmiten.

Preguntas Operativas

Más allá de la seguridad y la privacidad, las actividades de sus CSPs se cruzarán con muchas operaciones cotidianas de su organización. Comprender esto le ayudará a determinar si las maneras en que los CSPs manejan sus datos y sirven a su personal, brinda soporte o causa impacto en sus operaciones.

¿Cuál es el modelo de redundancia de arquitectura de almacenamiento y de la base de datos?

La redundancia en particular, es importante porque se enfoca en cómo tratar con el fallo de infraestructura sin afectar la continuidad de negocios.

¿Cuál es la frecuencia de elaboración de copias de seguridad?

Todos hemos oído este mantra desde que se introdujeron los equipos de cómputo: copia de seguridad, copia de seguridad, copia de seguridad. Y es muy importante entender la frecuencia con la que los CSPs hacen copias de seguridad. Obviamente, mientras más frecuentes sean las copias de seguridad, mejor será la redundancia de usted. Facilitará que su proveedor restaure el servicio hacia un punto específico de tiempo y si no hay ningún fallo.

¿Cuál es el tiempo de recuperación en caso de fallo?

Es inevitable que su proveedor tendrá un problema en algún momento. Es imprescindible comprender cuánto tiempo tardará el CSP para recuperar sus datos. ¿En minutos, horas, días o semanas? Los errores ocurren, pero usted necesita saber cuánto tiempo pasará para recuperarse de ese fallo cuando está usando un proveedor de servicio.

¿Cómo podemos acceder o descargar datos desde el servicio?

Esta pregunta le ayuda a comprender las diferentes filosofías de los proveedores de servicio y a obtener un mejor conocimiento de cómo esos pasos se alinean o entran en conflicto con sus procesos operativos.

¿Qué herramientas analíticas están disponibles para ver nuestros datos?

El proveedor de servicios puede tener una gran cantidad de datos en su servicio, y puede ser que usted no desee sacar todos esos datos y aprovechar herramientas de análisis de terceros para comprimirlos y darles sentido.

Es mucho más beneficioso si el proveedor de servicios le ofrece este servicio para que usted pueda hacer la agregación y el modelado de los datos.

Si hay corrupción de datos, ¿cuál es la máxima pérdida de datos que podemos esperar?

Esto debe vincularse con las preguntas de redundancia y recuperación, mencionadas anteriormente, y debe estar estrechamente alineado. ¿Cuánto tiempo tardará la recuperación de un fallo de datos, y cómo afectará realmente ese proceso de recuperación a la calidad de los datos?

Resumen

Estas preguntas sugeridas deben ayudar en el proceso de identificar, evaluar, seleccionar y trabajar con los CSPs. Estas preguntas también actúan como importantes comprobaciones de realidad en su evaluación continua sobre el rendimiento de su CSP actual, y sirven como un conjunto de nivel periódico para los nuevos servicios que pueda necesitar a medida que su empresa evolucione.

Recuerde que el seleccionar un CSP no es una tarea trivial. El realizar la selección incorrecta puede tener un gran efecto, incluso potencialmente catastrófico, en la organización si la preparación de seguridad el CESP no cumple las necesidades de usted, ahora y en el futuro. Al mismo tiempo, el seleccionar los CSPs adecuados puede ayudar a su organización de muchas maneras, en un sentido económico, con la asignación de recursos internos, con respecto a la confianza en la seguridad y la integridad de sus datos, y mucho más.

Conforme usted avance en el proceso de evaluación de CSPs potenciales, estas preguntas de seguridad, privacidad y operativas pueden mejorar su confianza en la selección final de sus partners CSP.

Por supuesto, estas preguntas deben ser ponderadas y ajustadas para que reflejen el modelo de negocios de su organización, sus prioridades operacionales, y su cultura corporativa. Pero estas preguntas representan una forma efectiva y eficiente para tomar decisiones más inteligentes para seleccionar partners en la medida en que aumente su uso de los servicios en la nube.

Pueden parecer muchas preguntas, pero a largo plazo usted agradecerá haber pasado tiempo repasándolas. Es mucho mejor tener la información que estas preguntas pueden brindar a tener que adivinar las respuestas.

Para obtener más información, vaya a **www.intelsecurity.com/cloudsecurity**.

Acerca del Autor

Jamie Tischart
CTO de Nube/SaaS de Intel Security

Jamie Tischart es el CTO de Nube/SaaS de Intel Security, es el responsable de dirigir la creación de las soluciones de nube de próxima generación de Intel Security y de crear una ventaja competitiva sostenible. Él ha trabajado en Intel Security durante más de 10 años en diversas funciones técnicas, incluyendo la Dirección Sénior de Ingeniería, Operaciones e Investigación de Nube y la Dirección Sénior de Ingeniería y Operaciones de Calidad de McAfee® Labs. Antes de unirse a lo que entonces era McAfee, Tischart ocupó varios puestos ejecutivos, de arquitectura de aseguramiento de calidad, de administración y de ingeniería en compañías como MX Logic, Blackbaud, Openwave, Newbridge Networks y Corel. Tischart Posee una maestría de la Universidad de Aspen. Vive con su familia en Colorado, donde ejerce sus pasiones en el desarrollo de SaaS, Cloud DevOps y operaciones de nube, junto con Agilidad para el Coaching y Liderazgo en Ingeniería de Calidad, mientras disfruta del esquí, la escritura y el hockey. Es un voluntario activo en muchas organizaciones, como Habitat for Humanity, Ronald McDonald House Charities of Denver, Inc. y Food Bank of the Rockies.

Acerca de Intel Security

Intel Security, con su línea de productos McAfee, se dedica a hacer que el mundo digital sea más seguro para todos. **www.intelsecurity.com**. Intel Security es una división de Intel.

McAfee. Parte de Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com