Study on the Security of Cloud Computing

February 26 2010

Not only does cloud computing help to save money, it also helps to increase IT security: Small and medium sized companies especially can profit from special cloud security solutions and the knowledge advantage of experienced providers. Large companies, however, should check thoroughly whether the terms of contract offer adequate security guarantees for the respective case, because failures and disruptions are not uncommon in cloud computing. These findings were the result from a study exploring the security risks of cloud computing carried out by the Fraunhofer Institute for Secure Information Technology (Germany).

The study provides an overview of prices and functions offered by the most important cloud providers and detailed risk assessments for various use cases.

The number of companies using cloud computing continues to increase and they are shifting their data, applications and business processes to server farms from providers such as Amazon, Google, IBM or Microsoft. Benefit: The companies do not have to purchase servers and software solutions themselves, but lease the necessary capacities for data, processing power and applications from professional providers. This saves money and effort and, furthermore, provides for high flexibility, because the activity of the leased service can be adjusted according to the customers needs.

But what happens in the case of a service failure? Who guarantees that the company secrets are secure on the external servers? Which security risks evolve when a cloud service subcontractor accesses the cloud

systems? Is the data destroyed after deletion? These and similar questions should be resolved before a company decides if and what cloud service to use. The strategy of outsourcing into the cloud on the one hand allows the companies to concentrate on their core competencies and to develop new business opportunities. But on the other hand the dependency on external IT systems is increasing, and a failure of these systems due to technical failures, malware or hacker attacks may not only cripple communication but can disrupt even whole business or production processes.

"Almost every large cloud service provider had an incident in the past in the areas of availability or security“, reports Dr. Werner Streitberger, one of the study's authors. "The current offerings in cloud services show that especially in the area of infrastructure a number of security technologies have been applied already. The cloud providers have not yet advanced the support of security technologies as much in the areas of architecture, management and compliance.“

The SIT study showed that small and medium sized companies would be able to increase their security by using cloud services despite certain risks. "They can obtain security solutions as a service from a specialised provider and thus benefit from the provider's experience in the implementation and running of secure services“, explains Streitberger.

Large companies, however, should review a cloud provider's security functions individually and decide also on an individual basis, whether the supplied security mechanisms are sufficient for the specific requirement of the company. "The current cloud service offerings show that a number of security technologies are already in use at infrastructure level, but in the areas of application and platform, management and compliance, the cloud providers have not yet fully achieved the required protection targets“, Streitberger criticizes. The responsibility for the data usually remains with the cloud user, so he needs to define exact

requirements how and which data may be stored and processed in a cloud service, and what security functions have to be in place.

The Service Level Agreement (SLA), i. e. the agreement about the rights and duties between the cloud user and the cloud provider, represent another weak point. The current customary agreements only provide minimal warranty for the quality of service for the cloud. Security guarantees exist rudimentarily and the functions necessary for the guarantees are insufficiently documented by the cloud provider. "Quite often security plays a secondary role in the offered service. We therefore recommend requesting detailed information about the cloud service from the various providers. A proof of concept may be a valuable option before using a cloud service in a production environment“, says Streitberger.

More information: The study can be ordered via the Internet at www.sit.fraunhofer.de/cloud-security

Provided by Fraunhofer-Gesellschaft