arsys

5 maneras de mejorar la seguridad en el Cloud

Cinco maneras de mejorar la seguridad en el Cloud desde la perspectiva y según la responsabilidad del cliente.

La **seguridad en el Cloud** es muy elevada. Los estándares de seguridad adoptados y las eficaces medidas que se ponen en marcha permiten desterrar, de una vez por todas, los mitos relacionados con este tema.

Repetir las **ventajas y beneficios del Cloud** en cuestión de costes, de flexibilidad, de eficiencia y de tantos otros aspectos positivos para las empresas y organizaciones sería repetirnos, así que hoy nos centraremos en un aspecto muy importante relacionado con la seguridad en la Nube, pero pocas veces tratado como tal.

Cuando una empresa decide migrar una parte de sus sistemas, o todos, a la Nube, contrata Servicios de Almacenamiento para sus datos, y otros servicios que necesita para realizar las tareas propias de su actividad. Al hacer esto, está alojando sus datos en máquinas físicas de un tercero (o de un conjunto de terceros).

El proveedor es el dueño de los equipos, el cliente tiene el control de sus servicios, pero **los datos y las aplicaciones que se almacenan en la Nube son exclusiva responsabilidad del cliente**. ¿Qué implicaciones tiene esto? ¿Cómo podemos mejorar la seguridad en la Nube desde esa perspectiva?

La mejor manera de mejorar la seguridad en la Nube es no dar nada por sentado en cuestiones de seguridad. Sí, un proveedor de confianza, con experiencia y con elevados estándares de calidad y certificaciones de seguridad es el mejor aliado posible. Y es una garantía en cuestiones de seguridad: no hay otro partner mejor para una empresa. Sin embargo, en el mundo de la seguridad informática no es posible alcanzar un 100% de protección. Por ello, es conveniente contar con estas cinco buenas prácticas en cuanto a seguridad en la Nube:

Conocer la propia responsabilidad

La **seguridad en el Cloud** se basa en un modelo de **responsabilidad compartida**. No es lógico trasladar toda la responsabilidad al proveedor en la Nube, ni tampoco transferirla al cliente final.

Las diferentes **responsabilidades** se pueden entender con facilidad: el **proveedor** debe hacerse responsable de la seguridad de los elementos físicos que ofrece, de la infraestructura de seguridad, de mantener el software actualizado y libre de incidencias; el **cliente** es responsable de enviar datos seguros (cifrados), de que sus propias aplicaciones están actualizadas y al día en cuanto a protección contra amenazas, y también es responsable acerca de quién accede a los servicios contratados y con qué fin.

Es decir, como usuarios debemos preocuparnos por gestionar lo que subimos a la Nube, y que sea seguro.

Cumplir con las normativas con todo rigor

Las normativas sobre protección de datos son fundamentales para garantizar la seguridad en la próxima generación de servicios en el Cloud. Hoy, también lo son. Sin ellas, los usuarios finales no estarían tan protegidos porque no existirían normas para la salvaguarda de su privacidad. Por eso, cuando una empresa migra parte de sus activos a la Nube, debe observar con detenimiento esas normativas y aplicar las políticas de seguridad más adecuadas para garantizar que sus actividades no infringen aquélla. Una estrategia interesante es ponerse en la piel de un auditor y llevar a cabo un escrutinio exhaustivo de todos los aspectos relacionados con la seguridad, para estar preparados.

Automatización de las defensas

Disponer de las herramientas adecuadas para automatizar procesos relacionados con la seguridad nos ahorrará muchos quebraderos de cabeza. Automatizar no significa despreocuparse, sino disponer de más tiempo y recursos para supervisar que todo esté en orden.

La gestión de configuraciones, las actualizaciones software, las auditorías de seguridad internas… la automatización de todo ello reduce el error humano y favorece la escala. Si, además, el software tiene ya los últimos parches de seguridad, podemos decir que estamos preparados ante muchas amenazas.

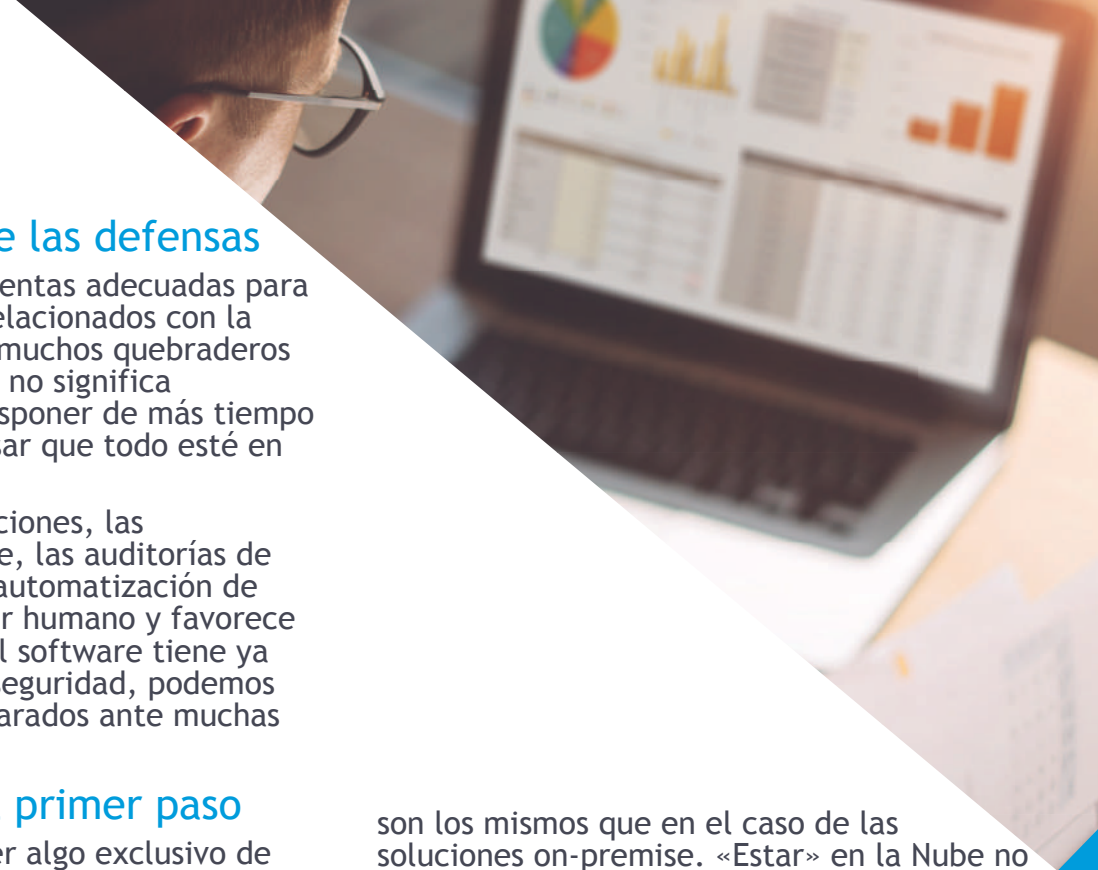
La seguridad es el primer paso

La seguridad no debe ser algo exclusivo de las últimas fases del desarrollo de un producto o de la cadena de valor. Las primeras fases de cualquier desarrollo, si no disponen de la seguridad correcta, son puntos muy vulnerables ante ataques (especialmente si hablamos de ingeniería social).

El security by default es imprescindible con los nuevos enfoques en cuestiones de seguridad: se verifica la vulnerabilidad del código fuente incluso mientras se desarrolla. Ese enfoque es totalmente válido en cualquier tipo de proceso interno, sin que haya de ser exclusivamente en el desarrollo software.

Aprender de lo experimentado

La Nube es una novedad para muchas empresas, pero los principios de seguridad



son los mismos que en el caso de las soluciones on-premise. «Estar» en la Nube no significa dar la espalda a la seguridad de las redes, servidores y puntos finales en las empresas con las soluciones de protección habituales.

Es preciso seguir monitorizando el tráfico, evitando accesos no autorizados y protegiéndose contra violaciones o pérdida de datos, entre otras cosas. La seguridad del correo electrónico sigue siendo algo crítico, por ser la puerta de entrada a muchas acciones malintencionadas.

El security by default es imprescindible con los nuevos enfoques en cuestiones de seguridad: se verifica la vulnerabilidad del código fuente incluso mientras se desarrolla. Ese enfoque es totalmente válido en cualquier tipo de proceso interno, sin que haya de ser exclusivamente en el desarrollo software.

arsys

www.arsys.es

www.facebook.com/arsys.es

twitter.com/arsys

www.linkedin.com/company/arsys-internet/