Fuente: Marko Hölbl ***LSI SIN (10)02***

Temas de Seguridad y Privacidad en Cloud Computing

CEPIS

El Consejo Europeo de Sociedades Profesionales de Informática (CEPIS) es una organización sin ánimo de lucro que busca la mejora y la promoción de altos estándares para los profesionales informáticos en reconocimiento del impacto que la Informática tiene en el trabajo, las empresas y en la sociedad. CEPIS que representa a 36 sociedades miembro de 33 países a través de la gran Europa, ha acordado la siguiente declaración:

1. Antecedentes

Cloud Computing (Computación en la nube) no es un concepto muy novedoso, de hecho Cloud Computing es una versión más avanzada de las Oficinas de Servicios de Proceso de Datos que teníamos hace 40 años. Sin embargo, las empresas más conocidas en el campo de las Tecnologías de la Información ofrecen ya u ofrecerán a corto plazo servicios de Cloud Computing a un rango de clientes desde organizaciones de todos los tamaños a individuos. Los más grandes y más conocidos proveedores de Cloud Computing incluyen a Amazon con EC2 [5], Microsoft con Azure [6] y Google con Google Apps (p.ej. Gmail, Google Docs, Google Calendar) [7]. El paradigma de Cloud Computing puede describirse en palabras sencillas como oferta de servicios específicos de TI que son hospedados en Internet, siendo los más comunes, Plataforma como Servicio (PaaS), Infraestructura como Servicio (IaaS) y Software como servicio (SaaS). Frecuentemente se comercializa Cloud Computing como una solución eficiente y barata que reemplazará el paradigma del cliente-servidor. El cambio de paradigma incluye/resulta en la perdida de control de los datos, así como también en nuevos temas de seguridad y privacidad. Por esta razón, se aconseja precaución al desplegar y usar Cloud Computing en las empresas. Después de todo, el primer gran tema de protección de datos en Europa apareció a finales de los años 60 del siglo pasado cuando una compañía sueca decidió realizar su proceso de datos en una oficina de servicios en Alemania y la legislación de protección de datos era diferente en ambos países.

Con Cloud Computing ganando popularidad rápidamente, es importante resaltar estos riesgos resultantes. Dado que los temas de seguridad y privacidad son de máxima importancia, se deben tratar antes de que Cloud Computing logre una parte importante del mercado. Muchos centros informáticos e importantes agencias de investigación son conscientes de estos riesgos y han realizado informes y análisis para documentarlos [1}, [2], [3] y [4].

2. Preocupaciones

Parece que no existe área de TIC que no sea afectada por Cloud Computing. Dos temas principales existen en los aspectos de seguridad y privacidad de Cloud Computing:

1. pérdida de control de los datos y
2. dependencia de los proveedores de Cloud Computing.

Estos dos temas pueden llevar a numerosas preocupaciones legales y de seguridad relacionadas con la infraestructura, la gestión de la identidad, control de accesos, gestión de riesgos, cumplimiento de reglamentaciones y legislación, auditoria y registro

de datos, control de integridad, así como riesgos dependientes del proveedor de Cloud Computing.

Asuntos típicos debidos a la perdida de control sobre los datos son:

1. La mayoría de los clientes son conscientes del peligro de dejar el control de los datos fuera de sus propias manos y almacenar datos en un proveedor exterior de Cloud Computing. Se pueden comprometer los datos por el propio proveedor de Cloud Computing o por otras empresas competidoras que son clientes del mismo proveedor de Cloud Computing. Existe una falta de transparencia para los clientes sobre como, cuando, porqué y donde sus datos son procesados. Esto está en oposición al requisito de protección de datos de que los clientes conozcan lo que ocurre con sus datos.
2. Muchos proveedores de Cloud Computing están capacitados para utilizar técnicas de minería de datos para analizar los datos de los usuarios. Esto es una función muy sensible e incluso más todavía ya que los usuarios almacenan y procesan datos sensible cuando utilizan los servicios de Computación en la nube. Esto es especialmente cierto para las aplicaciones de medios sociales que animan a los usuarios a compartir mucho de su vida privada , como p.ej. fotos privadas[1].
3. Los dispositivos móviles, en particular con su limitada capacidad de almacenamiento son incentivos para disponer de servicios facilitados por Cloud Computing en lugar de utilizar software en ordenadores individuales. Incluso los datos que deben ser transferidos de un dispositivo móvil a otro (local) dispositivo se transfieren, con frecuencia a través de la nube cuando aplicaciones orientadas a la nube están involucradas en el dispositivo móvil. En consecuencia los usuarios se ponen en riesgo sin ser conscientes de ello al asumir que los datos se transfieren localmente.
4. Dado que Cloud Computing es un servicio, debe ser accedido remotamente. La conexión entre el proveedor de Cloud Computing y el cliente no siempre está protegida adecuadamente, los riesgos de seguridad que amenazan la línea de transmisión incluyen escuchas, desviación de DNS y ataques de denegación de servicio.
5. El cambio de paradigma en Cloud Computing hace que el uso tradicional de la gestión de riesgos sea difícil o incluso imposible, independiente de del hecho que el control sobre los datos sea transferido al proveedor de Cloud Computing, gestión de riesgos y temas de cumplimiento están divididos entre el proveedor de Cloud Computing, el proveedor de Internet y el cliente. Sin embargo, el cumplimiento puede verse como uno de los factores importantes de confianza entre el proveedor de Cloud Computing y el cliente. El cumplimiento de reglamentos y de la legislación es también problemático. Los centros de datos de la Nube pueden estar geográficamente dispersos. En consecuencia, el cumplimiento de la legislación no está, en la actualidad, adecuadamente definida.
6. Como todo el control técnico se otorga al proveedor de Cloud Computing, el cliente quiere disponer de una auditoria externa de este proveedor. En consecuencia, información de registro de datos y de auditoría debe ser almacenada y protegida para posibilitar su verificación. El registro de datos

[1] Más información en ediciones especiales de aplicaciones de medios sociales puede ser encontradas en la declaración de CEPIS sobre redes sociales—Problemas de seguridad y privacidad de datos [8}

apropiado podría facilitar la posibilidad de investigación forense en caso de incidentes.

7. Existe también preocupación en relación con el borrado de datos: resulta difícil borrar todas las copias de material electrónico porque es difícil localizar todas las copias. Es imposible garantizar la total cancelación de todas las copias de los datos. En consecuencia, es difícil hacer cumplir la obligatoriedad de cancelación de datos. Sin embargo, la cancelación obligatoria de datos debería ser incluida en toda venidera reglamentación de servicios de Cloud Computing, pero aún así no se debería tener mucha confianza en ello: la edad de una "Cancelación de datos totalmente garantizada", si alguna vez ha existido, ya ha pasado. Esto tiene que ser considerado cuando se reúnen datos y se almacenan.
8. La legislación de protección de datos y de privacidad, ni siquiera es similar en muchos países del globo, pero Cloud Computing es un servicio global de cara al futuro. Consecuentemente, los problemas y los riesgos que afectan a las reglas de protección de datos en Europa deben ser consideradas de manera apropiada cuando las plataformas de Cloud Computing están localizadas en servidores en países no europeos.
9. Cloud Computing se basa en telecomunicaciones fiables y seguras entre redes que aseguran y garantizan las operaciones de los usuarios terminales de los servicios facilitados en la nube por el proveedor de Cloud Computing. Las redes de telecomunicación son, con frecuencia, suministradas separadamente de los servicios de Cloud Computing.

Temas típicos referentes a la dependencia en el proveedor de Cloud Computing son:

1. Una preocupación mayor se refiere a la dependencia de un proveedor específico de Cloud Computing en cuanto a disponibilidad. Si el proveedor de Cloud Computing fuera ala bancarrota y detuviese la provisión de servicios, el cliente podría experimentar problemas en el acceso a datos y, en consecuencia, potencialmente en la continuidad del negocio.
2. Algunos de los servicios más utilizados de Cloud Computing (p.ej. GoogleDocs) no incluyen algún contrato entre el cliente y el proveedor de Cloud Computing. En consecuencia, un cliente no tiene a que referirse si ocurren incidentes o aparece algún problema.
3. Cloud Computing es un servicio similar a otros servicios más tradicionales (p.ej. telecomunicaciones, transacciones bancarias, electricidad, gas, agua, etc.). Ambos, los servicios de Cloud Computing y los servicios tradicionales tienden a ser ofrecidos por grandes suministradores tratando con clientes más pequeños. En consecuencia, los clientes, generalmente dependen de los proveedores porque es difícil cambiar de proveedores si es que resulta posible en absoluto. Consecuentemente los servicios tradicionales (p.ej. telecomunicaciones, transacciones bancarias, electricidad, gas, agua, etc.) están generalmente regulados en cuanto al rango de funcionalidad (p.ej. funciones obligatorias, cobertura), precios, responsabilidad del suministrador y fiabilidad.

Cloud Computing corrobora una tendencia de que la seguridad en TIC no es ya una cuestión puramente técnica, sino una cuestión entre individuos y organizaciones y así incluye aspectos humanos y organizacionales como la gestión, contratación y cumplimiento legal.

3. Recomendaciones

Se deben considerar, en particular, los siguientes puntos.

1. Los temas de gestión de riesgos y de cumplimiento (legal) deben de estar bien definidos en el contrato entre el proveedor de Cloud Computing y el cliente y debe facilitar la transparencia en relación con el procesamiento y almacenamiento de datos, p.ej. la localización física del almacenamiento de los datos. De esta manera, la confianza entre el proveedor de Cloud Computing y el cliente puede ser reforzado.
2. El servicio facilitado debe de cumplir la regulación y la legislación que el cliente tiene que seguir y también los clientes deben de ser capaces de cumplir con la correspondiente regulación y legislación.
3. Los problemas y riesgos que afectan a las reglas de protección de datos en Europa deben de ser considerados adecuadamente cuando las plataformas de Cloud Computing están localizadas en servidores en países no europeos.
4. La línea de comunicación entre el proveedor de Cloud Computing y el cliente debe estar adecuadamente protegida para asegurar la confidencialidad, integridad, control de autenticidad y para minimizar el riesgo de ataques de denegación de servicio. Una abierta y cuidada especificación de las mediciones realizadas para asegurar la seguridad de la línea de comunicación debería ser obligatoria para cualquier proveedor de Cloud Computing y debería basarse en estándares y tecnologías abiertas y transparentes.
5. Los proveedores de Cloud Computing deberían ser obligados a asegurar la confidencialidad de los datos.
6. La obligatoriedad de la cancelación de datos debería de ser incluida en la potencial reglamentación de los servicios de Cloud Computing, pero no se debería confiar mucho en ello.
7. El hecho de que no haya garantía de la total cancelación de datos requiere ser considerado cuando se reuniesen y almacenan los datos.
8. Con el fin de garantizar la disponibilidad de los datos, copias de respaldo locales por el cliente, de datos esenciales deben ser consideradas.
9. Se debe fomentar la mejor promoción de software y el desarollo de software que permite la transferencia local de datos entre dispositivos.
10. Las redes de telecomunicaciones que soportan los servicios de Cloud Computing deberían estar securizadas y protegidas contra ataques de DOS y de Malware.
11. Se debería facilitar el registro de datos y auditoria adecuados. Una auditoria externa puede ser beneficiosa para la reputación del proveedor de Cloud Computing y también para reforzar la confianza del cliente.
12. Se debería educar a los no profesionales (p.ej. el usuario genérico) en relación con el nuevo paradigma. La educación debería prepararlos para tomar decisiones competentes cuando usen servicios de Cloud Computing, incluyendo que información debería ser transferida a la nube y bajo cuales circunstancias.
13. Los profesionales deberían ser capaces de gestionar los nuevos tipos de riesgos.
14. Dado que alguna regulación será necesaria en el futuro, p.ej. para equilibrar el poder entre proveedores y clientes de servicios de Cloud Computing, seria inteligente considerar sus debilidades y problemas antes de que Cloud Computing se convierta en un servicio o infraestructura críticos. Es necesario verificar cual de las dimensiones de conflicto y potencial regulatorio

será relevante (p.ej. la garantía y responsabilidad sobre la confidencialidad y la integridad de los datos procesados), en particular cuando un proveedor de Cloud Computing se convierte en parte de una infraestructura de información críticos, alguna reglamentación o limitación en relación con la posibilidad de su adquisición por un tercero, puede resultar apropiada.

15. Se debería fomentar la investigación sobre los conceptos básicos y problemas en informática, seguridad y privacidad en relación con los servicios de Cloud Computing. También asuntos referidos al posible impacto de plataformas de Cloud Computing de la validez de la certificación de aplicaciones que son certificadas de acuerdo a criterios (p.ej. Criterios Comunes--Common Criteria—sello europeo de privacidad, etc.) pueden tener que ser investigados.

Referencias

[1] J. Brodkin, Gartner: Seven cloud-computing security risks, available at: www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853.

[2] Cloud Computing Security Considerations, A Microsoft Perspective, Microsoft Whitepaper, 2010, available at: http://www.microsoft.com/malaysia/ea/whitepapers.aspx.

[3] Cloud Computing: Benefits, Risks and Recommendations for Information Security, ENISA Report, 2009, available at: www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.

[4] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, Cloud Security Alliance (CSA) Report, 2009, available at: www.cloudsecurityalliance.org/csaguide.pdf.

[5] Amazon Elastic Compute Cloud (Amazon EC2), http://aws.amazon.com/ec2/.

[6] Windows Azure platform, www.microsoft.com/windowsazure/.

[7] Google Apps, www.google.com/apps/

[8] CEPIS Statement, Social Networks – Problems of Security and Data Privacy, 2008, www.cepis.org/index.jsp?p=942&n=963#Social%20Networks