SEGURIDAD EN LA NUBE DURANTE LOS PRÓXIMOS AÑOS

Mario Alejandro Vasquez Martínez
Germán Lugo Martínez

nube

numero-29

INTRODUCCIÓN

Con el aumento del uso de las TIC, también crece el número de las amenazas en este ámbito, por lo cual la seguridad informática ha ganado relevancia. En ese sentido, uno de los principales nichos de la computación en los cuales hay que centrar la atención por su constante crecimiento y uso cada vez más generalizado es **la nube**.

Es interesante ver la tendencia que se está marcando, pues cada vez más empresas, escuelas y usuarios finales hacen uso de los servicios que esta permite, directa o indirectamente, aprovechando sus diferentes ventajas. Sin embargo, no siempre se considera que ponen en manos de terceros los datos, las aplicaciones e incluso la infraestructura (SaaS, PaaS, IaaS) que utilizan día con día.

La nube ha ganado gran popularidad gracias al empuje de las nuevas tecnologías, servicios y necesidades de los usuarios, pero aún falta atender aspectos que están en vías de desarrollo, por lo que se vuelve un objetivo muy atractivo para la delincuencia cibernética.

Tomando en cuenta que la nube aún tiene carencias, se deben considerar algunos puntos clave para infundir confianza en las personas, de modo que utilicen esta tecnología. En este sentido se deben cuidar aspectos de seguridad necesarios para afianzar las TIC a la vida cotidiana, con la finalidad de seguir cumpliendo con las expectativas de uso y mantener a salvo la información.

SISTEMAS DE AUTENTICACIÓN

Los sistemas de autenticación siguen siendo el talón de Aquiles en la seguridad informática. El objetivo de los ciberdelincuentes es vulnerarlos y obtener credenciales de administradores o usuarios con privilegios para poder llevar a cabo acciones maliciosas. En la actualidad, la mayor parte de estos sistemas se basan únicamente en usuario y contraseña, por lo que los atacantes seguirán realizando más ataques de *phishing* selectivo, ataques de fuerza bruta, robo de bases de datos y otras técnicas que se aprovechan del comportamiento del usuario promedio, por ejemplo, del hecho de que a menudo se repiten contraseñas para diferentes servicios.

Actualmente existe una amplia variedad de proveedores y aplicaciones disponibles para los usuarios o empresas que buscan hacer uso de la nube. Sin embargo, no hay una estandarización, ni normas o protocolos generales que se apliquen a este servicio, en especial al primer paso que es la autenticación, para la cual se garantice un nivel de seguridad más alto. Esta desventaja seguirá siendo aprovechada por los atacantes combinando la poca seguridad de las contraseñas y vulnerando algunos sistemas de autenticación para realizar robo de credenciales y cuentas, así como ataques directos a bases de datos de terceros.

Es importante considerar que, en este punto, los usuarios finales suelen ser el eslabón más débil en la cadena de la seguridad, por lo que la Ingeniería Social es y continuará siendo de las técnicas más usadas para obtener información que permita acceder a los sistemas.

Debido a esto, se necesitará que los profesionales de TI combinen características más robustas, entre los que se pueden encontrar los sistemas de autenticación en dos pasos y, en algunos casos, contraseñas de tipo biométrico (ya incluida en algunos dispositivos) para garantizar que las personas que accedan a los sistemas sean las autorizadas, así como también campañas de concientización de los usuarios, cuyas actividades en la red pueden afectar a la organización a la que pertenecen.

AMENAZAS

Los ciberdelincuentes cada día hacen uso de diferentes técnicas y herramientas que les permiten vulnerar y atacar a un sistema. En el caso de la nube ya no solo se realizarán ataques de tipo vertical, donde lo que se pretende es el robo de credenciales para escalar los permisos; ahora también se llevarán a cabo ataques de tipo horizontal en los que al comprometer algún servicio o aplicación se busca obtener acceso a otros que estén relacionados. Por ello se dice que el atacante se mueve lateralmente a través de cuentas de privilegios similares al afectado, buscando comprometer otro sistema. A partir de esto, los atacantes buscarán realizar acciones adicionales que pueden incluir el secuestro de información, el robo de identidad o la denegación de servicios, este último magnificado con la baja seguridad del Internet de las cosas (IoT).

Si bien a través de los años la mayoría de los atacantes se han enfocado en obtener reconocimiento personal por sus logros, en la actualidad esto ha cambiado, ya que ahora organizaciones e incluso gobiernos utilizan sus conocimientos para analizar, poner a prueba o atacar algún servicio o sistema, tanto para mejorarlos como para obtener algún beneficio a favor.

También ha crecido la implementación de programas de recompensas patrocinadas por empresas, conocidos como *bug bounty* en los que se reportan hallazgos de vulnerabilidades a cambio de una remuneración económica. Estas tendencias continuarán en los próximos años debido a que el manejo de información en la nube irá en aumento.

Se debe considerar que con la inclusión de herramientas automatizadas, las cuales se pueden encontrar en cualquier parte de la red, una persona sin conocimientos especializados puede ser un atacante en potencia, por lo que el éxito de sus ataques dependerá de los métodos de defensa con los que se cuente, la actualización constante y la buena implementación, descartando el entorno en donde se encuentren.

Hay que tomar en cuenta que conforme se sigan desarrollando nuevas tecnologías, serán más potentes los tipos de ataques, y por consiguiente, las organizaciones necesitarán robustecer su seguridad (con *firewalls*, IPS/IDS, antivirus, *antimalware*, etcétera) y pensar en implementar un departamento especializado en la seguridad de la información.

LEGISLACIÓN DE LA NUBE

Por último, un factor muy importante y que abre la puerta a muchos de los delitos que cometen los atacantes en la nube, es la falta de una legislación que se ajuste al ritmo de cambio en la tecnología, por lo que jurídicamente se tienen vacíos legales que no consideran casos específicos.

El que cada país tenga una reglamentación legal diferente o, en algunos casos, que ni siquiera exista, permite que los delincuentes encuentren una ventana idónea para realizar ataques a la nube sin consecuencias jurídicas.

La entrada y salida de datos entre diferentes países llevará a que las empresas proveedoras de este servicio tengan que ajustarse a las reglas legales de cada país en donde operan, por lo que tendrán que emplear políticas de identificación, clasificación y controles diferenciados de sus procesos y datos para cada caso. Esto sin duda se volverá un reto más para las empresas proveedoras.

En los casos de vulneración de servicios en la nube, cada vez tendremos más ejemplos y casos de litigio entre usuarios y proveedores, por lo que se debería poner especial atención en la legislación existente o en la falta de la misma.

Sin duda alguna, en este aspecto de la nube y en especial en el derecho informático habrá mucho qué trabajar. Por lo pronto se prevé que los consumidores en esta área empiecen por exigir ciertas condiciones como certificaciones para las empresas, controles normativos, servicios básicos, etcétera, con lo que las empresas definirán en qué mercado les conviene estar presentes, lo cual podría ser un obstáculo en el uso de los servicios de la nube para algunos sectores.

México cuenta con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), donde su reglamento en el artículo 52 dedicado al denominado cómputo en la nube describe algunas cláusulas que el proveedor debe cumplir, por ejemplo, garantizar la confidencialidad sobre los datos personales que resulten por el servicio. Además de proveer mecanismos como:

- Contar con la seguridad adecuada que mantenga la protección de los datos personales.

- Asegurar que los datos personales no podrán ser consultados por terceros o que no cuenten con los privilegios necesarios.

Asimismo, en el capítulo X del mismo reglamento, se describe el procedimiento de imposición de sanciones.

También existe una legislación para el caso del sector gubernamental, la denominada Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG) y recientemente la aprobación de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) lo cual es un avance más en la materia.

La legislación anteriormente mencionada podría generar confusiones que las empresas proveedoras de servicios en la nube tendrán que analizar para establecer sus reglas de operación.

CONCLUSIÓN

La nube tiene todo un futuro por delante y es un hecho que está marcando la pauta sobre cómo las empresas y los usuarios operarán en las siguientes décadas. Las problemáticas de la nube tendrán que resolverse en el camino. Para el caso de los sistemas de autenticación, se implementarán cada vez más sistemas que involucren mayor complejidad para asegurar que el usuario que accede sea quien dice ser, pero no bastará con la autenticación, sino que se empezarán a realizar estudios de comportamiento y aprendizaje automático que puedan predecir una suplantación.

En cuanto a los atacantes, estarán a la orden del día las amenazas, concentrándose principalmente en el robo de credenciales y denegaciones de servicio para poder perpetrar ataques de tipo vertical y

horizontal, y afectar a los proveedores tanto económicamente como en la confianza que tienen sus usuarios hacia ellos.

Los proveedores de servicios en la nube deberán enfocarse en mejorar sus políticas de privacidad, sus sistemas de autenticación y sobre todo gestionar sus bases legales de operación y jurisdicción en diferentes países para operar en un marco legal.

Debemos tener en cuenta el estado actual y el ritmo al que avanza la nube para saber a qué podríamos enfrentarnos, ya sea como empresas o como usuarios que buscan hacer usos de las aplicaciones o servicios que nos ofrece esta tecnología, y de esta forma minimizar riesgos.

Por último, los gobiernos tienen una responsabilidad muy importante para concientizar a las empresas y las personas sobre los riesgos y/o amenazas que existen en la red y de los cuales podrían ser víctimas. Cada vez deberán invertir más en campañas de prevención y de buenas prácticas para tratar de mitigar posibles daños.

Asimismo, será conveniente formar alianzas con otros gobiernos, por ejemplo el Convenio de Budapest al que México ha buscado adherirse y cuyo objetivo es alinear entre países las sanciones a los delitos informáticos que se cometen. Los gobiernos deberán encontrar los instrumentos que les permitan unir esfuerzos contra la delincuencia cibernética.

REFERENCIAS

Art. 47, Ley Federal de Transparencia y Acceso a la Información Pública y Gubernamental. Diario Oficial de la Federación, Distrito Federal, México, 11 de junio de 2002. Recuperado el 13 de Abril de http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFTAIPG.pdf

Art. 52, Capítulo II, Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Diario Oficial de la Federación, Distrito Federal, México, 5 de julio de 2010. Recuperado el 14 de Abril de http://dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011

Ley General de Protección de Datos Personales En Posesión de Sujetos Obligados. Diario Oficial de la Federación, Distrito Federal, México, 26 de enero de 2017. Recuperado el 20 de Mayo de http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Beek, C., Bulygin, Y., Frosst, D., Greve, P., Jarvis, J., et all. (2016). McAfee Labs 2017 Threats Predictions. California, Estados Unidos: Intel Corporation. Recuperado el 12 de marzo de 2017 de https://www.mcafee.com/au/resources/reports/rp-threats-predictions-2017.pdf

Casasola, M., Maqueo, M., Molina, M., Moreno, J., & Recio, M. (2014). La nube: nuevos paradigmas de privacidad y seguridad para un entorno innovador y competitivo. México, Distrito Federal: Centro de Investigación y Docencia Económicas A.C. Recuperado el 9 de marzo de 2017 de https://cidecyd.files.wordpress.com/2014/05/la-nube-nuevos-paradigmas-de-privacidad-y-seguridad-para-un-entorno-innovador-y-competitivo.pdf

Cisneros, F. (2016). La nube es una tendencia irreversible que permite hacer más con menos en esta época de reducción de presupuestos. Es muy fácil de implementar y es flexible. Ciudad de México, México: Instituto de Ingeniería, UNAM. Recuperado el 9 de marzo de 2017 de http://www.iingen.unam.mx/es-mx/BancoDeInformacion/MemoriasdeEventos/Documentos2016/Microsoft2016.pdf

Tableau Software (2016). Las 10 tendencias principales de la nube para 2017. United States: Tableau Software. Recuperado el 10 de marzo de 2017 de https://www.tableau.com/sites/default/files/whitepapers/whitepaper_top_10_cloud_trends_2017_es-es.pdf

SI QUIERES SABER MÁS, CONSULTA:

- Perspectivas: todo depende del cristal con que se mire la nube
- Internet de las cosas (IoT)
- Password-fu: Guía fácil para contraseñas realmente seguras
- Ingeniería Social
- Bug bounty
