“Mircea cel Batran” Naval Academy Scientific Bulletin, Volume XVIII – 2015 – Issue 1
Published by “Mircea cel Batran” Naval Academy Press, Constanta, Romania // The journal is indexed in:
PROQUEST SciTech Journals, PROQUEST Engineering Journals, PROQUEST Illustrata: Technology, PROQUEST Technology Journals, PROQUEST Military Collection PROQUEST Advanced Technologies & Aerospace

SECURITY THREATS AND RISKS IN CLOUD COMPUTING

Ciprian RACUCIU[1]
Sergiu EFTIMIE[2]
[1]Prof. Eng. , Ph.D. Military Technical Academy - Electronic, Information and Communication Systems for Defense and Security Doctoral School
[2]Inf. Ph.D. Student Military Technical Academy - Electronic, Information and Communication Systems for Defense and Security Doctoral School

Abstract: *Cloud computing presents complex challenges to companies that are trying to identify and mitigate risk. This research document aims to identify the biggest concerns related to cloud adoption strategies and to provide a context in making risk management decisions.*

Keywords*: Security, Cloud, Threats, Risks, Strategy*

INTRODUCTION

Cloud computing is an evolving term that describes different and new approaches to computing along with the development of many existing technologies. From a security point of view, adopting cloud computing inside a company is a complex decision that involves multiple factors. The cloud environment creates new risks and new opportunities. There are cases where moving to thecloud provides an opportunity to re-architect older applications and infrastructure to meet existing security requirements and there are cases where the risk of moving existing applications to new infrastructures outweigh the benefits. Shifting to cloud technologies exclusively can be affordable and fast but it can undermine important enterprise-level processes, security policies and best practices. In the absence of these standards, companies are vulnerable to security breaches.Cloud Computing isn’t necessarily less secure than current environments.Being a rapidly evolving field means that the security professionals have to continue to evolve the processes and to find new ways to improve the efficiency of the security enforcement and monitoring capabilities.

A security threat is a possible case in which a vulnerability can be exploited by an agent in order to breach security and thus cause possible harm or loss.

A security risk represents an event caused by deliberate acts that could result in the compromise of a company’s assets [1].

A study has shown [2]that the tendency to bypass information technology (IT) departments and information officers is among the most significant security risks associated with cloud computing.

DATA BREACHES AND DATA LOSS

A securityincident represents an event that compromises the integrity, confidentiality or availability of an information asset.

A data breach represents a security incident that results in the disclosure or exposure of proprietary data to an untrusted environment. For example sensitive or confidential data is viewed, copied, transmitted or used by an agent that is unauthorized to do so.

A data disclosure represents a data breach for which it was confirmed that data was actually disclosed and not just exposed to an unauthorized party.

A data loss represents the permanent loss of a company’s data asset.

Data breaches and data loss are considered top threats to cloud computing and the measures that are put in place to mitigate them are interlinked. For example the decision to encrypt the data stored on cloud can reduce the possibility of a data breach but the corruption of the encryption key can lead to data loss. Conversely keeping offline backups of cloud data can reduce the risk of data loss but increase the risk of data exposure.

The nature of cloud computing makes it difficult to respond to a security incident that needs to be investigated. Applications deployed to cloud infrastructures are not always designed with security in mind and this leads to security incidents. Additionally, vulnerabilities that also endanger traditional data centers like flaws in the infrastructure architecture or mistakes made during hardening procedures can add risk to cloud operations.

The proliferation of mobile devices with access to cloud and the increased dependency on cloud services withouta strengthened cloud security strategy increases the risk of a data breach in the cloud environment. The lack of visibility of end user practices and the lack of knowledge about the number of devices connected to a cloud network also increase this risk.

In a 2014 study [3]the respondents were asked to rate their organization’s effectiveness in securing data and applications used in the cloud and 51% say that the likelihood of a data breach increases due to cloud. 62% of respondents were unsure that cloud services were thoroughly vetted before deployment and 69% considered that the organizations failed to be proactive in assessing sensitive information that is destined to be stored on cloud.

According to the same study certain activities such as an increase in the backup and storage of confidential information in the cloud can increase the cost of a breach when customer data is stolen or lost. The quick expansion of the cloud service provider operations followed by financial difficulties also leads to costly data breaches. The least cost occurs when the use of IaaS (Infrastructure as a Service) increases.

Certain activities increase the cost of a breach when sensitive information assets thatcan affect the reputation of a companyare stolen. Bring Your Own Cloud (BYOC), a concept in which the employees of a company are allowed to use public or private third-party cloud services to perform certain job roles results in the most expensive data breaches involving reputation-sensitive data.

The right security technologies and procedures are needed in place in order to protect confidential information while using cloud resources. The majority of companies are circumventing security practices such as conducting audits on the data assets hosted on cloud.

The study shows that there is a lack of confidence in the security practices of cloud providers. There is a concern that the customers of a cloud service provider would not be notified in a timely manner in the case of a data breach or data loss and there is greater concern that cloud providers do not have the necessary security technologies in place. 64% of the respondents do not agree that cloud service providers are in full compliance with privacy and data protection laws and regulations.

The increasing number of devices used inside an organization makes it difficult to determine the extent of cloud use. The lack of visibility of the information assets stored on cloud puts sensitive and confidential information at risk. On average 35% of the information stored on cloud is estimated to not be visible to IT and this leads to the conclusion that many organizations are at risk because they do not know what confidential information that can affect the reputation of the company is stored in the cloud.Changes in an organization’s use of cloud services are also found to affect the likelihood of a data breach.

According to the *Data Breach: The Cloud Multiplier Effect*conducted by the Ponemon Institute, the use of cloud services multiplies up to three times theprobability of a data breach [3].

The lack of accepted security standards makes it difficult for organizations to move data to cloud provider environments and this translates in a difficulty to make risk assessment. Different companies have different views on an appropriate minimum standard for risk evaluation. This further emphasizes that organizations need a set of controls that the cloud providers not only need to implement but also pass regular audits. There is also a need for a requirement that mandates sharing details of the cloud vendor's controls infrastructure prior to the contract. A third-party auditor is also needed for assessing cloud vendors and attesting their security efficacy.

Companies also need a process for managing all security aspects, a process that facilitates the evaluation and selection of cloud service providers. There is a challenge for consumers to assess a provider's capabilities to deliver cost-effective services while protecting the client's data assets. In the model of service delivery a service provider has no access over the client's data beyond the level of management specified in the contract between the two entities. Companies that intent to use cloud providers should become familiar with the basic architectures and the potential areas for vulnerabilities in order to limit data breaches.

Traditional approaches to breach prevention have become ineffective with the rise of targeted attacks. The proportion of breaches discovered within days still falls well below that of time to compromise [5].

In [Fig. 1] we can observe the contrast on how often attackers are able to compromise a target in days with how often defenders detect compromises within that same time frame. We can observe that over the last decade the two lines diverged and that indicates a growing "detection deficit" between attackers and defenders. [5]

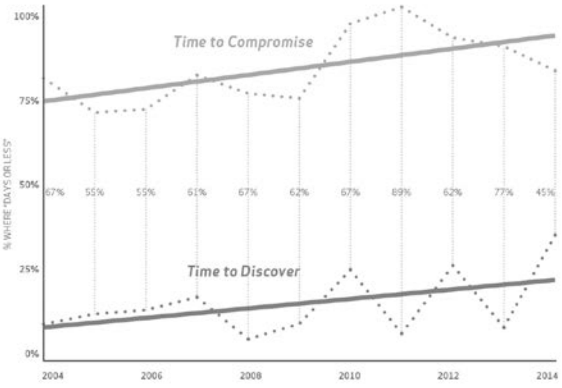

Fig. 1 The Defender-detection deficit

The *CSA Security Guidance for Critical Areas of Focus in Cloud Computing* states that "*The technology architecture and infrastructure of cloud providers may differ; but to meet security requirements they must all be able to demonstrate comprehensive compartmentalization of systems, data, networks, management, provisioning, and personnel. The controls segregating each layer of the infrastructure need to be properly integrated so they do not interfere with each other.*"

The Open Certification Framework (OCF) [4] is an effort of the Cloud Security Alliance to make a risk program for all types of organizations. This consists of three programs: CSA STAR Certification, CSA STAR Attestation and CSA STAR Continuous (that is not yet implemented).

CSA STAR Certification relies on an independent assessment performed by a third-party on a cloud service provider. The assessment is made against the ISO 27001 standard and the CSA Cloud Controls Matrix (CCM).

CSA STAR Attestation provides a report via the SSAE SOC 2 Report, an audit-reporting standard for customer consumption.

CSA STAR Continuous is planned for release in 2015. The purpose of this program is to provide a scanning and monitoring console that can be used by the customers to assess remotely a cloud provider's control statements using an XML-based tag format named CloudAudit and the Cloud Trust Protocol (CTP) for data transmission.

ACCOUNT HIJACKING

Account hijacking is a security threat represented by the stealing or hijacking of an individual's account associated with a service or computing device. In account hijacking, an attacker impersonates the victim in order to obtain personal information, sensitive or confidential data. Usually this type of attack is carried out using phishing, password guessing, spoofed emails and exploitation of software vulnerabilities. There are cases where an email account is linked to other online services and those get compromised as well.

The reuse of passwords amplifies the impact of such an attack. Cloud applications increase the risk because if an attacker gains access to an account he can spy transactions and manipulate data. The hijacked cloud service account can become a base for the attacker and the implications of such an attack can be hard on an organization. Stolen credentials can allow an attacker to access critical areas of cloud computing services compromising their integrity, availability and confidentiality. Defense in depth security strategies are needed in order to mitigate this type of attacks and to contain the damage caused by data breaches. Two-factor authentication is one of the proposed solutions to reduce the risk of account hijacking. Companies should also enforce a restrictive user access policy and prohibit the sharing of account credentials between the different services.

INSECURE INTERFACES AND APIs

Cloud customers can access a set of APIs offered by the service providers in order to manage the cloud services. These interfaces are used for provisioning, orchestration, management and monitoring. The availability and security of the cloud services depend on the security of these APIs and that is why they should be designed with security in mind in order to protect against attempts to circumvent the security policy. Sometimes security risks are introduced by the providers along with custom services that are built on top of these interfaces.It is important that cloud customers understand the full extent of the security implications associated with the management, use and monitoring of cloud Services. A weak set of interfaces exposes cloud consumers to security issues related to availability, confidentiality and integrity of data.

DENIAL OF SERVICE

Denial of service attacks are security threats that affect cloud users by preventing them from accessing hosted applications. The attack forces the cloud service to consume system resources like processing power, disk space or network bandwidth. This type of attack can lead to a non-responsive service causing potential financial losses and damages to the reputation of the cloud provider.

Cloud services on the Internet are commonly the target of Distributed Denial of Service (DDoS) attacks [5]. Common types of attacks include DNS amplification attacks, malformed UDP and TCP packets, SYN floods, and asymmetric application-level attacks.Asymmetric application-layer attacks take advantage of cloud resource vulnerabilities such as web servers and databases, allowing an attacker to take out a service using a small payload.

DDoS attacks can be detected by monitoring the traffic for significant elevation of the number of packets-per-second.There are cases where the service remains available for users but the bandwidth used to get to the service can be consumed, resulting in an unreliable or unreachable service.

In [Fig. 2] we can observe a graph that comprises data from the heaviest DDoS attacks in 2014 [5].

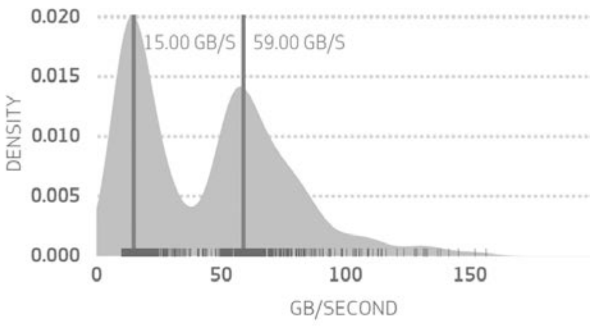

Fig. 2 Density of bandwidth in DDoS attacks (2014)

The mitigation ofdenial of service attacks can be difficult and the cloud service providers need to manage the risk of this type of attack.

The prevention of DNS amplification attacks is conditioned by the cooperation between DNS administrators everywhere. The majority of DNS amplification attacks leverage open DNS name servers, because they resolve DNS queries submitted by any device connected to the Internet. The system administrators must configure their DNS servers to ignore queries from hosts outside their domain.

Denial of service attacks can target any cloud service and cloud providers tend to be better prepared against DDoS attacks than enterprise infrastructures. Moving to cloud can be beneficial for a company due to the scaling of resources that cloud services can provide but in some cases the processing power consumed can become too expensive during an attack for clients that are billed on compute cycles and used disk space.

Cloud computing has the potential to be more secure than traditional infrastructures in the face of DoS attacks because cloud providers are better suited to keep services online while dealing with denial-of-service attacks.

A business continuity plan must be in place prior to any security event that might occur**.** Unprepared staff and stale security policies will increase the severity of such an event. The cloud provider itself should have a disaster recovery and a business continuity program that should meet the cloud customer's requirements.

ABUSE OF CLOUD SERVICES

The abuse of cloud services is a threat that emerges from the fact that an attacker can use large amounts of computing power for malicious purposes that range from cracking an encryption key to the staging of a DDoS attack. Cloud Service providers should take this threat in consideration while developing the incident response strategy and the acceptable use policy that SaaS users, PaaS developers, and IaaS administrators can use for risk reduction.

MALICIOUS INSIDERS

Malicious insiders are current or former employees, business partners, contractors etc. who have or have had valid access to an organization's resources and that are using that access to compromise the confidentiality, integrity or availability of the organization's data or information systems.

In a cloud scenario, insiders can have access starting from the IaaS, PaaS and SaaS to more potentially sensitive information by accessing critical systems. Organizations that rely only on the cloud service provider for security management are at great risk. Site administrators manage and maintain all the cloud computing process and client resources. They can use their knowledge of the security vulnerabilities of a company to access privileged information which can be sold or disclosed to third parties.

Key management in an encrypted cloud environment should be done by the customer to avoid attacks from malicious insiders.

An approach to mitigate the risk of insider threat is the alteration of the operating system. The goal is to monitor the data movement in such a way that every event is being observed by the instrumentation. The event-detection scheme should be performed by a mechanism that receives and acts on the detected events in real time. This mechanism should be adaptive in order to filter events that do not require intervention.

Mitigating the risk of malicious insiders can involve background screening performed by the human resources, user access restriction and authorization, management of user roles and responsibilities along with segregation of duties, encryption, policy enforcement, third party audits etc.

Organizations have basically used two approaches to manage privileged identities. The first approach is the creation of a set of shared accounts that all users that have the privilege can access when they need it.This approach lacks accountability and can be easily breached. The second approach is to give individual accounts to administrators with privileged access to every application they use**.** This approach is complex and hard to scale in the context of global delivery centers, virtualization and cloud computingandthe risks and costs associated with this type of accounts continue to increase.

Companies should make use of privileged identity management solutions that should address these issues. These solutions have to be an integral part of a complete identity and access management framework [6], not just a standalone solution and should include capabilities such as a centralized management of the entire privileged identity lifecycle, accessrequests based on the role and approvals, single sign-on services, secure storage of privileged accounts, monitoring and reporting.

SHARED TECHNOLOGY VULNERABILITIES

By sharing the infrastructure, platforms and applications, the cloud service providers are capable of delivering their service in a scalable way. If the cloud infrastructure components are not designed to offer isolation properties for infrastructures or applications that are used by multiple clients, the cloud provider is exposed to a new type of threat, vulnerabilities that exist in the shared technology. A single vulnerability can lead to the compromise of the entire client portfolio of the cloud service provider.

The hypervisor or virtual machine monitor is a computer software specific to cloud infrastructures that runs virtual machines. A successful attack on this component can expose the entire environment.

INSUFFICIENT DUE DILIGENCE

Organizations that plan to adopt cloud technologies should understand all of the aspects of such a change. Cloud providers promise operational efficiencies and cost reductions but this has to be done with complete understanding of the environment and services and applications that are placed in the cloud, otherwise organizations expose themselves to a new range of risks. Security issues arise when developers that are not familiar with the cloud environment are working on a cloud application. Adequate resources must be provided in order to perform due-diligence to understand the risks of adopting this new computing model.

Conclusions

Cloud computing usage is growing at a fast pace and is often the only way organizations can cope with the rapidly rising requirements. The lack of data visibility in the cloud along with the lack of confidence in the security practices of cloud providers leads to hesitance in the face of cloud adoption. There is a concern that the customers of a cloud service provider would not be notified in a timely manner in the case of a data breach or data loss and there is greater fear that cloud providers do not have the necessary security technologies in place. There is a need for enterprises to track their data as it travels in the cloud andto ensure that the data is protected.To minimize security risk and at the same time benefit from the advantages of cloud computing several components are required: isolation of the critical services to minimize shared technology threats, visibility across applications and infrastructures for a greater control over the data and regular audits in an automated threat detection process.

System administrators shouldcollaborate with cloud providers in order to deliver audit trails and accountabilityfor data events.

Prior to any security event that might occur, an organization should put in place a business continuity plan in case of an attack**.** Unprepared staff will increase the severity of a security breach. Also the cloud provider should have a disaster recovery and a business continuity program plan that the customer should take into consideration.

Despite a lack of best practices for reliable service delivery, transparency, accountability and confidentiality, cloud computing has the potential to be more secure in the face of DoS attacks than traditional infrastructures because cloud providers are better placed to keep services online while dealing with denial-of-service attacks than manyenterprise defenses.

Cloud customers should not rely solely on the cloud providers for security. Although cloud service providers have their own security monitoring tools that ensure the service delivery, companies that use cloud should allocate resources for monitoring data-critical business operations.

Bibliography

[1] Julian Talbot, Miles Jakeman - *Security Risk Management Body of Knowledge,* John Wiley & Sons, 2009
[2]Cloud Security Alliance - *The Notorious Nine Cloud Computing Top Threats in 2013,* 2013
[3]Ponemon Institute LLC Data Breach - *The Cloud Multiplier Effect*, 2014
[4] Cloud Security Alliance - *Security Guidance for Critical Areas of Focus in Cloud Computing*, 2009
[5]Verizon - *2015 Data Breach Investigations Report*, 2015
[6] IBM Software White Paper - *Avoiding Insider Threats To Enterprise Security,* 2012

Additional Bibliography

IBM Developer Works - *Avoid The Risks of Cloud Abuse,* 2013
KPMG - *Cloud Survey Report,* 2014