International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 3, Number 9 (2013), pp. 933-938

http://www. irphouse.com /ijict.htm

Ensuring Cloud Security Using Cloud Control Matrix

Swati Saxena

CSE Dept., Ansal Technical Campus, Lucknow.

Abstract

Cloud computing is the most evolutionary technology prevalent today, which is widely accepted by organizations due to cost-affordability, efficiency and flexibility. It enables the virtual organization to share geographically distributed resources as they pursue common goals, assuming the absence of central location, omniscience and an existing trust relationship. It shifts the responsibility of managing a complex IT infrastructure by offering a simple, cost-effective and efficient way to run a business. From a security perspective, a number of unchartered risks and challenges have been introduced from relocation to the clouds, deteriorating much of the effectiveness of traditional protection mechanisms. This paper presents an overview of Cloud Control Matrix (CCM), created by Cloud Security Alliance (CSA). CCM acts as a baseline set of security controls to help enterprises assess the risks associated with a cloud computing provider, thus securing the cloud transition and building a trust between the cloud customer and the cloud vendor.

Keywords: Cloud security, cloud customer, cloud provider, cloud security alliance, cloud control matrix.

1. Introduction

With cloud computing, you need not worry about IT infrastructure, because you need not own one [1]. Using cloud is an excellent way to reduce the business cost and make it more productive. Cloud computing presents IT on demand. However, before adopting the cloud, a business house needs to identify its assets and evaluate them [2]. A detailed risk analysis and preventive measures need to be discussed and agreed upon before a business migrates to a cloud. This calls for an extensive agreement between the cloud provider and the cloud user. This paper discusses cloud control matrix, CCM

v1.4, designed by the Cloud Security Alliance (CSA), aimed at establishing a better understanding and trust level between the cloud customer and the cloud provider. CCM is available for free download to help companies evaluate cloud providers and guide security efforts. Security remains a top concern for enterprises as they adopt cloud computing, and the Cloud Controls Matrix is an attempt to bridge the gap and provide a standard for security measures implemented in the cloud.

The organization of the paper is as follows-Section II introduces security threats prevalent in cloud computing. Section III introduces Cloud Control Matrix. Section IV describes the domains of CCM, followed by section V which discusses the potential benefits of CCM. This paper ends with a concluding note followed by references.

2. Security Threats

The rise in the scope of cloud computing has brought fear about the 'internet security' and the threat of security in cloud computing is continuously increasing [10]. Consumers of the cloud computing services have serious concerns about the availability of their data when required. Users have severe concerns about the security and access mechanism in cloud computing. Security issues in cloud can be broadly classified into four categories-

i) Security issues existing in cloud infrastructure, platform and hosted code
ii) Data security issues comprising of data integrity, data lock-in, data remanence, provenance, confidentiality and user privacy specific concerns
iii) Issues related to access control, authentication, authorization, encryption and user-id management
iv) Compliance issues in security audit, data location, operation traceability, etc.

3. Cloud Control Matrix- An Introduction

The Cloud Security Alliance Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. The CSA CCM provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains. The foundations of the Cloud Security Alliance Controls Matrix rest on its customized relationship to other industry-accepted security standards, regulations, and controls frameworks such as the ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum and NERC CIP and will augment or provide internal control direction for service organization control reports attestations provided by cloud providers. As a framework, the CSA CCM provides organizations with the needed structure, detail and clarity relating to information security tailored to the cloud industry. The CSA CCM strengthens existing information security control environments by emphasizing business information security control requirements, reduces and identifies consistent security threats and vulnerabilities in the cloud,

provides standardized security and operational risk management, and seeks to normalize security expectations, cloud taxonomy and terminology, and security measures implemented in the cloud [12].

4. Domains of Cloud Control Matrix

Cloud is mainly defined by the relationship and interface between the cloud customer and the provider. There are security risks and issue that need to be thoroughly discussed between the two parties before an enterprise considers engaging the services of a cloud provider. a lack of transparency in terms of the information a controller is able to provide to a data subject on how their personal data is processed is highlighted in the opinion as matter of serious concern. Data subjects must1 be informed who processes their data for what purposes and to be able to exercise the rights afforded to them in this respect [5]. A key conclusion is a comprehensive and thorough risk analysis between the business house and a cloud administration. Security, transparency and legal certainty for the clients should be key drivers behind the offer of cloud computing services [5].

In regard with this opinion, CSA has specifically designed a Cloud Control Matrix (CCM) to provide fundamental security principles to guide cloud vendors and prospective consumers in assessing the overall security risk of a cloud provider, thereby establishing a strong trust level between the two and establishing a market reputation of the provider. The CSA CCM provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains. The foundations of the Cloud Security Alliance Controls Matrix rest on its customized relationship to other industry-accepted security standards, regulations, and controls frameworks such as the ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum and NERC CIP and will augment or provide internal control direction for service organization control reports attestations provided by cloud providers [6].

The first domain of CCM deals with compliance concerns for regular audits, inspections and reviews of data, objects, application, infrastructure and hardware at regular intervals. The audit activities need to planned by the cloud provider and agreed upon with the stakeholders, in advance. It also states that statutory, regulatory and contractual requirements are defined for all elements in the information system.

Maintaining control over the data is paramount to cloud success. A decade ago, enterprise data typically resided in the organization's physical infrastructure, on its own servers in the enterprise's data center, where one could segregate sensitive data in individual physical servers. Today, with virtualization and the cloud, data may be under the organization's logical control, but physically reside in infrastructure owned and managed by another entity [7]. Data Governance domain of CCM will handle all the possible scenarios of data theft, misuse, leakage, disposal, retention and related risks. This domain establishes the foundation of a data lifecycle in a cloud. Defining ownership of data and objects containing data, classification and protection from

unauthorized access, use, loss, destruction and falsification, etc are dealt with keeping legal and jurisdiction context in mind.

Cloud computing is virtual. It happens, well, in the cloud. Because of that it's often easy to forget that somewhere data and information reside on real physical servers in brick-and-mortar locations that need to be secure [8]. The third domain of CCM Facility Security is all about the protection of the physical location of data in the cloud. The San Antonio based open cloud company Rackspace has employed most of the facility security features talked about in CCM [8].

Domain 4 of CCM deals with an employee's background screening, employment agreements and terminations to enforce technology based restriction on Cloud on what an employee can and cannot do vis-à-vis Cloud apps. For example, whether an employee can use public Cloud storage solutions like DropBox at work and more importantly, does the company allow information to be put into public Cloud storage services? Or can an employee use personal handheld devices like smartphone/tablet at/for work? For companies moving to the Cloud or those who have already made the transition, it is important to review and update HR policies to mitigate information security threats that come with this paradigm shift.

Information Security domain of CCM gives the cloud customer a chance to discuss managerial issues with the cloud vendor, like policies and their enforcement queries, roles and responsibilities of employees and clear-cut segregation of their duties, strategic planning of the management and their involvement/support, policies related to incident management and reporting. Apart from these, this domain also talks about source code access restriction, acceptable/unacceptable use of portable mobile devices and network infrastructure services.

CCM also details out the legal aspect of cloud services, like non-disclosure agreements and third-party agreements. This includes agreements involving processing, accessing, communicating, hosting or managing the organization's information assets, or adding or terminating services or products to existing information. Assets agreements provisions shall include security (e.g., encryption, access controls, and leakage prevention) and integrity controls for data exchanged to prevent improper disclosure, alteration or destruction.

In order to ensure continuity and availability of operations, a separate domain of operations management is included in CCM, which deals with establishments of policies and procedures for equipment maintenance. Future needs of resources and capacities must also be considered so as to reduce the risk of system overload.

Facilitating innovation (with increased speed) and cost-saving aspect of cloud computing can be viewed as risk-events by some cloud customers. By lowering the barriers of entry for new competitors, cloud computing could threaten or disrupt some business matrices, even rendering them obsolete in the future [11]. Example is that of streaming media over the internet which drastically reduced the sales of CDs and DVDs in the market. Organizations must develop and maintain an enterprise risk management framework to deal with such risks like reliability, transparency, performance issues, application portability or interoperability issues, etc. In this regard,

CCM has included a risk management domain to ensure that formal risk assessments are planned and scheduled at right intervals to determine the likelihood and impact of identified risks, using qualitative and quantitative methods. It also states that the identification, assessment, and prioritization of risks posed by business processes requiring third party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.

CCM also outlines the policies and procedures for management authorization for development and acquisitions of new application, systems, databases, infrastructures, services, operations and facilities. Changes to the production environment shall be documented, tested and approved prior to implementation. A program for the systematic monitoring and evaluation to ensure that standards of quality are being met shall be established for all software developed by the organization. Management shall have a clear oversight capacity in the quality testing process with the final product being certified as "fit for purpose" (the product should be suitable for the intended purpose) and "right first time" (mistakes should be eliminated) prior to release. Policies and procedures shall be established and mechanisms implemented to restrict the installation of unauthorized software.

Cloud computing security (sometimes referred to simply as "cloud security") is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. In this regard, CCM address all identified security, contractual and regulatory requirements for customer access. CCM considers security needs at every level, i.e. from data security, integrity to application security. Multi-factor authentication of remote users is discussed Along with separation of production and non-production environments to prevent unauthorized access and changes to information assets.

Location-aware technologies may be used to validate connection authentication integrity based on known equipment location. Applications shall be designed in accordance with industry accepted security standards (i.e., OWASP for web applications) and complies with applicable regulatory and business requirements. CCM also advocates the use of intrusion detection tools to facilitate timely detection, investigation by root cause analysis and response to incidents.

5. Conclusion

Cloud computing brought in the complexities that are often over-looked because of the monetary benefits [13]. The pressing needs for integrating, monitoring and managing cloud services call for a robust framework that can take care of the elementary issues regarding cloud security, at all aspects.

A detailed study and implementation of CCM facilitates transparency between the cloud customer and the cloud vendor, thereby, strengthening the trust between them and making cloud computing a secure way to the future of business.

References

[1] http://maltatoday.com.mt/en/blogsdetails/blogs/The-relevance-of-Cloud-Computing-to-the-business
[2] https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
[3] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, Security Issues for Cloud Computing, International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010 39
[4] www.savvis.com/en-us/info_center/pages/whitepapers.aspx
[5] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf
[6] https://cloudsecurityalliance.org/research/ccm/
[7] http://www.vormetric.com/sites/default/files/wp-data-security-in-the-cloud.pdf
[8] http://www.rackspace.com
[9] http://www.cloudtweaks.com/2013/05/hr-security-risk-prevention/
[10] R. La‘Quata Sumter, ―Cloud Computing: Security Risk Classification‖,ACMSE 2010, Oxford, USA
[11] http://www.coso.org/documents/Cloud%20Computing%20Thought%20Paper.pdf
[12] https://cloudsecurityalliance.org/research/ccm/
[13] https://cloudsecurityalliance.org/wp-content/uploads/2012/02/Areenterprisesreallyreadytomoveintothecloud.pdf