SaaS vs Software Instalado Localmente, La Verdad Detrás De Los Mitos De Seguridad

Existen grandes discusiones sobre el SaaS vs software instalado localmente. Se habla de una gran variedad de mitos, siempre dando el punto a favor en cuanto a los proveedores de SaaS.

Este tipo de discusiones siempre llegan a la conclusión (errónea) de que aquellos interesado por el bienestar económico de la empresa suelen ser paranoicos acerca de los **problemas de seguridad del software de nube**. Sin embargo, son pocos los que se atreven a estudiar las empresas que brindan este tipo de soluciones tecnológicas, y aquellos que no hacen este trabajo siguen teniendo la paranoia en cuanto a la seguridad.

A continuación te mostraremos 3 puntos que debes evaluar al momento de adquirir un servicio de SaaS con una empresa, o si deseas montar tu propia estructura.

1. Acceso no autorizado al hardware de alojamiento

Los controles internos deben ser evaluados para asegurar que los empleados no pueden acceder a los servidores ó bases de datos que albergan los datos mas importantes de los clientes o la empresa. Curiosamente, en varias de las empresas que

brindan este servicio, no cuentan con este control interno.

Existe una clara ventaja para las empresa que dar este servicio y que de forma externa pueden combatir este riesgo. Pueden aplicar controles como el acceso biométrico, dactilar, etc. En realidad, para personas como tu, y cualquier otro que no este relacionado con la empresa, conseguir el acceso físico en la mayoría de los centros de datos es casi tan difícil como entrar en Fort Knox.

2. Acceso no autorizado a través de ataques de penetración

- Este es el mayor riesgo conocido, aunque no es el más grande riesgo. Los medios de comunicación a menudo se centran en las empresas de alto perfil que han sido hackeadas. Por lo general no todo el sitio, o incluso los datos sensibles no son vulnerados en su totalidad. La evaluación de la protección del sitio de alojamiento es importante.

---

3. Entrada no autorizada al sitio de alojamiento

Este es el mayor riesgo de **seguridad de aplicaciones**, simplemente porque hay la mezcla de ingeniería social (por lo general a través de phishing) y otros riesgos de penetración

externas. Ambos pueden mitigarse asegurando con fuertes **controles de contraseña**, así como la autenticación de dos factores.

Además, es necesario evaluar la tecnología y la infraestructura desde el punto de vista del rendimiento. ¿Puede la aplicación alojada cumplir con los tiempos de respuesta requeridos, tanto en condiciones normales de uso y de recuperación de desastres?

Mientras que cualquier aplicación tiene la posibilidad de **tener un acceso no autorizado**, en **SaaS** no representa mayor amenaza que el software internamente alojado, y en muchos casos es más seguro. Es bueno que leas los comentarios para asegurarte de la reputación de los proveedores de esta tecnología.