WHITE PAPER

Hybrid Cloud Computing + Cybersecurity

December 15

2012

This white paper is presented by SDV INTERNATIONAL to help readers understand the important considerations that organizations must make before choosing a cloud solution, particularly when sensitive data is being stored.

.:. SDV INTERNATIONAL, LLC .:.
.:. Phone: (202) 455-6554 .:.
.:. Email: info@SDVInternational.com .:.
.:. Website: www.SDVInternational.com .:.

The Hybrid Cloud Solution for Sensitive Data

Challenges with Hybrid Cloud Solutions, System Security and Reliability

Some companies consider the utilization of hybrid computing clouds because they combine on-premises capacity with the capacity of external high-availability pooled resource computing clouds in a manner that reduces cost and increases speed [3]. For example, a company implementing a hybrid cloud solution for the processing and storage of sensitive personnel records might combine in-house servers in a Human Resources Department with the cloud environment of a third-party vendor. Organizations have the opportunity to utilize security controls over on-premise equipment, while little control may be exercised in cloud environments. The challenge for an organization that attempts to utilize a hybrid cloud environment lies in balancing the benefits of the cloud, while mitigating the risks of using 3rd party cloud service providers (CSP).

Some applications, such as hosted email (i.e. Google Apps), are straightforward and just as secure as Microsoft Exchange hosted with on-premise servers [4]. Other applications, with limited application programming interface (API) and protocol standardization make on-premise and cloud storage integration difficult, and potentially less secure [4]. The challenges that companies will face before deciding to implement a hybrid solution will include a thorough evaluation of the systems that the organization wishes to integrate with the cloud, making sure that the protocols being used are secure, and that the 3rd party cloud architecture is otherwise secure.

In addition, if such company personnel are involved in classified U.S. government projects, it is important that vendors consider where the cloud data is hosted, whether in the U.S. or aboard, and who the cloud vendor employs to maintain the information systems.

Who is Accountable & Responsible?

Ultimately, the responsibility to maintain security primarily rests on the company, but should also include accountability by the cloud service providers. Moreover, the company that owns the sensitive data will ultimately be responsible if a security breach occurs. Many states require that companies report security breaches to customers and employees [2]. When companies announce such breaches, stakeholders face heightened concern, and an organization's reputation may suffer; potentially resulting in losses.

While the employer will be responsible for security breaches, it may seek to work with 3rd party cloud vendors that have a secure infrastructure, which may be determined through extensive research, interviews and evaluations, industrial and governmental certifications, and by independent review from trusted organizations.

Questions to Ask Cloud Service Providers (CSP)

Organizations can take specific steps to evaluate CSPs. Initially, the company must make its requirements clear to the CSP. Requirement areas typically include: personnel requirements, including clearances, roles, and responsibilities; availability limits; customer support; non-disclosure agreements; logical and physical access controls; system configuration and patch management; data backup and recovery procedures; and certification and accreditation (C&A) needs [1]. In addition, the company may assess the competency of the CSP, which might include an evaluation of the CSP's past performance and technical approach. With regard to past performance, an evaluator might glean insight into the CSP competency by comparing the size, scope and magnitude of previous projects. With regard to technical approach, the company may evaluate the CSP's personnel qualifications, frequency of security training, adoption rate for new technologies, use of secure protocols (i.e. HTTPS, PGP, Public Key Infrastructure technologies), encryption practices for data at rest (i.e. CypherCloud for Google Apps), and change management procedures [1].

Security Provisions Needed for the Cloud Architecture to Ensure Secure Computing

For organizations that place a high priority on securing sensitive data, they might require that their CSP engages in an ongoing C&A program that follows a commonly accepted approach, such as NIACAP, FISMA, DIACAP.

Sources:

1) Jansen, W. & Grance, T. (2012) NIST Pub. 800-144: Guidelines on Security and Privacy in Public Cloud Computing. National Institute of Standards and Technology (NIST). Retrieved from www.nist.gov

2) Marne, G. (2006). Reporting Breaches: When should companies go public following a security breach? Computer Fraud & Security, 200616-18. doi:10.1016/S1361-3723(06)70421-3

3) Mazhelis, O., & Tyrvainen, P. (2012). Economic aspects of hybrid cloud infrastructure: User organization perspective. Information Systems Frontiers, Volume 14(4), P. 845-869.

4) Stevens, A. (2011) When hybrid clouds are a mixed blessing. The Register White Papers. Retrieved from www.therigister.co.uk