



TÉCNOLOGÍAS EN LA NUBE: LA NUEVA TENDENCIA A NIVEL GLOBAL

Actualmente, todos aquellos quienes utilizamos las diferentes tecnologías a diario, estamos muy acostumbrados a escuchar el concepto de “*nube*” en relación a la informática. Definiciones como “servidores en la nube”, “acceso remoto”, “plataformas colaborativas online”, etc., están permanentemente dentro de nuestro vocabulario sin que, en muchas ocasiones, tengamos del todo claro qué significan, qué implican o qué tecnología las sostiene. Es por ello que, a lo largo del presente boletín, nos ocuparemos de explicar qué son las tecnologías en la nube, cómo funcionan, cuáles son sus ventajas y qué debemos tener en cuenta desde el punto de vista de la seguridad para que constituyan verdaderamente herramientas útiles y no futuros dolores de cabeza.

¿Qué es la nube?

Las “tecnologías en la nube” es un nuevo paradigma de la informática que consiste en la conformación de una red que interconecta múltiples servidores o redes de servidores entre sí, de forma horizontal, y permite a los usuarios acceder a sus contenidos en todo momento y desde cualquier lugar.

Sin caer en tecnicismos, podríamos decir que “la nube” hace referencia a un **nuevo paradigma en el terreno de la informática el cual consiste en la conformación de una red que interconecta múltiples servidores o redes de servidores** -en los que se almacenan diferentes tipos de datos e información- **entre sí, de forma horizontal**. En decir, gracias a la arquitectura con la que se distribuyen, el hecho de tener un punto de acceso alcanza para llegar a toda la red. Eso, en términos muy simples es una “nube” y eso mismo define perfectamente al propio Internet; la gran red dentro de la que navegamos diariamente no es otra cosa que una enorme nube. Es por ello que, hoy en día, los servicios de cloud computing se brindan a través de Internet.

Ahora bien, ¿cómo funcionan los servicios y tecnologías en la nube?

La implementación de nuevas tecnologías puede ayudarnos a aumentar nuestros niveles de seguridad. No debemos olvidar que la tecnología en sí misma no es buena ni mala, todo depende de la conciencia y el criterio que los usuarios tengan a la hora de usarla, tanto respecto de los fines como del modo.

A partir de la arquitectura que mencionábamos antes, las empresas desarrolladoras de software comenzaron a diseñar servicios que funcionaran en línea y permitieran a los usuarios, con tan sólo una conexión a Internet, acceder a aplicaciones, archivos, plataformas de trabajo, etc., y tanto almacenar como compartir, datos e información inmediatamente y en tiempo real con otras personas que utilicen la misma tecnología. Esto constituye una gran ventaja para empresas y diversas entidades, como universidades y organismos públicos, ya que pueden acceder y disponer de diferentes elementos específicos en cualquier momento y lugar.

A la vez, la utilización de servicios en la nube tiene la ventaja de evitar a los usuarios el hecho de tener que instalar y configurar gran cantidad de aplicaciones y software –con el consecuente ahorro de recursos de disco duro y memoria correspondiente– ya que los programas se ejecutan directamente desde el servidor del proveedor de la tecnología cloud que otorgue el servicio en cada caso.

Como contrapartida, una de los aspectos negativos de éstas tecnologías es el hecho de que siempre requerirán una conexión a Internet y, como sabemos, el acceso a la red puede verse dificultado por múltiples causas.

Por otra parte, otro de los problemas que acarrea la utilización de cloud computing –y que más nos interesa desde **BA-CSIRT**– tiene que ver con cuestiones de seguridad.

Concretamente, **el mayor riesgo de utilizar la nube para volcar información personal, importante y sensible, consiste en la posibilidad de que la misma llegue a manos equivocadas; es decir, que personas no autorizadas puedan acceder a ella.** Si bien existen ataques diseñados para irrumpir en los sistemas y robar información, la mayoría de las veces los incidentes de seguridad que ocurren derivamos del uso de servidores y servicios online se deben a configuraciones de privacidad incorrectas o deficientes o descuidos por parte de los usuarios, es por ello que consideramos fundamental la concientización en este punto.

En relación a si confiar o no en la nube como usuarios, Sebastián Stranieri –CEO de la empresa VU Security– comenta:

“Los riesgos, como se explica en varios de los informes de VU Labs, tienen que ver con las vulnerabilidades del software y los modelos de conexión remota, que suelen ser inseguros. Durante 2017, por ejemplo, se dieron ataques masivos utilizando cámaras de vigilancia para bebés que, gracias a una vulnerabilidad, permitían ejecutar un código malicioso que dio de baja servicios de resolución de nombres durante horas, bloqueando los accesos a sitios relevantes a escala global.”

Gracias a que cada vez son más las empresas y entidades que incorporan cloud computing en sus servicios, disponemos cada día de más dispositivos interconectados y sincronizados entre sí. Si bien ello nos permite tener acceso a nuestra información de forma mucho más ágil, también nos obliga a tomar más precauciones y recaudos para cuidar nuestra privacidad.



Según la tendencia mundial y de acuerdo con la opinión de muchos especialistas, se cree que en pocos años las tecnologías en la nube cubrirán la totalidad del mercado.

Llevar la información a la nube eleva la complejidad de cualquier tipo de ataque y, además, facilita el control de accesos y la trazabilidad de la información. Este tipo de soluciones no sólo optimiza la inversión y costos de recursos técnicos y humanos, sino que también evita ataques del tipo Phishing, Pharming y robo de identidad, entre otros.

Debido a que se pueden sumar diferentes capas de seguridad, mantener todo en la nube también ayuda a resguardar la privacidad de la información. Cada día tenemos una vida más conectada a dispositivos y somos más dependientes a éstos. Por lo tanto, debemos ser cuidadosos y conscientes sobre qué información les proporcionamos.

Hay empresas que aún no han implementado soluciones de ciberseguridad, porque a veces es percibida como un obstáculo, algo engorroso que dificultará la vida de los usuarios. Sin embargo, en cuanto aumente la concientización sobre ciberseguridad se darán cuenta que es todo lo contrario. **Es necesario que empresas y ciudadanos sean educados en esta materia y motivar el desarrollo de soluciones de ciberseguridad para la prevención de fraude y protección de la identidad simples de implementar y con baja fricción transaccional para los usuarios.** Cada vez tenemos más información personal en la nube, y por ello también aumenta la necesidad de resguardarla con mayor seguridad."

Desde **BA-CSIRT** coincidimos en que la implementación de nuevas tecnologías, en este caso de cloud computing, no solo resulta beneficiosa sino que, además, puede ayudarnos considerablemente a aumentar nuestros niveles de seguridad. Claro está, desde ya, que todo dependerá de cómo se realice dicha implementación; es decir: **la tecnología en sí misma no es buena ni mala, todo depende de la conciencia y el criterio que los usuarios tengan a la hora de usarla, tanto respecto de los fines como del modo.** En tal sentido, recomendamos enfáticamente, revisar cuidadosamente las configuraciones de privacidad de todas las cuentas y servidores que se utilicen online y ser precavidos acerca de qué información se comparte y/o envía por Internet ya que, como siempre decimos, todo contenido que se sube a la red nunca podrá ser eliminado definitivamente. ■

