IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 1, Ver. III (Jan – Feb. 2015), PP 01-04
www.iosrjournals.org

Identified Vulnerabilitis And Threats In Cloud Computing

Mr.Amol R.Yadav
Lecturer, Department of Computer Engineering,
Shree Santkrupa Institute of Engineering & Technology(Polytechnic), Ghogaon, Karad-India

Abstract: *Nowadays Cloud computing becomes a popular research subject. Almost all types of organizations adopting cloud computing technology. Organizations use the Cloud as (SaaS, PaaS, and IaaS) and deployment models (Private, Public, Hybrid, and Community. As cloud services are more efficient to the service providers and clients but some issues in case of security Is important, which we have to take in to account. These types of issues may be faced by service providers as well as clients. In this paper we will revise some cloud security threats.*

Keywords: *Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Application presentation Interfaces (APIs).*

I. Introduction

The number and types of cloud computing service providers increases over the world. They offer the services as an applications, platforms as well as infrastructures in the illusion of unlimited networking resources to the users. But the issues related to the security and effectiveness of cloud services is important from the view of service providers as well as service users. The responsibility goes both the ways, however: the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the user must take measures to fortify their application and use strong passwords and authentication measures. In this document we try to assist the organizations to manage and control the calculated risks about the valuable data of client organizations. In addition this threat research document will be essential for implementing the security policies. The rise and rise of mobile usage and the Cloud have seen third party attackers change their approaches. Cloud services, social media websites and smartphone operating system devices have all become new targets, while traditional user data and website denial of service hacks remain popular. We categorized the analysis of threats in this document. When an organization elects to store data or host applications on the public cloud, it loses its ability to have physical access to the servers hosting its information. As a result, potentially business sensitive and confidential data is at risk from insider attacks. According to a recent Cloud Security Alliance Report, insider attacks are the third biggest threat in cloud computing. Therefore, Cloud Service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data center. Additionally, data centers must be frequently monitored for suspicious activity. In order to conserve resources, cut costs, and maintain efficiency, Cloud Service Providers often store more than one customer's data on the same server. As a result there is a chance that one user's private data can be viewed by other users (possibly even competitors). To handle such sensitive situations, cloud service providers should ensure proper data isolation and logical storage segregation.

II. Categories of Threats

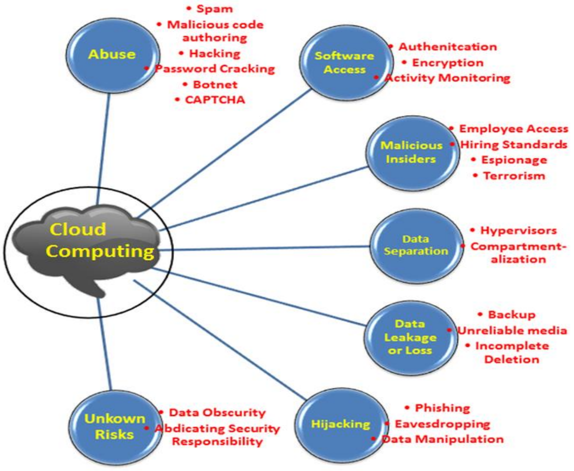

Fig-1. Categories of Threats

A. Abuse of Resources

Almost cloud service providers offer their services with frictionless and easy registration process. So anyone can get access with only credit card. Some providers offers free trial period also. By misusing this information the spammers, malicious code authors, and other criminals have been able to conduct their activities with relative impunity. PaaS providers usually face such type of attacks. Also the possibility is that hackers can attack the PaaS providers also by tracking the confidential information like password and usernames.

For controlling the abuse of PaaS providers can controls operating systems, servers, and network infrastructure needed to run the SaaS application. The provider also controls what social media tools to download to the developer's mobile device. The provider sets the user, resource, data requests, and social media threshold levels. Also for access providers has to control logging capabilities by setting proper authorization. Also SaaS provider manages access controls by limiting the number of authorized users who can concurrently access the application as set forth in a user threshold policy. The provider limits the number of users who can use social media tools as set forth in a social media threshold policy. The provider controls operating systems, servers, and network infrastructure needed to run the SaaS application. The provider also controls what social media tools to download to the mobile device or to use with the device.

B. Insecure Interfaces

Cloud service providers use varieties of software interfaces and APIs that customers use to manage and interact with cloud service. The security and availability of general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy. Since the APIs are accessible from anywhere on the Internet, malicious attackers can use them to compromise the confidentiality and integrity of the enterprise customers. An attacker gaining a token used by a customer to access the service through service API can use the same token to manipulate the customer's data. Therefore it's imperative that cloud services provide a secure API, rendering such attacks worthless. Attackers over the past three years have begun to actively target the digital keys used to secure the Internet infrastructure.

C. Techology Shearing Issues

Working of cloud computing is actually based on shearing of resources. Almost providers present their services in scalable way of shearing infrastructure which is not generally developed for working under multi-tenant architecture. To remove these types of obstacles a virtualization hypervisor mediates access between guest operating systems and the physical compute resources. On the highest layer, there are various attacks on the SaaS where an attacker is able to get access to the data of another application running in the same virtual machine. The same is true for the lowest layers, where hypervisors can be exploited from virtual machines to gain access to all VMs on the same server (example of such an attack is Red/Blue Pill). All layers of shared technology can be attacked to gain unauthorized access to data, like: CPU, RAM, hypervisors, applications, etc.

To enforce these type of problems service venders has to implement security best practices for installation/configuration, Monitor environment for unauthorized changes/activity, Enforce service level agreements for patching and vulnerability remediation, Conduct vulnerability scanning and configuration audits.

D. Data Leakages

Stored data on cloud may loss due to various reasons like hardware failure, drive failure, service vender accidently delete the data, attacker can alter the data, natural phenomenon, etc. Therefore better way to protect the data is to take backup of data time to time. Backup of data solves the problem of data loss. Unlinking the data may cause complexity to identify and recombining the data. These types of occurrences common in almost cloud systems. The confidentiality of data is maintained by venders by providing the encryption method. If there will be loss of any encryption key then there will be chances of data leakages. The threat of data compromise increases in the cloud, due to the number of and interactions between risks and challenges which are either unique to cloud, or more dangerous because of the architectural or operational characteristics of the cloud environment. For recovering these types of threats the venders has to implement strong API access control, provide strong encryption algorithms and keys, analyzing the data protection all stages, and also implement strong backup alternative options.

E. Service Hijacking

This type of attacks occurs mostly on trial and error basis. The service is hacked by attempting the credentials and password provided by the venders to the service users for using the service for maintaining the confidentiality of valuable data. But attacker may attack this data by observing the sessions of users. These types of attacks are not new in market. There is possibility of users to provide the common or easy passwords for maintaining the privacy, but if an attacker gains access to user's credentials, they can eavesdrop on user's activities and transactions, manipulate data, return falsified information, and redirect user's clients to illegitimate sites. User's account or service instances may become a new base for the attacker. From here, they may leverage the power of user's reputation to launch subsequent attacks. To prevent from such threats the venders has to prohibit the sharing of account credentials between users and services, use strong authentication techniques for maintaining the security, implement the methods for detecting the unauthorized access to the services in cloud. It is responsibility of cloud venders to explain the terms and policies of securities to the service users.

F. Malicious Insiders

The threat of a malicious insider is well-known to most organizations. This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure. For example, a provider may not reveal how it grants employees access to physical and virtual assets, how it monitors these employees, or how it analyzes and reports on policy compliance. To complicate matters, there is often little or no visibility into the hiring standards and practices for cloud employees. This kind of situation clearly creates an attractive opportunity for an adversary ranging from the hobbyist hacker, to organized crime, to corporate espionage, or even nation-state sponsored intrusion. The level of access granted could enable such an adversary to harvest confidential data or gain complete control over the cloud services with little or no risk of detection. Some observable insider activities are clearly harmful to the organization—for instance, an insider deleting critical applications from the organization's servers. However, not all insider activity is so blatantly malicious. A clever insider seeking to avoid detection will attempt to use authorized access to the target information systems, and do so in a manner unlikely to raise suspicion. In reviewing the literature, we find many novel proposals for detection of specific insider-related activity, but few that compares the proposed insider behavior to similar non-malicious behaviors, or even acknowledge the necessity of doing so. Few publicly available data sets exist that characterize normal user behavior in relation to indicators of insider threats, much less indicators related to cloud-based insiders. Researchers addressing the challenge of collecting and analyzing normal user behavior should be careful to include attributes useful for cloud-based research as well. Researchers should consider correlating access requests across multiple disparate systems, exploring how often and how much data users transfer from the organization to cloud-based systems (e.g., web-based mail), and how often cloud-based administrative tools are used. Collecting and sharing such information will greatly enhance the ability of other researchers to propose and validate indicators of malicious cloud-related insider behavior. For remediation I suggests to the venders to enforce strict supply chain management and conduct a comprehensive supplier assessment, Specify human resource requirements as part of legal contracts, require transparency into overall information security and management practices, as well as compliance reporting.

G. Data Separation

Every cloud-based service shares resources, namely space on the provider's servers and other parts of the provider's infrastructure. Hypervisor software is used to create virtual containers on the provider's hardware for each of its customers. But CSA notes that "attacks have surfaced in recent years that target the shared technology inside Cloud Computing environments." So, investigate the compartmentalization techniques, such as data encryption, the provider uses to prevent access into your virtual container by other customers. Although you should address these security issues with the cloud provider before you entrust your data to its servers and applications, they shouldn't be a deal breaker. Cloud computing offers small businesses too many benefits to dismiss out of hand. After all, you already met many of these security challenges the first time you connected your network to the Internet.

H. Unknown Risks

One of the tenets of Cloud Computing is the reduction of hardware and software ownership and maintenance to allow companies to focus on their core business strengths. This has clear financial and operational benefits, which must be weighed carefully against the contradictory security concerns complicated by the fact that cloud deployments are driven by anticipated benefits, by groups who may lose track of the

security ramifications. Versions of software, code updates, security practices, vulnerability profiles, intrusion attempts, and security design, are all important factors for estimating your company's security posture. Information about who is sharing your infrastructure may be pertinent, in addition to network intrusion logs, redirection attempts and/or successes, and other logs. Security by obscurity may be low effort, but it can result in unknown exposures. It may also impair the in-depth analysis required highly controlled or regulated operational areas.

III. Conclusion

At this stage as cloud computing is an important aspect in day to day life in networking world but side by side the threatening issues have to take in account and have to find an efficient way to overcome these issues.

References

[1]. Top threats to cloud computing V1.0,cloud security alliance,2010
[2]. K. Thejaswi, I. Sheeba, C. Bhuvana, P. Lavanya , Insight Of Cloud-Specific Culpabilities, Risks, Threats.
[3]. Adam Swidler, seven security threats in cloud,2010.
[4]. Shaikh, F.B., Haider, S. Dept. of Comput. & Technol., SZABIST, Islamabad, Pakistan (IOSRJEN)ISBN- 978-1-4577-0884-