International Journal of Latest Trends in Engineering and Technology
Vol.(9)Issue(2), pp.074-078
DOI: http://dx.doi.org/10.21172/1.92.13
e-ISSN:2278-621X

PREVENTIVE MEASURES FOR CLOUD ATTACKS

G.Rekha[1] & C.Pradeepthi[2]

Abstract- As Cloud Computing is becoming an emerging technology, more and more industries are moving towards Cloud Computing, with tremendous data being generated every hour, the need of the hour is not just 24X7 availability but also security. The small and medium-size organizations can manage their projects by using cloud-based services and also able to achieve productivity enhancement with limited budgets. But, apart from all of these benefits, it may not be fully trustworthy. Cloud Computing do not keep data on the user's system, so there is a need of data security. The user pays progressively attention about data security due to this off-side storage of data on cloud computing. In this paper, all possible threats to security in cloud computing are presented and we shall discuss security concerns in Cloud Computing and shall also suggest some measures to improve security.
Keywords – Cloud Computing, Hypervisor, Intrusion Detection, Security mechanism.

I. INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction[4]. There are three service models of Cloud computing namely Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a service (IaaS). As per NIST's recommendations, four deployment models of Cloud Computing have been proposed, namely Private Cloud, Community Cloud, Public Cloud and Community Cloud. Since it is relatively inexpensive and less time consuming to deploy existing applications over the latter three deployment models, serious security issues need to examined. Our research paper is an attempt to investigate these issues and suggest solutions in order to maximize the benefits of Cloud Computing.

1.1 Threat No. 1: Data breaches

Cloud environments face many of the same threats as traditional corporate networks, but due to the vast amount of data stored on cloud servers, providers become an attractive target. The severity of potential damage tends to depend on the sensitivity of the data exposed. Exposed personal financial information tends to get the headlines, but breaches involving health information, trade secrets, and intellectual property can be more devastating. When a data breach occurs, companies may incur fines, or they may face lawsuits or criminal charges. Breach investigations and customer notifications can rack up significant costs. Indirect effects, such as brand damage and loss of business, can impact organizations for years. Cloud providers typically deploy security controls to protect their environments, but ultimately, "organizations are responsible for protecting their own data in the cloud".

1.2 Threat No. 2: Compromised credentials and broken authentication

Data breaches and other attacks frequently result from lax authentication, weak passwords, and poor key or certificate management. Organizations often struggle with identity management as they try to allocate permissions appropriate to the user's job role. More important, they sometimes forget to remove user access when a job function changes or a user leaves the organization. Multifactor authentication systems such as one-time passwords, phone-based authentication, and smartcards protect cloud services because they make it harder for attackers to log in with stolen passwords. The Anthem breach, which exposed more than 80 million customer records, was the result of stolen user credentials. Anthem had failed to deploy multifactor authentication, so once the attackers obtained the credentials, it was game over. Many developers make the mistake of embedding credentials and cryptographic keys in source code and leaving them in public-facing repositories such as GitHub. Keys need to be appropriately protected, and a well-secured public key infrastructure is necessary. They also need to be rotated periodically to make it harder for attackers to use keys they've obtained without authorization. Organizations planning to federate identity with a cloud provider need to understand the security measures the provider uses to protect the identity platform. Centralizing identity into a single repository has its risks. Organizations need to weigh the trade-off of the convenience of centralizing identity against the risk of having that repository become an extremely high-value target for attackers.

[1] Department of Computer Science & Engineering, SPMVV, Tirupathi, Andhra Pradesh, India
[2] Department of Computer Science & Engineering, SPMVV, Tirupathi, Andhra Pradesh, India

1.3 Threat No. 3: Hacked interfaces and APIs

Practically every cloud service and application now offers APIs. IT teams use interfaces and APIs to manage and interact with cloud services, including those that offer cloud provisioning, management, orchestration, and monitoring.The security and availability of cloud services -- from authentication and access control to encryption and activity monitoring -- depend on the security of the API. Risk increases with third parties that rely on APIs and build on these interfaces, as organizations may need to expose more services and credentials. Weak interfaces and APIs expose organizations to security issues related to confidentiality, integrity, availability, and accountability.APIs and interfaces tend to be the most exposed part of a system because they're usually accessible from the open Internet.

1.4 Threat No. 4: Exploited system vulnerabilities

System vulnerabilities, or exploitable bugs in programs, are not new, but they've become a bigger problem with the advent of multitenancy in cloud computing. Organizations share memory, databases, and other resources in close proximity to one another, creating new attack surfaces. Fortunately, attacks on system vulnerabilities can be mitigated with "basic IT processes,". Best practices include regular vulnerability scanning, prompt patch management, and quick follow-up on reported system threats.

1.5 Threat No. 5: Account hijacking

Phishing, fraud, and software exploits are still successful, and cloud services add a new dimension to the threat because attackers can eavesdrop on activities, manipulate transactions, and modify data. Attackers may also be able to use the cloud application to launch other attacks.Common defense-in-depth protection strategies can contain the damage incurred by a breach. Organizations should prohibit the sharing of account credentials between users and services, as well as enable multifactor authentication schemes where available. Accounts, even service accounts, should be monitored so that every transaction can be traced to a human owner. The key is to protect account credentials from being stolen.

1.6 Threat No. 6: Malicious insiders

The insider threat has many faces: a current or former employee, a system administrator, a contractor, or a business partner. The malicious agenda ranges from data theft to revenge. In a cloud scenario, a hellbent insider can destroy whole infrastructures or manipulate data. Systems that depend solely on the cloud service provider for security, such as encryption, are at greatest risk.

1.7 Threat No. 7: The APT parasite

This advanced persistent threats (APTs) "parasitical" forms of attack. APTs infiltrate systems to establish a foothold, then stealthily exfiltrate data and intellectual property over an extended period of time. APTs typically move laterally through the network and blend in with normal traffic, so they're difficult to detect. The major cloud providers apply advanced techniques to prevent APTs from infiltrating their infrastructure, but customers need to be as diligent in detecting APT compromises in cloud accounts as they would in on-premises systems. Common points of entry include spear phishing, direct attacks, USB drives preloaded with malware, and compromised third-party networks.

1.8 Threat No. 8: Permanent data loss

As the cloud has matured, reports of permanent data loss due to provider error have become extremely rare. But malicious hackers have been known to permanently delete cloud data to harm businesses, and cloud data centers are as vulnerable to natural disasters as any facility. Cloud providers recommend distributing data and applications across multiple zones for added protection. Adequate data backup measures are essential, as well as adhering to best practices in business continuity and disaster recovery. Daily data backup and off-site storage remain important with cloud environments. The burden of preventing data loss is not all on the cloud service provider. If a customer encrypts data before uploading it to the cloud, then that customer must be careful to protect the encryption key. Once the key is lost, so is the data. Compliance policies often stipulate how long organizations must retain audit records and other documents. Losing such data may have serious regulatory consequences. The new EU data protection rules also treat data destruction and corruption of personal data as data breaches requiring appropriate notification. Know the rules to avoid getting in trouble.

1.9 Threat No. 9: Inadequate diligence

Organizations that embrace the cloud without fully understanding the environment and its associated risks may encounter a "myriad of commercial, financial, technical, legal, and compliance risks". Due diligence applies whether the organization is trying to migrate to the cloud or merging (or working) with another company in the cloud. For example, organizations that fail to scrutinize a contract may not be aware of the provider's liability in case of data loss or breach. Operational and architectural issues arise if a company's development team lacks familiarity with cloud technologies as apps are deployed to a particular cloud. The organizations they must perform extensive due diligence to understand the risks they assume when they subscribe to each cloud service.

1.10 Threat No. 10: Cloud service abuses

Cloud services can be commandeered to support nefarious activities, such as using cloud computing resources to break an encryption key in order to launch an attack. Other examples including launching DDoS attacks, sending spam and phishing emails, and hosting malicious content.Providers need to recognize types of abuse -- such as scrutinizing traffic to recognize DDoS attacks -- and offer tools for customers to monitor the health of their cloud environments. Customers should make sure providers offer a mechanism for reporting abuse. Although customers may not be direct prey for malicious actions, cloud service abuse can still result in service availability issues and data loss.

1.11 Threat No. 11: DoS attacks

DoS attacks have been around for years, but they've gained prominence again thanks to cloud computing because they often affect availability. Systems may slow to a crawl or simply time out. “Experiencing a denial-of-service attack is like being caught in rush-hour traffic gridlock; there is one way to get to your destination and there is nothing you can do about it except sit and wait,” the report said. DoS attacks consume large amounts of processing power, a bill the customer may ultimately have to pay. While high-volume DDoS attacks are very common, organizations should be aware of asymmetric, application-level DoS attacks, which target Web server and database vulnerabilities. Cloud providers tend to be better poised to handle DoS attacks than their customers. The key is to have a plan to mitigate the attack before it occurs, so administrators have access to those resources when they need them.

1.12 Threat No. 12: Shared technology, shared dangers

Vulnerabilities in shared technology pose a significant threat to cloud computing. Cloud service providers share infrastructure, platforms, and applications, and if a vulnerability arises in any of these layers, it affects everyone. “A single vulnerability or misconfiguration can lead to a compromise across an entire provider’s cloud,” the report said. If an integral component gets compromised -- say, a hypervisor, a shared platform component, or an application -- it exposes the entire environment to potential compromise and breach. It is recommended that a defense-in-depth strategy, including multifactor authentication on all hosts, host-based and network-based intrusion detection systems, applying the concept of least privilege, network segmentation, and patching shared resources.

2. PREVENTIVE MEASURES

International Standards Organization (ISO) defined a standard ISO 7498-2 that states that prevention, detection and elimination all are needed to control and minimize threat in Information Security. Same concept is followed in Cloud computing, but prevention and detection processes are difficult to implement due to complex nature of Cloud. Security requirement for a secure Cloud computing are discussed below

2.1 Identification and authentication:

Users are provided rights to access information in Cloud, but the access can be limited by some constraints. Information Assurance (IA) Technology Professionals defined that Cloud provider controls the access privileges of Cloud user. Users or enterprises are provided a unique ID and corresponding password for their identification and level of services are provided to that authenticated entity after successful verification.

2.2 Authorization:

Authorization ensures that integrity of the Cloud is maintained, thus it plays an important role in security of Cloud. It is kept in back end of any Cloud as all Cloud facilities lies there. Information Assurance team stated that any organizations will be immune from damage from insiders if authorized access is maintained to protected information assets.

2.3 Confidentiality:

In Clouds, Data or information is stored across multiple distributed databases and any attacker can access data if confidentiality is not kept under notice during development of Cloud. Confidentiality ensures that only authorized data can only be accessed by authorized users not by any unauthorized user. Safety of Cloud data is not only the major concern but preventing any attacker to access personal information of any Cloud user is also need to addressed

2.4 Integrity:

The integrity ensures that Cloud data is not modified or tampered. So Cloud should be in same state if no authorized operation is performed on Cloud. Unauthorized alteration or modification of Cloud data may lead to low trust rating of Cloud.

2.5 Non-repudiation:Non-repudiation is a major problem in Cloud as it cannot be proved that whether that action was performed or not for e.g. in a faulty environment and without any precaution we cannot be ensured that a search query in Cloud was performed properly. Jun Feng showed that applying token provisioning in Cloud applications for data transmission

using digital signature and confirmation receipts (i.e. digital receipt of message sent or received confirmation) may ensure non-repudiation.

2.6 Availability:

Availability is major requirement for information security in Clouds .The NIST defined Availability as whether resources of any Cloud are accessible or available to Cloud user or not. It can be affected permanently or temporarily. It can be attacked by blocking some resources so that Cloud user cannot access them anymore, such attacks are equipment outages, Denial of service attacks, and natural disasters etc.

2.7 Deploying Intrusion Detection Systems:

Attacks on systems and data are a reality in the world we live in. Detecting and responding to those attacks has become the norm and is considered due diligence when it comes to security. As a matter of fact, most of the standards and regulations applied in the technology space today have explicit instructions regarding the need for monitoring and alerting, or intrusion detection. Deploying Intrusion Detection Systems offers a lot of choices namely deployment at guest OS level, as a separate Virtual Machine, at hypervisor level, at virtual network level or at physical network level.

2.8 Securing Hypervisor:

A hypervisor, also called a virtual machine manager, is a program that allows multiple operating systems to share a single hardware host. Each operating system appears to have the host's processor, memory, and other resources all to itself. However, the hypervisor is actually controlling the host processor and resources, allocating what is needed to each operating system in turn and making sure that the guest operating systems (called virtual machines) cannot disrupt each other.

2.9 Data encryption for the Cloud:

Confidentiality, Integrity and Availability are concerns that need to be addressed before applications are ported into Cloud. Deploying data encryption can address these concerns but the choice of techniques can baffle any customer. Data can be encrypted while it is at rest (in the Storage Array) or while it is in transit (at the Network Level). Organizations such as Cipher Cloud offering Cloud enabled services have implemented strong software-based cryptographic key management based on the NIST SP 800- 21 standard that included key rotattion, split custodians, key encrypting keys and many other capabilities.

3. CONCLUSION AND FUTURE WORK

It has now been established that the business is taking a leading role in adopting cloud. This is because ever more the businesses realise that cloud computing is helping to achieve business goals. Public We have identified potential weak-links in the Cloud implementations of various CSP's and have suggested measures to mitigate the security threats. We have also envisioned a road map for future work related to Cloud Computing which involves identifying the main challenges when migrating services to the cloud. We further aim to identify the security issues and the problems which can derive from loss of control. We shall also attempt at a possible implementation of a reliable monitoring tool which shows the mapping of the client's services to the underlying virtualized and physical layers wherein the status and performance of these services could be monitored near real-time. The contents of data security are more extensive in the cloud. This security policy designed the data in the cloud computing that it just to solve the client's own data security protection. Once the data is stored into the public cloud, the protection of its data security will be more complex both from a technical and management. Especially the users require a higher for data integrity, security and controllability. If you want to enjoy the additional benefits of public cloud, you must still to wait for cloud computing security technology. We believe that the proposed "technology + management" Safety management philosophy which will be an important direction to address the cloud computing security issues in the future.

4. REFERENCES

[1] [1] Peter Mell, Timothy Grance, "NIST Definition of Cloud Computing v15," 2011 www.csrc.nist.gov/groups/SNS/cloud-computing/clouddef-v15.doc.

[2] [2] Zhang, Q., Cheng, L. & Boutaba, R., "Cloud computing: state-of-the-art and research challenges." Journal of Internet Services and Applications,1(1), p.7-18. 2010.

[3] [3] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. "Above the clouds: a Berkeley view of cloud computing," EECS Department University of California Berkeley Tech Rep UCBEECS200928, 2009 http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf.

[4] [4] Guo C, Lu G and Li D "BCube: A high performance, server-centric network architecture for modular data centers". In: Proceeding SIGCOMM ACM (2009).

[5] [5] Ghemawat S, Gobioff H, Leung "The Google file system". Proceeding SOSP '03 Proceedings of the nineteenth ACM symposium on Operating systems principle Pages 29-43, 2003.

[6] [6] Hadoop Distributed File System, www.hadoop.apache.org.

[7] [7] Dean J, Ghemawat S, "Map Reduce: simplified data processing on large clusters". Communication of the ACM, Volume 51, Pages 107-113, ACM 2008.

[8] [8] Hanqian Wu; Yi Ding; Winer, C.; Li Yao; , "Network security for virtual machine in cloud computing," Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference on , vol., no., pp.18-21, Nov 30 2010.

[9] [9] Behl, A.; "Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation," Information and Communication Technologies (WICT), 2011 World Congress on , vol., no., pp.217-222, 2011.

[10] [10] S. Skorobogatov, “Side-channel attacks: new directions and horizons”, ECRYPT2 School on Design and Security of Cryptographic Algorithms and Devices, 29 May-03 June 2011, Albena near Varna, Bulgaria.